Cybercrime Convention

Last change: 29.07.2026

PDF generated on: 05.10.2026



ONLINE COMMENTARY
THE OPEN ACCESS
LEGAL COMMENTARY

TABLE OF CONTENTS

Art. 1 CCC (Convention on Cybercrime) 5
Art. 2 CCC (Convention on Cybercrime) 27
Art. 3 CCC (Convention on Cybercrime) 41
Art. 4 CCC (Convention on Cybercrime) 53
Art. 5 CCC (Convention on Cybercrime) 63
Art. 6 CCC (Convention on Cybercrime) 75
Art. 7 CCC (Convention on Cybercrime) 87
Art. 8 CCC (Convention on Cybercrime) 97
Art. 9 CCC (Convention on Cybercrime) 105
Art. 11 CCC (Convention on Cybercrime) 119
Art. 12 CCC (Convention on Cybercrime) 125
Art. 16 CCC (Convention on Cybercrime) 141
Art. 18 CCC (Convention on Cybercrime) 155
Art. 25 CCC (Convention on Cybercrime) 171
Art. 27 CCC (Convention on Cybercrime) 183
Art. 28 CCC (Convention on Cybercrime) 201
Art. 29 CCC (Convention on Cybercrime) 209
Art. 32 CCC (Convention on Cybercrime) 229
Art. 33 CCC (Convention on Cybercrime) 269
Art. 34 CCC (Convention on Cybercrime) 283

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 1 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 1 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 1 CCC N. XXX.

Chapter I – Use of terms
Article 1 – Definitions

For the purposes of this Convention:

a. "computer system" means any device or a group of i nterconnected or related devices,
one or more of which, pursuant to a program, performs automatic processing of data;

b. "computer data" means any representation of f acts, information or concepts in a form
suitable for processing in a computer system, including a program suitable to cause a

computer system to perform a function;

c. "service provider" means:
i any public or private entity that provides to users of i ts service the ability to
communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of s uch
communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a
computer system, generated by a computer system that formed a part in t he chain of
communication, indicating the communication's origin, destination, route, time, date, size,
duration, or type of underlying service.

CONTENT

I. General Provisions 8
II. Computer System (Let. A) 8
A. A System 9
B. A Program 10
C. Automated Data Processing 11
D. Outlook 12
1. The Dematerialization of Computer Systems 12
2. The Internet of Things (IoT) 13
3. Artificial Intelligence 13
III. Computer Data (Letter b) 14
A. The Form of Data 15
B. Types of Data 16
C. Programs 17
D. Outlook 17
E. Digression: The Distinction Between Subscriber Data, Traffic Data, and Content Data in Swiss Criminal Law 17
1. Subscriber data 18
2. Traffic data (or secondary data) 18
3. Content Data 19
IV. Service Provider (subpar. c) 20
A. Access Providers 20
B. Hosting and Content Providers 22
C. Outlook 23
V. Traffic Data (Letter d) 23
Bibliography 26
Travaux législatifs 26

I. GENERAL PROVISIONS

1 The Convention on Cybercrime begins by providing, in Article 1, four definitions of the key concepts referred to in the various articles that follow. The drafters of the Convention did, however, specify in their Explanatory Report that the Parties would not be required to reproduce verbatim, in their domestic laws, the four concepts defined in Article 1 of the Convention. However, they did specify that national laws must cover these concepts in a manner consistent with the principles of the Convention and provide an equivalent framework for its implementation. The purpose of these definitions is therefore clear: to place all Parties on an equal footing to ensure that they are referring to the same concepts. This helps, in particular, to**avoid disputes**, such as a Party refusing to enforce certain provisions on the grounds that it interprets a concept differently from another Party.

2 The drafters of the Convention were clearly **aware of the rapid evolution** of information technology. This is undoubtedly why they decided to formulate the definitions in Article 1 of the CCC as technologically neutral as possible, limiting themselves to a functional description of each concept. This strategy has paid off, since, twenty-five years later, these definitions remain relevant despite the considerable technological advances that have taken place during this period.

II. COMPUTER SYSTEM (LET. A)

3 The definition adopted by the drafters of the Convention on Cybercrime consists of **three aspects**. First, it presupposes the existence of a device. This device may be standalone or networked. The definition therefore encompasses both personal computers and interconnected computer environments. The second element is the presence of a program. The device must therefore operate on the basis of pre-established instructions. The device cannot be purely mechanical. A music box or a clock, therefore, are not computer systems. Finally, data processing must occur automatically. It is not sufficient for the device to merely store data passively; it must automatically perform a process to transform that data. A camera, a voice recorder, or a USB flash drive are therefore not computer systems.

In its guidelines, the Committee of the Convention on Cybercrime clarified that the definition of "computer system" includes, for example, **modern mobile phones** that are multifunctional and have, among their functions, the ability to generate, process, and transmit data—such as accessing the Internet, sending emails, transmitting attachments, and downloading content or documents. The same applies to **personal digital assistants**, with or without wireless functionality, which also generate, process, and transmit data. 4

The definition adopted deliberately approaches the computer system from the perspective of its **functionality**, rather than its form. This approach provides sufficient flexibility for the definition to evolve over time and include technologies that did not yet exist in 2001, such as *smartphones*, the Internet of Things (*IoT*), or *cloud computing*. 5

A. A System

Computer science is fundamentally based on data processing. This concept will be discussed in more detail below in Section III. At this stage, data can be defined as intangible digital information. However, in order to be processed, this information requires a **set of hardware components** that enable both its processing and storage. 6

Although it is not the most important component of a computer system, the **motherboard** nevertheless serves as its backbone. It is a large electronic board that serves as the foundation for all the system's components. The truly central element of the computer system is the **processor.** It represents the heart of the system, in that it processes all the instructions and requests it receives from the various components. Once the data has been processed, the processor must be able to store it temporarily somewhere, since it has no memory of its own. The data is therefore temporarily stored in **RAM.** However, this memory can only store data while the computer system is powered on. When it is turned off, all data contained in this memory is lost. It is therefore necessary to provide permanent storage for this data on an appropriate device, such as a hard drive, an external hard drive, a USB flash drive, a DVD, etc. 7

The final components essential to the operation of a computer system are **peripherals**. Input devices allow data to be entered into the system, such as a mouse, keyboard, or scanner. In contrast, output devices display the data pro- 8

cessed by the system, such as a monitor, printer, or DVD burner. All these physical elements are called *hardware* and together form a system.

9 However, it would be simplistic to assume that all the components making up the system must necessarily be located in **a single place** in a compact configuration, as this would limit the concept of a system to a personal computer or a *smartphone*. In fact, there are currently supercomputers that each occupy an entire hall. Conversely, there are also systems whose components are scattered all over the globe.

10 A system can operate in an **isolated** manner or in an interconnected manner. Before the widespread adoption of the Internet in the mid-1990s, most systems operated in isolation. Since then, this mode of operation has become the exception, reserved for situations requiring the highest level of security—particularly to prevent any intrusion via external connections.

11 Devices are **interconnected** when they are linked to one another via a wired or wireless connection—such as radio waves, infrared links, fiber optics, or satellite links—thereby forming a network. This network may be limited to a specific geographic area, such as a home, a business, or a university. This is known as a local area network (*Local Area Network* or LAN). However, such a network can also extend over a much larger area, such as a city, a country, or a continent. This is referred to as a wide area network (*Wide Area Network* or WAN). The largest wide area network is the Internet, since it consists of a multitude of interconnected networks spanning the entire globe.

12 Finally, the concept of a device also includes **other devices** that enable computers connected to networks to exchange data. As such, servers, routers, switches, modems, and gateways must also be classified as devices.

B. A Program

13 In contrast to hardware components are software components, which encompass all the programs that enable **the operation and use** of the various components of the computer system.

14 A program can be defined as a **set of commands** that, when executed by a computer system, produce a specific result.

15 Just as with hardware components, programs should be distinguished based on the task they perform. The “boot” program for any computer system is the

BIOS (*Basic Input and Output System*) or **UEFI** (*Unified Extensible Firmware Interface*). It is contained in a chip connected to the motherboard and provides the elements necessary for booting the system. In addition, it handles the basic management of the computer system's various hardware components and acts as an interface between these components and the operating system.

The **operating system**, for its part, is the central program of the computer system. It ensures the overall and consistent operation of the system by coordinating the various requests sent to the computer system by the user, as well as the interactions between hardware components and other programs. In other words, the operating system acts as an essential interface between application software and the system's hardware components. 16

Finally, application programs each perform a specific **function**. For example, Word© is used for word processing, Photoshop© for image processing, and Outlook© for sending and receiving emails. These programs, however, rely on the operating system to access hardware resources and perform the tasks for which they were designed. 17

C. Automated Data Processing

Automated data processing refers to the fact that data is processed automatically by a program, **without** the need for direct **human intervention**. This processing may involve the acquisition, storage, or retrieval of data. 18

As we will see below in Section III, data constitutes intangible digital information. In order to be processed by a computer system, information from the physical world must be converted into a **language understandable by the device**. Thus, pressing a keyboard key, a mouse button, or a touchscreen is translated into binary code and converted into electrical, logical, or optical signals. 19

Once the physical information has been converted into electrical, logical, or optical signals, the program is able to perform automated data processing. When processing is complete, the data is once again translated into a **language intelligible to the user**. The program can thus, for example, display alphabetic characters on a screen when a user presses keys on a keyboard, send the visual information displayed on the screen to a printer so that it is reproduced on paper when the the user clicks the "print" icon, or even establish 20

a phone call when the user taps the green phone icon on the touchscreen of their *smartphone*. Each instruction given by the user to the computer system results in the creation of computer data, which is processed automatically by programs and then returned to the user in a form they can understand.

D. Outlook

1. The Dematerialization of Computer Systems

21 As early as the 1980s, the idea of distributed computing emerged, notably through the slogan coined by Sun Microsystems: "*The network is the computer!*" This approach is based on the **pooling of computing resources** to process larger volumes of data. From this perspective, when the network in question is the Internet, the "computer" it represents consists of all the computers connected to it, which amounts to a particularly vast computing capacity. It was in this context that, starting in the late 1990s and with the widespread adoption of the Internet, distributed computing projects began to emerge. These projects involve offering individuals the opportunity to make the computing power of their personal computers available via the Internet when they are not using them, in order to perform calculations that require very high processing capabilities.

22 Over time, this concept of resource sharing expanded beyond just the processor. The entire computer architecture has gradually been reimagined to become a **distributed architecture**, in the sense that the various available resources are no longer necessarily located in the same place or on the same machine. A prime example of a distributed architecture that experienced explosive growth in the early 2000s is the so-called "peer-to-peer" (*peer-to-peer*) model. This model enables file sharing within an architecture in which each computer acts as both a client and a server.

23 Between the late 2000s and the early 2010s, *cloud computing* ("cloud computing"), which involves using remote computer servers connected to the Internet to store, manage, and process data, rather than relying on a local server or a personal computer. In particular, this technology allows users to create a virtual computing system, install an operating system and applications on it, and generate, process, and save data there. All that is needed is a device connected to the Internet; all other resources are made available virtually and in a decentralized manner, originating from various locations and sometimes from

different service providers around the world. In such a configuration, it is easy to see how the term "system" can become problematic, since there is no longer a physical unity of components.

2. The Internet of Things (IoT)

In recent years, we have witnessed a veritable explosion in the number of **connected objects**. Whether they are watches, ovens, televisions, or vehicles, virtually all everyday objects exist in a form that can be connected to the Internet. 24

In the 1990s, SCHMID asserted, citing the Federal Council's Message, that vending machines for food, gasoline, and tickets, photocopiers, or slot machines could not be classified as computer systems, on the grounds that the federal legislature had intended to limit the concept of a computer system solely to devices capable of performing **so-called "higher-level" functions."** 25

This view can no longer be defended today. Connected devices are now an integral part of the Internet, can be controlled remotely, and are capable of performing so many tasks that they meet all the criteria for being classified as computer systems within the meaning of Art. 1(a) of the Swiss Civil Code (CCC). This **paradigm shift**, however, raises serious problems. Connected devices generally do not benefit from security measures equivalent to those of traditional computers. Cybercriminals can therefore more easily gain unauthorized access to a smartwatch to extract the payment methods it it contains, unlock a door connected to a home automation system to enter a residence, or even gain access to a corporate network by connecting without authorization to the connected coffee machine in the cafeteria, than by accessing a personal computer that is specifically protected against unauthorized access. As a result, the scope of application of Art. 2 of the Swiss Civil Code (CCC), for states that do not require—as Switzerland does—that the offense be committed in violation of security measures, is particularly broad and is likely to expand even further in the coming years. 26

3. Artificial Intelligence

As noted above (in Section II, Subsection B), the definition set forth in Art. 1(a) CCC presupposes that a computer system is equipped with a program. In principle, this program executes a series of commands predefined by humans. With the rise of artificial intelligence, the **immutable nature of programs** is 27

no longer necessarily a given. Systems based on artificial intelligence are, in fact, capable of autonomous learning and can, in certain configurations, modify their own source code or adapt the parameters of the environment in which they operate. This raises the question of whether the concept of a computer system, as currently defined, remains broad enough to encompass these technological developments, or whether a redefinition is necessary to account for future advancements in the field of artificial intelligence. In our view, the current definition is broad enough to encompass the technological developments known to date. Indeed, even if artificial intelligence is capable of rewriting a program's source code to adapt to its environment, the computer system continues to operate on the basis of a program.

28 **Two emerging issues**, however, may require a redefinition in the coming years. The first is autonomous, deployed agent-based artificial intelligence—that is, agents capable of negotiating, migrating between environments, creating other agents, or modifying their own infrastructure without human intervention. This raises the issue of the unity of the computer system, as it would no longer be possible to clearly determine at what point a swarm of agents still constitutes a single computer system or multiple systems. Furthermore, the Convention does not address the concept of ephemeral, distributed, and self-organizing computer systems. The second issue concerns neuromorphic artificial intelligence—that is, AI without separate programs. An example of this is Intel's Loihi chips, which mimic the human brain. Unlike traditional processors, these chips process information event-driven and integrate memory into the processor. There is therefore no longer a "program " distinct from the hardware. Execution and learning are inseparable, meaning that the current definition of a computer system would become obsolete.

29 In the medium term, it would therefore be necessary to**expand the definition** of a computer system to include, on the one hand, deployed autonomous agents and, on the other hand, to any hardware or hybrid device that performs data processing through machine learning, even when execution does not rely on a separate program.

III. COMPUTER DATA (LETTER B)

30 Computer data is defined as "*any representation of facts, information, or concepts in a form suitable for computer processing, including a program capable of causing a computer system to perform a function*" (Art. 1, Letter b, CCC).

This definition, taken from that of the International Organization for Standardization (ISO), is characterized by its **technological neutrality**. This has given it the advantage of having withstood remarkably well the rapid evolution of technologies since the Convention's adoption in 2001.

A. The Form of Data

Computer systems use a **language** that is fundamentally different from that of humans. A text, an image, or a musical work created by humans has, in and of itself, no meaning for a computer. To be understood and processed, this information must be converted into a language that is intelligible to the machine. It is in this context that the definition of "computer data" adopted in the Convention uses the terms "which lends itself to processing." This means that the representation of facts, information, or concepts must be capable of being processed directly by a computer system, without requiring prior transformation to enable the system to recognize it. Computer data is therefore information that can be directly understood and utilized by a computer. 31

Computing is based on a **binary system**, which means it uses only the digits 0 and 1. This basic unit of information is called a *bit.* A sequence of eight bits constitutes a byte (e.g., 10011101), which can represent 2^8, or 256 distinct values. This system makes it possible to translate information from human language into instructions that a machine can understand. Depending on the program being used, a byte can represent a number, a letter, a color, or even a sound. For example, when a user presses the letter "a" on their computer keyboard in a word processing program, this action is converted into binary code as "01100001." This byte constitutes data that the computer can process by displaying an "a" on the screen. Similarly, colors are converted into values distributed across three axes: red, green, and blue. A value of 0 indicates that the color is absent, and a value of 255 indicates that the color is at maximum intensity. Thus, an apricot-colored pixel in a drawing program will be represented by the values 230 on the red scale, 126 on the green scale, and 48 on the blue scale—which, in binary, is "111001101111111011000000." This 24-bit data allows the drawing program to display an apricot-colored pixel on the white page. 32

The preceding examples illustrate that, in computer science, a data unit is the basic unit that contains information. Conversely, when a set of data is com- 33

bined to form a coherent whole, it is referred to as a **file**. This can be text, an image, a video, or an audio recording.

B. Types of Data

34 The definition in Art. 1(b) of the Swiss Civil Code (CCC) makes **no distinction** between different types of data. All computer data is covered, whether personal or not, private or public, understandable by humans or only by machines. The content of the data is also irrelevant, whether it consists of factual data (dates, times, measurements, etc.), information (reports, analyses, etc.) or abstract concepts (models, algorithms, codes, etc.). Therefore, data stored on storage media, temporary data, data in transit, metadata, and even encrypted data all constitute "data" within the meaning of Art. 1(b) of the Swiss Civil Code (CCC).

35 In our view, in addition to human-generated data, we must include data automatically produced by a computer system from preexisting data—referred to as **derived or inferred data**—particularly through processes of transformation, combination, or algorithmic analysis. Examples include user profiles, scores, predictions, or classifications generated without direct human intervention. Although this data is not initially provided by a user, we believe it should also be included in the definition of Art. 1(b) of the Swiss Civil Code (CCC), provided that it is suitable for computer processing and can be utilized by a computer system.

36 In our view, the definition of computer data also extends to **volatile** (or ephemeral) data, including data temporarily stored in a system's random-access memory, dynamically generated during program execution, or intended to disappear automatically after a very short period of time. Although its lifespan is brief, such data is of particular importance in the context of criminal investigations, especially in cases of unlawful access (Art. 2 CCC) or a violation of system integrity (Art. 5 CCC) through a distributed denial-of-service attack.

37 Given that the definition of computer data focuses solely on function, it is irrelevant whether the data is intelligible to a human being. Data remains computer data even when it is **encrypted, compressed, fragmented**, or stored in a form that does not allow for immediate reading. Data encryption is not relevant from a legal standpoint, as it constitutes merely a technical method of

data processing intended to restrict access. Consequently, the legal status of the data does not change simply because it is encrypted or temporarily rendered unusable by cybercriminals.

C. Programs

38 The clarification "including a program," intended by the drafters of the Convention, aims to remove any ambiguity regarding the inclusion of **programs** in the definition of Art. 1(b) CCC. This approach is entirely consistent for two reasons. From an IT perspective, a program is a set of instructions contained in source code, which itself consists of a multitude of characters—that is, data—that determine how the data provided to it is to be processed. From a systematic perspective, the inclusion of programs in the definition of computer data is consistent with the Convention drafters' clearly stated intention not to distinguish between different types of data.

D. Outlook

39 Although it was impossible, at the time the Convention was drafted, to foresee future developments in information technology, the choice of a **technologically neutral** definition has made it possible to include all new types of data that have emerged since 2001. This is particularly true of crypto-assets, data generated by connected devices, and *datasets*—that is, structured collections of data intended for training machine learning models.

E. Digression: The Distinction Between Subscriber Data, Traffic Data, and Content Data in Swiss Criminal Law

40 The rapid evolution of technology over the past thirty years has necessitated **significant legislative changes** to distinguish which types of data could be obtained and under what conditions. The first Act on the Surveillance of Postal and Telecommunications Correspondence (LSCPT) was adopted on October 6, 2000, and entered into force on January 1, 2002. It was completely revised in 2016 and subsequently underwent several partial revisions, including a major one in 2024.

41 The legislature considered that not all data were of equal importance. It proceeded from the premise that the greater the infringement on privacy—guaranteed by Art. 13 of the Constitution—the stricter the conditions under which

such data could be obtained would have to be. The law thus distinguishes between **three types of data**: subscriber data (*Bestandesdaten*), traffic data (*Randdaten*), and content data (*Inhaltsdaten*).

42 The Convention on Cybercrime makes this same distinction in Article 18.

1. Subscriber data

43 Subscriber data includes the **identification information of the subscriber** of a connection. This includes, in particular, the last name, first name, date of birth, address, and, if known, the user's occupation (Art. 21(1)(a) LSCPT), as well as addressing resources (Art. 21(1)(b) LSCPT) and types of services (Art. 21(1)(c) LSCPT) that were used.

44 This data corresponds to that listed in**Art. 18 § 3 CCC**, namely: the type of communication service used, the technical measures taken in this regard, and the service period (subpar. a); the subscriber's identity, postal or geographic address, and telephone number, as well as any other access number, and data concerning billing and payment, available on the basis of a contract or service agreement (subparagraph b); any other information regarding the location of the communications equipment, available on the basis of a contract or service agreement (subparagraph c) .

45 These are the **least sensitive data**. Obtaining them constitutes only a minimal intrusion into privacy. Under Swiss law, obtaining such data is therefore subject solely to the conditions of Art. 197(1) of the Swiss Criminal Procedure Code and does not require authorization from the Court for Coercive Measures.

2. Traffic data (or secondary data)

46 Traffic data consists of information indicating **with whom, when, for how long, and from where** the person under surveillance has communicated or is communicating, as well as the technical characteristics of the communication in question (Art. 8(b) of the Interception of Communications and Telecommunications Act).

47 In a landmark ruling, the Federal Supreme Court specifically held that **the history of IP addresses** of members who have logged into a social network constitutes traffic data and not subscriber data. This ruling, which has been

heavily criticized in legal scholarship, was recently upheld in an unpublished decision.

The Convention on Cybercrime defines them in Art. 1(d) CCC. They will be examined in detail in Chapter V below. 48

This **data** is **more sensitive** than subscriber data. The Swiss legislature has therefore decided to impose stricter requirements for obtaining it. Consequently, the conditions set forth in Art. 197, paras. 1 and 2, and Art. 273, para. 1, of the Swiss Criminal Procedure Code (CPP) must all be met cumulatively. Obtaining this data is therefore possible only when there are serious grounds for suspecting that a crime or misdemeanor has been committed. Mere assumptions or vague suspicions are not sufficient. Nor is it possible to obtain this data in cases involving a minor offense. In addition, the collection must be justified in light of the seriousness of the offense (principle of proportionality) and that the measures taken thus far as part of the investigation have been unsuccessful, or the investigations would have no chance of success or would be excessively difficult in the absence of surveillance (principle of subsidiarity). 49

Furthermore, obtaining this data is only possible with the**authorization** of the Court for Coercive Measures (Art. 274 CCP). 50

3. Content Data

Content data corresponds to the very **substance of communications** (Art. 8(a) LSCPT). This refers to the written or oral expression of human thought, in particular the text composed by the author of an email or message or the words spoken by a party during a telephone conversation. 51

Surveillance of content data is **the most intrusive form of surveillance** and constitutes the most serious infringement of the secrecy of telecommunications and privacy. It therefore goes without saying that the requirements established by the Swiss legislature are the strictest of the three types of data. 52

Content data is referred to in Art. 21 of the Swiss Civil Code (CCC). The drafters of the Convention also held the view that such data could not be obtained to prosecute just any offense. They therefore incorporated the **principle of proportionality** by stipulating that such data could be collected only to prosecute certain serious offenses that must be defined under domestic law. 53

54 The collection of content data is governed by **Art. 269 of the Swiss Criminal Procedure Code (CPP)**. It requires the existence of serious suspicion that a crime or misdemeanor has been committed, as exhaustively listed in Art. 269(2) of the CPP. In this case as well, mere assumptions or vague suspicions are not sufficient. The collection of such data must also be justified in light of the seriousness of the offense (principle of proportionality). It is therefore not sufficient that the offense being prosecuted appears on the list in Art. 269(2) of the Criminal Procedure Code; rather, the specific gravity of the offense in the particular case must also justify the surveillance measure. Finally, the measures taken thus far during the investigation must have been unsuccessful, or the investigation would have no chance of success or would be excessively difficult without surveillance (principle of subsidiarity).

55 As with traffic data, the collection of content data is possible only with the **authorization** of the Court for Coercive Measures (Art. 274 CPP).

IV. SERVICE PROVIDER (SUBPAR. C)

56 According to Art. 1, subpar. c, of the Swiss Civil Code (CCC), "*the term 'service provider' refers to any public or private entity that offers users of its services the ability to communicate via a computer system, and any other entity that processes or stores computer data for this communication service or its users*." This definition distinguishes between **two types** of providers: access providers and storage or content providers.

A. Access Providers

57 The service providers referred to in Art. 1(c)(1) CCC are access providers (*access provider*), that is, those who enable users to **connect to a network** and **communicate with one another** via a computer system.

58 These are primarily telecommunications operators (e.g., Swisscom, SFR, Deutsche Telekom, Vodafone, TIM) that enable individuals to connect to the Internet. In our view, this definition must be understood much more broadly and extended to include all **entities that provide access to a network** via a computer system. This includes private companies or public entities that provide users with Internet access points (e.g., railroads, hotels, municipalities, etc.), private companies or public entities that operate a private network and provide their users with access to that network, as well as individuals who

have an Internet access point or a home network—particularly in the form of a Wi-Fi hotspot—and who offer third parties the opportunity to connect to it.

This **broad interpretation** is confirmed by the drafters of the Convention, who emphasize in their Explanatory Report that it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, free of charge or for a fee. The closed group may consist of employees of a private company to whom services are provided via a corporate network. 59

In our view, the phrase "that offers users of its services the ability to communicate" encompasses not only public or private entities that provide network access, but also all those that **make communication physically possible**. The concept of "access provider" thus extends to all entities that make available infrastructure or a service enabling the transmission, routing, or forwarding of data across the network, provided that they offer a functional communication service to users. However, this does not apply to purely technical or industrial actors who limit themselves to manufacturing, supplying, or maintaining equipment without themselves offering a communication service. 60

From a purely functional perspective, the definition in Art. 1(c)(1) of the Swiss Civil Code (CCC) also covers certain categories of**network intermediaries** who, without providing traditional Internet access, play a decisive role in enabling effective communication via a computer system. This is particularly the case for providers of virtual private network (*VPN*) services, who provide their users with secure and anonymous access to resources available via the network, combining functions of routing, transmission, and encryption of communications. 61

From a functional perspective, Art. 1(c)(1) of the Swiss Civil Code (CCC) may also apply to **operators of infrastructure services** essential to Internet communication, such as providers of publicly accessible domain name system (DNS) resolution services or operators of Internet exchange points (*Internet Exchange Points* or IXPs), provided they offer a service that enables the routing or interconnection of communications between users or network providers. 62

B. Hosting and Content Providers

63 The **service providers** covered by Art. 1(c)(2) CCC are those that make storage space (*hosting providers*) or content for websites (*content providers*) available, either free of charge or for a fee.

64 **Storage providers** (*hosting providers*) are entities that offer Internet users servers that enable the storage or processing of data. They fall into **two categories**: those that store or process data on behalf of the entities mentioned in point (i) and those that store or process data on behalf of users of the services offered by the persons referred to in point (ii):

65 The first category includes hosting providers that process or store data from **access providers**. This includes, in particular, traffic data (see Section V below), data from the *Domain Name System* (DNS)—which associates domain names with the IP addresses of the servers on which they are hosted—and data concerning the various servers through which emails pass.

66 The second category concerns providers that store or process data belonging to the **users** of internet service providers. This includes, in particular, entities that host websites, provide space for deploying virtual computing systems, or offer environments in which data can be backed up, managed, or processed remotely (*cloud computing*).

67 In the context of *cloud computing*, the classification as a service provider within the meaning of Art. 1(c)(2) of the Swiss Civil Code (CCC) applies equally to the various commonly distinguished service models, namely Infrastructure as a Service (*IaaS*), Platform as a Service (*PaaS*), and Software as a Service (*Software as a Service* or SaaS). Regardless of the form adopted, these models all involve the storage, processing, or provision of computer data on behalf of third parties, which justifies their inclusion in the definition of service providers covered by Art. 1(c)(2) of the Swiss Code of Obligations (CCC).

68 Service providers also include entities that operate **content delivery networks**

(*Content Delivery Networks* or CDN). These entities provide caching, temporary storage, and optimized distribution of data through geographically distributed servers.

However, the definition in Art. 1(c)(2) of the Swiss Civil Code (CCC) is not intended to apply to a mere content provider (e.g., a person who enters into a contract with a hosting provider to host their website) if that provider does not also offer communication services or other data processing services. Conversely, in our view, websites that, in addition to making content available, provide **communication services**—such as websites that offer email accounts, instant messaging, or discussion forums—fall within the scope of the definition in Art. 1(c)(2) of the Swiss Civil Code (CCC). The same applies to websites that offer **data processing services**, including data encryption, text translation, financial data analysis, and the automated collection of unstructured data and its conversion into organized data (*web scraping*). 69

This analysis also applies to **online platforms** and **social networks** which, beyond the distribution of content, offer structured features for communication and interaction among users. These services generally involve the creation of accounts, the exchange of messages, the publication of content, as well as the automated processing of data for the purposes of classification, targeted advertising, or moderation. 70

C. Outlook

Finally, like the definition adopted for computer data, the definition of "service provider" is designed to be technology-neutral. This approach has allowed it to incorporate the **new types of services** that have emerged since 2001, particularly entities that offer services based on artificial intelligence to process or generate data. It should be noted, however, that it is not artificial intelligence per se that is covered by the definition, but rather the functions of storing, processing, or communicating computer data that it enables. 71

V. TRAFFIC DATA (LETTER D)

The final definition provided by the Convention appears in Art. 1, Letter d of the CCC, according to which "traffic data" *"means any data relating to a communication passing through a computer system, produced by that system as part of the communication chain, indicating the origin, destination, route, time, the date, the size and duration of the communication, or the type of underlying service"*. This data has a **special legal status**, insofar as it can serve as evidence—or even proof—in criminal investigations. It is generated by the various computer systems involved in the communication chain in order to 72

route the communication from its point of origin to its destination. It is therefore an auxiliary element of the communication itself itself.

73 Traffic data is necessary to identify the **source of the communication**; it serves as a starting point for gathering further evidence or as a constituent element of the evidence of the offense. However, due to the enormous volume of communications exchanged daily, the data relating to these communications has a very limited retention period. It is therefore essential to act swiftly to trace the route of the suspicious communication before the traces disappear. Given the often lengthy duration of ordinary international mutual legal assistance procedures in criminal matters, the Convention provides for the option to use the expedited disclosure procedure set forth in Art. 17 CCC. This procedure makes it possible to obtain information on the communication's route without delay and to gather other evidence before it is deleted, or to identify a suspect. This expedited and less formal procedure remains consistent with the principle of proportionality, insofar as the collection of traffic data constitutes a significantly lesser infringement of personality rights than the collection of content-related data, since it does not reveal the content of the communication, but only its path.

74 Art. 1(d) of the Swiss Civil Code (CCC) sets forth an **exhaustive** list of categories of traffic data that are subject to special provisions under the Convention, namely: the origin, destination, route, time, date, size, and duration of the communication, or the type of underlying service.

75 The **origin** and the **destination** correspond to the points in the network from which a communication is sent and received. Depending on the mode of communication used, they are identified by telephone numbers or, more generally, by IP addresses assigned to the relevant computer systems at a given time. These identifiers do not necessarily allow for the direct identification of an end user, particularly in the case of dynamic, shared, or masked IP addresses resulting from processes such as network address translation (NAT), relay services (e.g., the TOR network), or virtual private networks (VPN). They are of particular importance for criminal investigations, as they make it possible to identify the computer system or network access point at the origin or destination of the communication.

76 The **path** describes the route taken by the communication through the various relay points in the network, in particular routers, intermediate servers, or

other transit infrastructure. It corresponds to the sequence of computer systems through which data is routed from its point of origin to its destination. In practice, this route can be partially or fully reconstructed from the data generated by these various systems, subject to technical limitations related, in particular, to the network architecture, the use of intermediary services, or the encryption of communications.

The **time** and **date** are expressed in Coordinated Universal Time (UTC). This information is essential when dealing with dynamic IP addresses. Since these addresses are constantly reassigned based on user needs, it is essential to have this information in order to ask the internet service provider to which computer system it assigned an IP address at a given time. This information must be obtained as quickly as possible, since, depending on the country, it is retained for only six to twenty-four months at most. Once this period has elapsed, the data is destroyed, and it becomes impossible to identify the user to whom an IP address was assigned. This difficulty does not exist, however, with static IP addresses, since they are permanently assigned to the same users. 77

The **size** of the communication is expressed in bits or bytes and corresponds to the volume of data exchanged. It can serve as an indicator for investigators regarding the type of data exchanged, insofar as certain types of content—such as images, audio recordings, or audiovisual content—generally generate larger volumes of data than simple text messages. However, this indicator must be interpreted with caution, given contemporary techniques for compressing, fragmenting, and encrypting data streams. 78

The **duration** of the communication is measured in hours, minutes, and seconds. It corresponds to the length of time during which a communication was established or a data exchange took place between the computer systems involved. This information can provide contextual details useful to the investigation, particularly for distinguishing one-time communications from prolonged or repeated connections, without, however, revealing the content of the exchanges that occurred during that period. 79

Finally, the **type of underlying service** refers to the communication method or functional category of service used in the context of the data exchange, such as email, instant messaging services, viewing online audiovisual content, or downloading data. This is a general classification of the service used, which 80

can be difficult to determine precisely when multiple services are combined within a single communication stream or when data is encapsulated or encrypted.

BIBLIOGRAPHY

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

TRAVAUX LÉGISLATIFS

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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 2 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 2 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 2 CCC N. XXX.

Chapter II: Measures to be taken at the national level

Section 1: Substantive criminal law

Title 1: Offences against the confidentiality, integrity and availability of computer data and systems

Art. 2 Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining

computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

CONTENT

I. General 30
II. Legally protected property 30
III. Fundamental elements 31
A. A computer system 31
B. Access to the computer system 31
C. Unlawfulness 33
D. Intention 34
IV. Optional additional elements 35
A. Access in violation of security measures 35
B. The purpose of obtaining computer data or another special purpose 36
C. A computer system connected to another computer system 37
V. Comparison with Swiss law 37
Bibliography 39
Materials 39

I. GENERAL

1 Illegal access to a computer system is the basic offence in the field of cybercrime. It is often the prerequisite criminal conduct for the commission of another computer-related offence, such as data interference (art. 4 CCC), system interference (art. 5 CCC), computer forgery (art. 7 CCC) or computer fraud (art. 8 CCC). However, some cybercriminals simply gain unauthorized access to a computer system, out of bravado or for the sheer technical challenge it represents, without committing any subsequent offence. It is therefore justified to criminalize this behavior in its own right, rather than having it absorbed into the offences punishable under the following articles. Thus, the perpetrator is guilty of illegal access by the mere fact of gaining access to a computer system. It is not necessary for him to steal or modify data in the computer system.

2 Some might see hacking as a relatively harmless, playful activity enjoyed by a few geeks in search of new challenges. The reality, however, is quite different. Hacking is far more widespread than one might think at first glance, and its perpetrators pursue far less honorable aims than mere entertainment.

3 Naturally, strong security measures are the most effective way of protecting a computer system against unauthorized access. Given the threat to the security of computer systems and data that hacking represents, technical measures must be accompanied by legislative measures designed to dissuade cybercriminals from taking action, or to punish them if they commit malicious acts. In this way, the interests of organizations and individuals in being able to run, operate and control their IT systems without disruption or hindrance of any kind are best protected.

II. LEGALLY PROTECTED PROPERTY

4 Art. 2 CCC protects the inviolability of computer systems. This protection under criminal law is necessary for at least two reasons.

5 On the one hand, illegal access to a computer system can result in substantial repair costs for the rightful owner. The perpetrators often modify data in order to gain access to the system. What's more, victims are often unaware of the intrusion until some time after it has taken place. It is therefore particular-

ly difficult to trace what has been modified by the perpetrators, and what new data has been generated by the computer system as a result. Once identified, these data must be restored to their original state. These operations can be very time-consuming and costly.

On the other hand, illegal access enables authors to consult information to which they should not have access (e.g. confidential reports, trade secrets, customer lists, accounting documents, credit card numbers, personal data, etc.). This information can then be resold on the black market, which can cause far greater damage to the rightful owner than simply restoring the system's protection. 6

III. FUNDAMENTAL ELEMENTS

A. A computer system

According to art. 1 let. a CCC, "the term 'computer system' means any isolated device or set of interconnected or related devices, which performs or of which one or more elements perform, in execution of a program, automated data processing". The notion of computer system thus includes all hardwares (motherboard, processor, hard disk, screen, keyboard, printer, etc.) and softwares (BIOS, operating system, software, updates, etc.), as well as the devices that connect these different elements to each other (cables, router, wifi terminal, etc.). 7

For further details on this concept, please refer to art. 1 CCC above. 8

B. Access to the computer system

One might be tempted to compare illegal access to a computer system with the offence of trespass. Access to the computer system would thus be the digital equivalent of breaking into the dwelling. The reassuring thing about this analogy is that it's easy to visualize the situation intellectually. However, the virtual world is more complex than that, and the contours of legal notions are necessarily more blurred. 9

An analogy with the real world is complicated. If one were to be made, however, access to a computer system could be compared to entering a medieval castle. Access to the castle is limited by a surrounding wall and moat. The main gate is usually guarded by guards. They check that those entering the 10

fortress are authorized to do so. Once inside, individuals can access certain parts of the castle and not others, depending on their rank. Rank is defined by the lord to whom the castle belongs. Each part of the castle contains objects that can be viewed, touched, modified or even destroyed. For these items too, the castle lord determines who can do what with which object. The lord is the only one with access to every room in the castle, and the only one who can act as he or she sees fit with every object in the castle.

11 A computer system operates in a similar way to a castle. To gain access to the computer system, the user generally has to enter a login and password. Once logged in, the user can access all or part of the computer system according to his or her accreditation level, which is determined by the computer system administrator. This accreditation level also determines what the user can and cannot do in the parts of the computer system to which he or she has access, i.e. only view the title of documents contained in a folder, open them to read, edit or delete them. The administrator is the only person with access to the entire computer system, and with the rights to perform any action he or she wishes with the data contained therein.

12 The analogy with the real world ends there, however. Indeed, the notion of "access" in the virtual world cannot be compared to that of "penetration" in the real world. In computing, the notion of "access" means that the author succeeds in establishing a connection with all or part of a computer system. Strictly speaking, therefore, there is no physical movement of the author from one place to another.

13 In the simple form of the offence, the means used by the perpetrator to connect to the computer system is irrelevant. The perpetrator may therefore establish a connection by means of local or remote access. If the perpetrator establishes a local connection with a computer system to which he or she has physical access, this will be done using a keyboard - hardware or virtual - and a mouse, or even simply with the fingers for tablets and smartphones. They may also use a terminal to connect to a central computer system. If, on the other hand, the author decides to establish a remote connection, he or she can use any telecoms network. The type of network (local, public, private, etc.) and the type of connection (wired or wireless) are of no importance.

14 Nor is the extent of access decisive in determining whether an offence has been committed. Access may be total, in which case it extends to the entire

computer system. It may also be only partial. In this case, it concerns only part of the computer system. This is the case, for example, when the perpetrator only accesses a user's session or part of the data stored on a server.

The offence is committed as soon as the connection to the computer system is established. There is then nothing to prevent the perpetrator from acquiring knowledge of the data contained in the computer system. However, it is not necessary for the perpetrator to become aware of the data for the offence to have been committed. In practice, however, these two events usually coincide, since at the moment when access is established, the data is displayed on the screen. 15

The notion of access as defined in art. 2 CCC must be clearly distinguished from data interference as defined in art. 4 CCC. To commit the offence, it is sufficient for the perpetrator to gain access to a computer system. Even if, in practice, the establishment of illegal access regularly results in the modification of data, such deterioration is not necessary for the commission of the offence. 16

Finally, only the establishment of illegal access is punishable. Maintaining lawful access after the owner of the computer system has informed the user that he or she is no longer authorized to access it is not punishable. A case in point is the employee who, in the course of his professional activity, uses his private computer to connect to the company network and who, once dismissed, continues to consult company files. However, the absence of punishability lasts only as long as the connection. If he interrupts the connection and establishes a new one, he is guilty of the offence. In our opinion, this absence of punishability is clearly a loophole that has been misleadingly described, as the Parties probably simply did not envisage this possibility when drafting the text. 17

C. Unlawfulness

To be punishable, the perpetrator must have acted without right. This involves first determining whether the computer system is public - i.e. open to all - or whether access to it is restricted, or a combination of both. If the computer system is public, access to it cannot be unlawful, and any infringement is excluded. On the other hand, if access to all or part of the computer system is restricted, unauthorized access is punishable. 18

19 It is the owner of the computer system who determines who is authorized to access which part of the system. This means that not only those who have not been authorized to access the computer system are liable to punishment, but also those who have been authorized to access one part of the computer system, but who access another part of the computer system to which they have not been granted access. On the other hand, persons who have been granted access to the computer system by its rightful owner, and who comply with the limits of this access, are not liable to punishment.

20 The rightful owner of a computer system is not always its administrator. This is particularly true of medium-sized and large computer systems. In such cases, the management of the IT system is delegated by its owner to a third-party administrator. This administrator may be either an individual or a legal entity. In both cases, the owner of the IT system authorizes the administrator to access it in order to carry out his or her mission. In other words, the administrator does not have unauthorized access to the computer system, as long as this is for the purpose of fulfilling his or her mission. On the other hand, access is unauthorized when it is for another purpose, such as consulting private or confidential information not intended for the administrator.

21 When the management of an IT system is delegated to a company, all the natural persons in charge of this task within the company are authorized to access it. However, this is not the case for individuals within the legal entity to whom this task has not been assigned. If these people do access the computer system, they do so without right, as they are not doing so to carry out the task entrusted to the legal entity.

22 A person specifically mandated to test the security of a computer system, who manages to gain access to the system by circumventing the protection measures in place, is not acting unlawfully, as he has been authorized to do so by his beneficiary.

D. Intention

23 Illegal access is intentional. Intention must cover all the objective elements of the infringement. The perpetrator must therefore be aware that he or she is accessing a computer system without right, and have the will to do so. Any fraudulent intent is sufficient. If the perpetrator suspects that he is accessing all or part of a computer system to which he should not have access, but es-

tablishes a connection anyway, he is guilty of illegal access. On the other hand, if the perpetrator makes a handling error and establishes an unauthorized connection in spite of himself, intent is lacking and the offence is not committed.

The law punishes only the establishment of illegal access, and not the fact of maintaining access against the will of the rightful owner. Consequently, anyone who inadvertently accesses a computer system but, once connected, explores its contents, is not punishable. 24

If the author mistakenly believes that the computer system he is accessing is public, or if he mistakenly believes that he is entitled to access it for some other reason, he has committed an error of fact. 25

IV. OPTIONAL ADDITIONAL ELEMENTS

When the Convention on Cybercrime was being drafted, a majority of Parties wanted to criminalize outright piracy. Others, on the other hand, were opposed to a general criminalization of hacking, on the grounds that simple intrusion does not necessarily cause damage and that, in some cases, acts of hacking even make it possible to discover and close security loopholes. To take account of these considerations, and given that the national legislation of many countries already contained provisions that punished hacking in various forms, Parties were given the option of limiting the punishability of illegal access by requiring the fulfilment of one or more additional constituent elements. 26

A. Access in violation of security measures

The Convention on Cybercrime first gives Parties the option of punishing illegal access only when it is committed in violation of security measures. The Czech Republic, Finland, Germany, Japan, Lithuania, Peru, the Slovak Republic and Switzerland have made use of this option. 27

This additional requirement means that the computer system must be protected against unauthorized access. In other words, if the author gains unauthorized access to an unprotected computer system, he is not punishable. 28

The notion of security measures must be understood broadly. It encompasses both physical and virtual security measures. With regard to physical security 29

measures, the computer system may, for example, be located in a locked room that can only be accessed with a key, magnetic badge, fingerprint, retinal scan or voice print. Virtual security measures may include firewall protection, PIN codes, passwords, double or even triple authentication.

30 If the perpetrator is unable to bypass the security measures, or if he spontaneously decides to end his activity before having bypassed them, only one attempt is possible. This poses a problem, however, since art. 11 § 2 CCC does not require Parties to punish attempted illegal access. Each State is therefore free to deal with this aspect as it sees fit, with the result that such conduct may not be punishable at all, depending on the national legislation of the States Parties.

B. The purpose of obtaining computer data or another special purpose

31 Another possibility open to Parties is to require that the perpetrator acted with a special purpose. Several States have made use of this possibility.

32 The United States of America has decided to require that the perpetrator has acted in order to obtain data. Although this possibility has been given to the Parties, its use is regrettable, as it empties the norm of much of its substance. In fact, this provision was specifically designed to punish the acts of hackers who gain access to computer systems out of bravado, but are not interested in the data they contain. Requiring this specific special purpose therefore seems contrary to the spirit of the norm.

33 Belgium, for its part, has stated that illegal access is criminalized only when committed with fraudulent intent or malicious intent. Fraudulent intent seems to refer to the desire to obtain an undue advantage for oneself or for others. As for malice aforethought, it probably refers to the intention to cause harm to others in any form whatsoever.

34 The Principality of Andorra and the Slovak Republic have decided to prosecute illegal access only if it is committed with the aim of obtaining data without right, of damaging it (in the case of the Principality of Andorra only) or for some other criminal purpose. This wording is intended to prevent perpetrators from escaping conviction on the grounds that they were pursuing a purpose other than obtaining or damaging data. In our opinion, however, it must be interpreted in the light of the special purposes listed in art. 2 CCC, and is

similar both in terms of the purpose pursued by the perpetrator and its criminal intensity. On January 1, 2021, the Slovak Penal Code was amended and the Reserve of the Slovak Republic adapted. Section 247 has been revised. In its simple form, this provision no longer requires any special purpose (§ 247 par. 1). On the other hand, § 247 par. 2 provides for a qualified form when the perpetrator causes considerable harm.

Finally, Canada has indicated that it will only prosecute illegal access if it is committed with criminal intent. This last notion is particularly imprecise, and consequently creates considerable legal uncertainty. What's more, it seems to overlap with the notion of intent. In our view, it should therefore be interpreted restrictively. 35

Chile initially entered a reservation identical to that of Canada. However, it amended its legislation in 2022. In its new version, acceso ilícito is punishable when committed intentionally. Special intent is no longer required. However, when illegal access is committed with the aim of obtaining or using data contained in the computer system, the penalty is increased. 36

C. A computer system connected to another computer system

Finally, the Convention on Cybercrime allows Parties to limit the punishability of illegal access to connections established without right with a computer system via another computer system. By making use of this possibility, Parties can exclude cases in which the perpetrator physically accesses the computer system he is targeting, without passing through a network. 37

The only States to have made use of this possibility are the Slovak Republic and Japan. The Slovak Penal Code has since been amended. The new wording of § 247, which entered into force on January 1, 2021, no longer provides for this requirement in its current version, so the Slovak Republic's reservation has been adapted. 38

V. COMPARISON WITH SWISS LAW

Under Swiss law, hacking is punishable under art. 143bis of the Swiss Criminal Code. This provision punishes unauthorized access to another person's computer system, specially protected against access, by means of a data transmission device. However, this standard does not meet the requirements of art. 2 CCC in three respects. 39

40 Firstly, the convention makes no distinction between computer systems. It protects the integrity of all computer systems, irrespective of their affiliation. Art. 143bis para. 1 of the Criminal Code, on the other hand, only criminalizes unauthorized access to a computer system "belonging to another person". Given that this provision is to be found in Title 2 of the Criminal Code, i.e. offences against property, this wording must be interpreted with regard to real rights. The computer system must therefore belong to a person other than the author. If the author is the owner or co-owner of the computer system, this constitutive element is not fulfilled, since it does not belong to another person. Thus, if several sessions have been opened in the same computer system, the author, (co-)owner of the computer system, who accesses a session other than his own, is not punishable. The majority of legal writers, on the other hand, take the view that "belonging to others" means that a person other than the author is authorized to access and dispose of the computer system or a computer subsystem. Such an interpretation would, however, make the notion of "belonging to another person" redundant with the constitutive element of unlawful access. The reason why the legislator has mentioned these two elements separately is that they are two notions which must be analyzed independently of each other. To be consistent with the Convention, the term "autrui" in art. 143bis para. 1 of the Criminal Code should therefore be deleted.

41 Art. 143bis para. 1 PC requires the perpetrator to have accessed the computer system by means of a data transmission device. This means, for example, that a perpetrator who takes advantage of his victim's absence to enter his office and log on directly to his computer is not guilty of undue access to a computer system, since he is not using a data transmission device. Art. 2 § 2 CCC allows Parties to limit criminal prosecution to unlawful access committed by means of a computer system connected to another computer system. However, Switzerland has not declared that it will avail itself of this possibility. Consequently, the constituent element of access by means of a data transmission device should be deleted.

42 Finally, art. 143bis of the Swiss Criminal Code establishes an offence prosecuted only on complaint. However, when an offence is only prosecuted on the basis of a complaint, a criminal authority cannot take the matter into its own hands. Since there is a conflict of doctrine as to whether a complaint lodged in the requesting state is sufficient to implement international cooperation, it would be prudent to prosecute undue access to a computer system ex officio.

In view of the foregoing, it is clear that Swiss law does not comply with art. 2 CCC. Art. 143bis of the Swiss Criminal Code should therefore be amended. 43

The technical IT concepts contained in this contribution were drafted with the help of Mr. Yannick Jacquey, ICT Manager with a federal diploma. Our warmest thanks to him.

BIBLIOGRAPHY

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 / Crameri 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

MATERIALS

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

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 3 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 3 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 3 CCC N. XXX.

Art. 3 Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

CONTENT

I. General 43
II. Legally protected property 43
III. Basic elements 43
A. Computer data 43
B. Non-public transmission 44
1. The notion of transmission 44
2. Non-public nature 45
C. The special case of electromagnetic emissions 45
D. Interception by technical means 47
E. Unlawfulness 48
F. Intention 49
IV. Optional additional constituent elements 49
A. The purpose of obtaining computer data or another special purpose 49
B. A computer system connected to another computer system. 50
V. Comparison with Swiss law 50
Bibliography 51
Materials 52

I. GENERAL

To guarantee complete legal protection, unlawful access had to be supplemented by unlawful interception. As we have seen above (cf. Art. 2 N. 9ss), unlawful access punishes the unlawful intrusion into a computer system and the consultation by unauthorized persons of the data stored therein. Illegal interception, on the other hand, sanctions the violation of the confidentiality of data circulating within the computer system, as well as data exchanged between the computer system and the outside world. 1

II. LEGALLY PROTECTED PROPERTY

This provision protects the right to confidentiality of transmitted data. The offence represents the same violation of the right to secrecy of communications as the conventional tapping and recording of telephone conversations between individuals. Art. 3 CCC takes up the guarantee of the right to respect for correspondence contained in art. 8 ECHR and applies it to all forms of electronic data transfer, whether by telephone, fax, e-mail or file. 2

III. BASIC ELEMENTS

A. Computer data

According to art. 1 let. b CCC, "the term 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable for causing a computer system to perform a function". The notion of computer data is therefore very broad, encompassing in particular all letters, symbols or programming codes that can be entered, processed and stored by a computer system. 3

For further details on this notion, please refer to what has been written on art. 1 CCC. 4

B. Non-public transmission

1. The notion of transmission

5 Contrary to what the etymology of the term "transmission" might suggest, the notion of transmission in art. 3 in initio CCC does not refer solely to remote exchanges between two devices. As the prepositions "to", "from" or "within" a computer system suggest, it concerns all data in circulation. The only data not covered by this concept is that which is permanently stored on a medium, such as a hard disk, USB stick or DVD.

6 The transmission of data "inside" a computer system covers data circulating in and between the motherboard, processor, graphics card, computer screen or printer. It even extends to data stored in the computer system's random access memory, since such data is not permanently stored in this memory, but is only held there for a few moments before continuing to circulate within the computer system.

7 Data transmissions "to" or "from" a computer system presuppose that the receiver or sender of the data is a computer system, while the other may be a human or a computer system.

8 The transmission of data from a human being "to" a computer system involves the human being entering data into the computer system, for example using a keyboard, mouse or joystick. Conversely, the transmission of data to a human being "from" the computer system refers to the return of data from the computer system to the human being, by displaying the data on a screen or printing a document on a printer.

9 Finally, when data transmission takes place between two computer systems, it takes place both "to" and "from" a computer system. This is the case, for example, when data is exchanged between a computer and a server, between two computers, or between a computer and a smartphone. It doesn't matter whether the two computer systems belong to the same person or to different people. Nor does it matter how the data is transmitted. Data can be exchanged via a wired or wireless connection (Wifi, NFC, Bluetooth, radio wave, etc.).

10 The preceding elements show that the notion of transmission is very broad. In order to restrict the scope of this provision, art. 3 in fine CCC allows the Par-

ties to limit criminal prosecution to the illegal interception of data transmitted between two remotely connected computer systems.

2. Non-public nature

Art. 3 CCC concerns only non-public transmissions. Non-public character relates to the transmission and not to the data transmitted. It is therefore irrelevant whether the data transmitted is public or private. Only the nature of the transmission is decisive. 11

In our opinion, a transmission is non-public when it is limited to a certain number of people or to specific individuals. This is the case, for example, of the transmission of a videoconference presentation that can only be followed by a limited number of participants, or of films made available only to subscribers by a streaming company. 12

However, the notion of non-public transmission does not mean that the transmission must take place over a network that is not public. Transmission can take place using a public network; it simply has to be restricted to a specific number of people. 13

To restrict transmission to a specific number of people, technical measures must necessarily be put in place. However, these security measures need not be particularly advanced. A system that checks whether the person wishing to access the transmission is one of the authorized persons is sufficient. This could involve following a link sent by e-mail, entering a code supplied in advance, or identifying oneself by means of a login and password. 14

C. The special case of electromagnetic emissions

When the Convention on Cybercrime was drawn up between April 1997 and December 2000, the experts wanted to anticipate technological developments. Illegal interception was therefore not limited to data transmission alone, but was extended to electromagnetic emissions. 15

To understand how the interception of electromagnetic emissions works, we need to remember that computer data correspond in binary language to a succession of "0s" and "1s". This is the form in which computer systems process data. From a microtechnical point of view, this means generating different electrical impulses for a "0" and a "1". This is what transistors are for. Schemat- 16

ically, computer systems are made up of a multitude of transistors. These transistors vary the voltage across the system's electronic components from low to high, depending on whether the bit being processed is a "0" or a "1". These innumerable voltage variations create an electromagnetic field that propagates around the computer system. This enables a person in the vicinity, equipped with a suitable device, to pick up this flux, convert it back into "0s" and "1s" and thus reconstitute the computer data processed by the computer system.

17 For the experts, the legal arsenal seemed incomplete if it were limited to punishing the interception of data transmitted to, from or within a computer system, without simultaneously punishing the capture of electromagnetic waves emitted by a computer system. In the real world, this would have been tantamount to punishing the bugging of a person's apartment, while leaving the eavesdropping of that person's conversations from behind the apartment's front door unpunished.

18 In particular, it should be remembered that when the text of the convention was being drafted, fax machines were in widespread use. This device sent uncoded data, at a frequency and with an electrical intensity that made it fairly easy to pick them up and then reconstitute them in a comprehensible language. Experts certainly identified this as a security flaw that could be exploited by cybercriminals, which led them to include the capture of electromagnetic waves in the list of punishable behaviors.

19 Over the years, faxing has almost completely disappeared. Today, the capture of electromagnetic waves has become very marginal, if not non-existent, due to the technical difficulties involved in capturing these signals. The electrical cables used in today's information technology are much more insulated than in the late 90s, and the electrical impulses are much weaker. At the same time, the amount of data exchanged every second has exploded. As a result, it is now virtually impossible to capture magnetic waves from a single source and reconstruct them into intelligible data.

20 When the text of the convention was drawn up, however, the experts could not anticipate the direction in which the technology would evolve. This is why this behavior - even if it is now anecdotal - is included in the list of offenses punishable under art. 3 CCC.

D. Interception by technical means

Art. 3 CCC applies only to data interception by technical means. The physical removal of data, such as the theft of a USB stick sent by post, or the theft of a laptop turned on and unlocked in a public place, are therefore not punishable under this provision. 21

The interception referred to in art. 3 CCC can be either direct or indirect. The perpetrator intercepts data directly when accessing the computer system itself. The simplest form is the installation of a Trojan horse in the computer system, enabling the perpetrator to gain access. The perpetrator can also use a backdoor or exploit a security flaw. All these techniques enable the perpetrator to gain knowledge of the data circulating in the computer system in real time. 22

Interception is said to be indirect when the perpetrator intercepts the flow of data exchanged between two devices. This is the case, for example, of capturing the data flow between a device and a Wifi terminal to which it is connected. Within a local area network (LAN), the perpetrator can also usurp the MAC address of a computer system at the time of broadcasting, in order to have data packets sent to the system whose address has been usurped. Another technique is port mirroring. Initially, the aim of this system is to control the data exchanged within a network. To achieve this, a copy of all data passing through a network switch is sent to a computer control system. By taking control of the network switch, however, the perpetrator can redirect the copied data to his own computer system, enabling him to gain knowledge of all data exchanged on the network. 23

The notion of "technical means" used by the parties is very broad and imprecise. Nor is it accompanied by an exemplary list. This choice is undoubtedly intended to enable the standard to adapt more easily to technological innovations. In any case, the devices concerned are those which enable the content of communications to be listened in on, controlled or monitored. These include technical devices connected to transmission lines, as well as devices for collecting and recording wireless communications. However, the technical means referred to in art. 3 CCC are not limited to hardwares. Software, passwords and other codes are also included. 24

E. Unlawfulness

25 To be punishable, the author must have acted without right. It is the rightful owner of the data who determines who is authorized to access it. All persons who have not been authorized to consult the data are therefore liable to prosecution. On the other hand, persons who have been authorized to access the data by the rightful owner, or who are authorized to do so by law or contract, are not liable to punishment.

26 National laws contain exceptions to the guarantee of data confidentiality. In particular, they allow intelligence services to access data not intended for them. They also enable prosecuting authorities to monitor data flows in real time as part of a criminal investigation. Such interceptions are not illegal as long as they are carried out in strict compliance with the legal provisions in force. However, surveillance may only be carried out in serious cases, and must be subject to subsequent judicial review.

27 The interception of data is also not considered unlawful where it is contractually authorized. This is particularly the case where the computer system administrator is responsible for maintenance. In this case, he is not punishable if he intercepts the data he needs to carry out his work, as he has been authorized to do so by the rightful owner. Similarly, the person in charge of monitoring a network is not punishable if he or she intercepts data obtained through proper use, such as port mirroring. On the other hand, when such persons take advantage of the technical possibilities available to them to intercept data which is not necessary for the performance of their work, they are acting unlawfully.

28 In the context of employment relationships, the lawful interception of data is conceivable, but under restrictive conditions. Generally speaking, the European Court of Human Rights has held that employees' private communications are protected by art. 8 ECHR. Employer surveillance is therefore only conceivable if the employee has been informed of the surveillance of his communications, the nature and extent of such surveillance, and the degree of intrusion into his private life and correspondence. If the employer complies with these conditions, the interception of employee data is lawful.

29 Originally, art. 3 CCC was not intended to penalize common commercial practices aimed at obtaining information about users. Since the entry into force of the Convention on Cybercrime, commercial practices have evolved

considerably, and the information that commercial enterprises seek to obtain in order to target their advertising is increasingly important. As a result, national legislation has significantly strengthened data and consumer protection. As a result, websites are frequently required to obtain the consent of Internet users before collecting data about them, notably through the use of "cookies". Without the consent of the rightful owner, the collection of such data could constitute illegal interception.

F. Intention

Unlawful interception is intentional. Intention must relate to all the objective elements of the offence. The perpetrator must therefore be aware that he is obtaining data improperly and have the will to do so. Any fraudulent intent is sufficient. In its simple form, the aim pursued by the perpetrator is irrelevant. 30

IV. OPTIONAL ADDITIONAL CONSTITUENT ELEMENTS

Art. 3 CCC allows Parties to restrict punishability to particular acts by adding one or two of the constituent elements listed at the end of this provision. 31

Depending on how illegal interception is transcribed into national law, this offence may be closely linked to illegal access (art. 2 CCC). In view of the fact that some States have chosen to limit the repression of illegal access to cases committed with a specific purpose or by means of a computer system connected to another computer system, it was necessary to allow these States to restrict illegal interception to these same cases. 32

A. The purpose of obtaining computer data or another special purpose

The first possibility open to Parties is to require that the perpetrator acted with a special purpose. Several States have availed themselves of this possibility. 33

Canada, Japan and Peru have indicated that they would only prosecute illegal interception if committed with criminal intent. The latter notion is particularly imprecise, and consequently creates considerable legal uncertainty. Moreover, it seems to overlap with the notion of intent. In our view, it should therefore be interpreted restrictively. 34

35 Chile initially entered a reservation identical to that of Canada, Japan and Peru. However, it amended its legislation in 2022. In its new version, interceptación ilícita no longer requires a special purpose.

36 Switzerland, for its part, has declared that it will only prosecute illegal interception if the perpetrator has acted with the intention of illegitimate enrichment.

37 The Principality of Andorra, Belgium, the United States of America and the Slovak Republic, while declaring that they would only prosecute unlawful access if the perpetrator had acted with a special purpose, have waived this requirement for unlawful interception.

B. A computer system connected to another computer system.

38 The Convention on Cybercrime also allows Parties to restrict the punishability of unlawful interception solely to data transmitted between two connected computer systems. The only States to have made use of this possibility are Japan and Peru.

39 In this case too, it is surprising to note that the Slovak Republic has refrained from making use of this possibility, even though it had expressly stated that it would only prosecute illegal access if committed by means of a computer system connected to another computer system.

V. COMPARISON WITH SWISS LAW

40 In its Message on the approval and implementation of the Council of Europe's Convention on Cybercrime, the Federal Council acknowledged that "Swiss criminal law does not have regulations corresponding to Art. 3 of the Convention, but several criminal norms provide partial protection". In his view, this was a combination of arts. 143, 143bis and 321ter of the Swiss Criminal Code. In reality, this is absolutely not the case.

41 Art. 143bis of the Swiss Criminal Code only punishes intrusion into a computer system, not the interception of data.

42 As for art. 321ter of the Swiss Penal Code, it punishes a crime in its own right, since the offence can only be committed by an employee of a company providing a postal or telecommunications service.

As for art. 143 of the Swiss Criminal Code, this is the provision that most closely resembles art. 3 of the CCC. To meet the requirements of the Convention, however, this provision would have to be amended in four respects. 43

Firstly, the legal assets protected by the two standards are different. Art. 3 CCC protects the confidentiality of transmitted data, whereas art. 143 PC protects "the right of the legitimate recipient of the data to dispose of it freely and in accordance with his will". The legal asset protected by art. 143 of the Swiss Criminal Code should therefore be adapted. 44

Secondly, art. 3 CCC penalizes the interception of non-public transmissions, regardless of whether the data transmitted is public or not. However, art. 143 of the Swiss Criminal Code only punishes the theft of data specially protected against access. The theft of public data transmitted in a non-public manner therefore does not fall within the scope of Art. 143 of the Swiss Criminal Code. In practice, however, this is the most common case, as electronically transmitted data are generally not specially protected against access. 45

Secondly, art. 143 of the Swiss Criminal Code only protects a right of disposal over data. Computer data does not always have intrinsic value. To require a purpose of unlawful enrichment therefore amounts to excluding criminal protection in all cases where the perpetrator subtracts data of no value. In view of the legally protected asset, this constitutive element should be removed. 46

Finally, art. 3 CCC is not limited to non-public transmissions, but also includes electromagnetic emissions. However, these are not protected by art. 143 of the Criminal Code. They should therefore be added. 47

For all these reasons, it has to be said that Swiss law does not comply with art. 3 CCC and should therefore be adapted. 48

The technical IT concepts contained in this contribution were drafted with the help of Mr. Yannick Jacquey, ICT Manager with a federal diploma. Our warmest thanks to him.

BIBLIOGRAPHY

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 / Crameri 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

MATERIALS

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

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 4 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 4 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 4 CCC N. XXX.

Art. 4 Data interference

[1] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

[2] A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

CONTENT

I. General information 55
II. Legally protected property 55
III. Basic constituent elements 55
A. Computer data 55
B. Punishable conduct 56
1. Deleting and erasing data 56
2. Damage, deterioration and alteration of data 56
3. Commission mode 57
C. Unlawfulness 58
D. Intention 59
IV. Optional additional constituent element 59
V. Comparison with Swiss law 60
Bibliography 61
Materials 61

I. GENERAL INFORMATION

Over the past twenty years, society as a whole has made the transition to a digital world. A large proportion of commerce is conducted online, financial transactions are carried out via e-banking, and authorities, companies and private individuals store large quantities of information on personal computers, servers or even clouds. Despite the scale of change already achieved, this evolution seems far from over. Indeed, it is highly likely that society will continue to become even more digitalized in the decades to come. 1

Digital documents are gradually replacing paper documents. In line with this trend, more and more documents are in electronic format. 2

In view of the growing importance of computer data in the digital world, it was justified to protect them against malicious acts. While art. 2 and 3 CCC protect data confidentiality, art. 4 CCC aims to ensure data integrity and availability. 3

II. LEGALLY PROTECTED PROPERTY

The purpose of art. 4 CCC is to provide computer data and programs with protection similar to that afforded to tangible property against intentional damage. The legal interests protected by this provision are, on the one hand, the integrity of data and computer programs and, on the other, the proper functioning or use of data and computer programs. 4

III. BASIC CONSTITUENT ELEMENTS

A. Computer data

According to art. 1 let. b CCC, "the term 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program designed to cause a computer system to perform a function". The notion of computer data is therefore very broad, encompassing in particular all letters, symbols or programming codes that can be entered, processed and stored by a computer system. 5

For further details on this concept, please refer to art. 1 CCC above. 6

B. Punishable conduct

7 For a computer system to function properly, the data it processes must be available and intact. In order to guarantee these two aspects, art. 4 CCC lists five punishable acts. The suppression and deletion of data is intended to protect data availability. The criminalization of damage, deterioration and alteration is designed to protect data integrity. This list of behaviors is exhaustive. It does, however, cover all possible harmful behaviors.

1. Deleting and erasing data

8 In computer terms, data is expressed in binary language as a succession of "0s" and "1s". This is the form in which data is processed and stored. When the user records data, the computer system saves the series of "0 "s and "1 "s corresponding to this data to an empty space on the recording medium (e.g. hard disk, DVD, USB stick, etc.). In order to be able to find this data when the user needs it again, the computer system has a kind of map which tells it where the data is located on the medium.

9 Data deletion involves destroying the means of locating the data. The data still exists, but the user can no longer determine its location on the medium and therefore can no longer access it. The computer system considers the space on the media to be free, and therefore saves the new data on top of the deleted data. The only way to recover deleted data is to use a data recovery program as quickly as possible. This program reads the entire media and reconstructs a map of the recording medium to locate the data. This enables data to be recovered before others are recorded over it.

10 Unlike deletion, data erasure is the definitive destruction of data. The data no longer exists on the storage medium. In principle, they can no longer be recovered.

2. Damage, deterioration and alteration of data

11 Data integrity is just as essential to the smooth operation of information systems as data availability. Its importance is so great that it is even the subject of an ISO standard. Data integrity refers to the reliability, accuracy and completeness of data. In other words, data whose integrity is guaranteed is data that has not been modified since it was first recorded. The notion of data integrity concerns both data content and data form.

In the real world, the notion of guaranteed data integrity can be compared to sending a parcel through the post, where it is certified that it really comes from the sender indicated on the parcel, that it was sent on the date and in the place indicated on the postmark, that the parcel has not been opened, that its contents are indeed those sent by the sender, and that nothing has been removed or added to the parcel after it has been sent. 12

In this context, data "damage" and "deterioration" are overlapping concepts. They describe negative damage to the form or content of data or programs. Damaged or deteriorated data is therefore no longer reliable, accurate or complete. It is no longer possible to be sure that they originate from the sender from whom they appear to originate, that they are in fact the data that was sent by the sender, and that no data has been deleted, added to or altered. 13

"Alteration" refers to the modification of existing data. This modification may concern both the form and content of the data. This is a very broad term, encompassing all actions carried out on data by which one or more elements are added, replaced or deleted. 14

3. Commission mode

The various types of behavior we have just examined can be committed directly by the perpetrator. However, it is also possible to use a bot to carry out these acts. This has the advantage that the perpetrator only has to give instructions once to the program, which then automatically repeats the requested actions as many times as necessary. It is to be feared that the development of artificial intelligence will make this task even simpler and more efficient in the future. WormGPT is undoubtedly the forerunner of a new form of infringement, as it enables content generated by artificial intelligence to be implemented in other IT systems, whereas the latter has until now been confined to an IT sandbox. 15

That said, even without using a bot, artificial intelligence already offers countless possibilities for modifying data. For example, it can easily be asked to rewrite a text by replacing one idea with another, or to modify an image by substituting one element with another. In future, therefore, it will become increasingly difficult to distinguish between genuine and modified data. 16

In the vast majority of cases, data breaches are achieved through punishable conduct. However, data breaches can also occur as a result of inadequate pro- 17

tection of the IT system. In our opinion, in such cases, there may be commission by omission on the part of the IT system administrator, since, by virtue of his function, he has a legal duty to act, and is therefore in a position of guarantor vis-à-vis the data owner.

C. Unlawfulness

18 To be punishable, the author must have acted without right. It is the rightful owner of the data who determines who is authorized to modify it. Anyone who has not been authorized to modify the data is therefore liable to prosecution. On the other hand, persons who have been expressly authorized by the rightful owner to modify the data, or who are authorized to do so by law or contract, are not liable to prosecution.

19 Nowadays, it is common for data to be modified by conclusive act. This is the case, for example, whenever messages are exchanged via instant messengers such as WhatsApp, Telegraph or Threema. All these applications encrypt data before it is sent, and decrypt it when it is received. This is data modification. It is, however, lawful, firstly because it is accepted by users by means of a conclusive act and, secondly, because it ensures data confidentiality.

20 Another case of data modification by conclusive act is application updates. During an update, a new version of the program is installed in place of the old one. Existing data is erased, and new data is written and recorded on the storage medium. This process is lawful, provided that the user has the choice of whether or not to install the update. In our opinion, the application publisher who forces the user to install a new version of the application, failing which it becomes unusable, or the data unreadable, makes himself punishable.

21 With regard to acts authorized by law, certain national legislations contain exceptions to the data integrity guarantee. In particular, they allow prosecuting authorities or intelligence services to install govware in computer systems in order to monitor the activity of those using them, for example to discover the perpetrator of a crime or to obtain information useful for the protection of the state. The installation of such spyware is not illegal, as long as it is carried out within the strict framework laid down by law. However, surveillance may only be carried out in serious cases, and must be subject to subsequent judicial review.

The modification of data is also not unlawful where it has been contractually authorized. This applies in particular to the computer system administrator, who is responsible for maintenance. He is not punishable if he updates the programs installed in the computer system. On the other hand, he is punishable if he takes advantage of his status to delete or modify a user's data without his authorization. 22

Similarly, a computer specialist commissioned to carry out penetration tests on a computer system is not punishable if he modifies data to create a breach in the defences put in place to protect access to the computer system. On the other hand, a hacker who acts in the same way without authorization is punishable. 23

D. Intention

A breach of data integrity must be intentional. Intention must cover all the objective elements of the offence. The perpetrator must therefore be aware that he or she is unduly damaging data, and have the will to do so. Any intent on the part of the perpetrator is sufficient. 24

IV. OPTIONAL ADDITIONAL CONSTITUENT ELEMENT

Art. 4 § 2 CCC authorizes States parties to make a reservation and to prosecute only conduct that has caused serious harm. 25

The text does not define the notion of "serious harm". As for the explanatory report, it simply states that each State is free to interpret this notion as it wishes. However, the Parties have opted for the notion of "harm" rather than "damage". It is therefore clear that harm is not limited solely to the economic aspect. Harm can therefore also correspond to the work time required to recover or recreate the data, as well as to the consequences of the disappearance or impossibility of using the data. 26

The parties also specified that the damage must be serious. This adjective, in conjunction with the notion of prejudice, means that it must be of a certain magnitude. It is therefore conceivable that the damage must represent a substantial sum of money, a significant number of working hours or have serious consequences. 27

28 Azerbaijan, Lithuania, the Slovak Republic, Chile and the United States of America have made use of the possibility offered by art. 4 § 2 CCC. Azerbaijan, Lithuania, the Slovak Republic and the United States of America have clarified that in their domestic law, the notion of serious injury must be interpreted as having caused serious damage. The Slovak Penal Code has since been amended. Section 247 has been replaced by section 247b. In its simple form, the occurrence of serious harm is no longer required (§ 247b par. 1). On the other hand, the occurrence of serious harm has become a qualified form of the offence (§ 247b par. 2 let. a). Chile, for its part, spoke of serious damage. It can thus be seen that, even if the letter of the Convention allows for a very broad interpretation, all the States that have availed themselves of the possibility offered by art. 4 § 2 CCC have limited the notion of harm to the economic aspect alone.

29 In this respect, it is interesting to note the original way in which Swiss law has dealt with the question of serious prejudice. Instead of limiting criminal prosecution to conduct that has caused serious harm, art. 144bis ch. 1 para. 2 of the Swiss Penal Code provides for a qualified form of prosecution when the harm caused by the perpetrator is considerable.

V. COMPARISON WITH SWISS LAW

30 In Swiss law, data interference (art. 4 CCC) has its counterpart in art. 144bis ch. 1 PC. The legal interests protected by these two standards are not strictly identical, however, since art. 4 CCC protects the integrity and proper functioning or use of stored data or computer programs, whereas art. 144bis ch. 1 PC protects the right to intact data. They are, however, very similar and overlap in their purpose.

31 As far as the conduct punishable under art. 4 CCC is concerned, it is all covered by art. 144bis ch. 1 PC. The concepts of "damage", "deterioration" and "alteration" in art. 4 CCC are covered by the term "modifies", which includes all forms of transformation. The concept of "erasure" referred to in the Convention, i.e. the definitive destruction of data, is identical in Swiss law. Finally, the "deletion" of data referred to in art. 4 CCC is covered by the term "puts out of use", which encompasses all forms of behaviour by which the rightful owner is prevented from making proper use of his or her data.

Lastly, art. 144bis ch. 1 of the Swiss Penal Code establishes an offence that can only be prosecuted on the basis of a complaint. However, when an offence is only prosecuted on the basis of a complaint, a criminal authority cannot take action itself. Since there is a conflict of opinion as to whether a complaint lodged in the requesting state is sufficient to implement international cooperation, it would be prudent to prosecute data deterioration ex officio in all cases, or else to lodge a declaration limiting prosecution to cases where the damage caused is considerable. 32

The technical IT concepts contained in this contribution were drafted with the help of Mr. Yannick Jacquey, ICT Manager with a federal diploma. Our warmest thanks to him.

BIBLIOGRAPHY

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 / Crameri 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

MATERIALS

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)

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 5 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 5 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 5 CCC N. XXX.

Art. 5 System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

CONTENT

I. General information 65
II. Legally protected property 65
III. Basic constituent elements 66
A. A computer system 66
B. Punishable conduct 66
1. Introducing data 66
2. Data transmission 67
3. Damage, deterioration and alteration of data 67
4. Deleting and erasing data 68
5. Mode of commission 69
C. Serious interference with the operation of the computer system 70
D. Unlawfulness 71
E. Intention 72
IV. Comparison with Swiss law 72
Bibliography 73
Materials 74

I. GENERAL INFORMATION

Over the last few decades, society has undergone profound changes. Many services have become digitalized. Smartphones, which didn't even exist twenty years ago, are now ubiquitous in everyone's lives. Aware of this change, companies have adapted their services to these new devices, with the vast majority offering online services. This underlying trend has been further accelerated by the coronavirus pandemic that hit the world's population between 2020 and 2022. The health measures put in place by the authorities significantly restricted contact between individuals. As a result, the trade had to find new ways of doing business in order to survive. 1

Today, more than ever before in human history, all players in society are interconnected. Thanks to their smartphones, individuals can access their e-banking accounts, trade online, store data in the cloud or stream video from anywhere in the world, at any time. 2

This extreme interconnectedness, however, creates an equally extreme interdependence. This reality is perfectly illustrated by the large-scale cyberattack that hit Estonia for several days in 2007. One of the world's most connected countries was completely paralyzed. State administration, the banking system, commerce: nothing functioned, causing considerable damage to society as a whole. Today, even more than in the early 2000s, it is vital that IT systems can function without hindrance. 3

In view of the considerable damage that hindering the proper functioning of IT systems can cause, it was essential to protect the proper functioning of these systems by means of a penal standard. 4

II. LEGALLY PROTECTED PROPERTY

The legal asset protected by art. 5 CCC is the right of the operator and users of a computer or telecommunications system to ensure that it functions correctly. 5

III. BASIC CONSTITUENT ELEMENTS

A. A computer system

6 According to art. 1 let. a CCC, "the term 'computer system' means any isolated device or set of interconnected or related devices, which performs or of which one or more elements perform, in execution of a program, automated data processing". The notion of computer system thus includes all hardwares (motherboard, processor, hard disk, screen, keyboard, printer, etc.) and softwares (BIOS, operating system, software, updates, etc.), as well as the devices that connect these different elements to each other (cables, router, wifi terminal, etc.).

7 For further details on this concept, please refer to art. 1 CCC above.

B. Punishable conduct

8 Art. 5 CCC lists seven punishable acts: the introduction, transmission, damage, deletion, deterioration, alteration or suppression of computer data. This list is exhaustive. Behavior which hinders the proper functioning of the computer system, but which is not included in this list, is therefore not punishable. This is the case, for example, of moving data within the computer system, although this is just as harmful as damaging or deteriorating data.

1. Introducing data

9 The notion of "introduction" must be interpreted in the sense that the author introduces data from outside the target computer system. Some authors even go so far as to camouflage this data by giving it the appearance of completely innocuous files, to prevent it from being spotted too easily. From the outside, this data therefore appears to be original system data.

10 However, art. 5 CCC does not extend to all data introduced into the computer system, but only to data intended to hinder its proper functioning. This means malicious data or programs which slow down or even completely block the operation of the computer system. This can be achieved either by activating a feature that slows down or blocks the data processing process, or by deactivating a feature that is necessary for the computer system to function properly. Examples include the installation of a Trojan horse which enables the perpetrator to take control of all or part of the computer system, or the installa-

tion of a virus which paralyzes the processor or destroys a boot sector, preventing the computer from restarting.

2. Data transmission

The term "data transmission" refers to the sending of data from one computer system to another. The conduct referred to here is the sending of data which interferes with the proper functioning of the computer system. In particular, the parties wanted to criminalize denial-of-service and distributed denial-of-service attacks. A denial-of-service attack consists in sending such a large quantity of data to a target computer system that the latter is unable to process it all, and eventually crashes. 11

Over the years, the performance of computer systems, particularly servers, has increased considerably. Load balancing and high-availability techniques have made denial-of-service attacks virtually impossible. Cybercriminals have therefore evolved the denial-of-service attack into a distributed denial-of-service attack. This attack is similar to the previous one, with the difference that the perpetrator has control over a multitude of computer systems, to which he gives orders to simultaneously send very large quantities of data to the target computer system. Given the sheer volume of data coming in from all directions, the target computer system is unable to process them all, and eventually crashes. This type of attack is currently relatively widespread. It is almost always linked to ransom demands in exchange for stopping the attack, or to some other fraud such as data theft. Even today, there is no solution for effectively defending against distributed denial-of-service attacks. Moreover, the damage caused to victims is particularly significant, since they are either deprived of the use of their computer system, or impoverished by the payment of the ransom. 12

3. Damage, deterioration and alteration of data

Data integrity is essential to the proper functioning of information systems. Its importance is such that it is even the subject of an ISO standard. 13

Data integrity refers to the reliability, accuracy and completeness of data. Data of guaranteed integrity is data that has not been modified since it was first recorded. By way of illustration, the concept of guaranteed data integrity could be compared to sending a parcel by post, where it is certified that it was actually sent by the sender named on the parcel, that it was sent on the date 14

and at the location indicated on the postmark, that the parcel was not opened during transit, and that the contents of the parcel were not altered after it was sent.

15 It goes without saying that data content, i.e. the information contained in the data (e.g. text, code, image, etc.), is just as important as formal data integrity. In addition to guaranteeing the formal integrity of the data, it is therefore essential to also guarantee that the content of the data has not been corrupted. In the example of the package given above, formal data integrity is represented by the packaging, while data content integrity corresponds to the object inside the package.

16 The damage and deterioration of data referred to in art. 5 CCC are behaviours that overlap in the field of information technology. In both cases, the integrity or content of data or programs is adversely affected. Damaged or deteriorated data is no longer reliable, accurate or complete. The perpetrator modifies the data on the target computer system so that it can no longer be used correctly for data processing. For example, simply renaming a folder containing files essential to the proper functioning of the operating system is enough to bring the entire computer system to a standstill. Modifying the programming code of a software program can also block its proper functioning. More recently, cybercriminals have been encrypting data and then selling the encryption key.

17 Alteration refers to the modification of existing data in the computer system, as a consequence of another act performed by the perpetrator. It is a very broad generic term, encompassing all modifications made to data, i.e. the addition, replacement or deletion of data. These modifications may concern both the formal integrity and the content of the data. A case in point is the modification of data following the introduction of a Trojan horse or the installation of a virus.

4. Deleting and erasing data

18 Computer data is stored on storage media (e.g. hard disk, DVD, USB stick, etc.) in the order in which it was created. In order to be able to retrieve specific data when the user needs it again, the computer system establishes a kind of index, so that it knows which data is where on the medium.

Deleting data involves destroying all or part of this index, which enables the data to be located. The data still exists, but the computer system can no longer know where it is on the medium, and therefore can no longer access it. 19

Unlike deletion, data erasure is the definitive destruction of data. The data no longer exists on the storage medium. 20

When the author deletes or erases data essential to the proper functioning of the computer system, such as the operating system, the system becomes unusable and ceases to function. 21

5. Mode of commission

The various types of behavior we have just examined can obviously be committed directly by an individual. However, this would take a great deal of time. In practice, therefore, cybercriminals tend to use malware or bots to carry out these acts automatically. The rapid development of artificial intelligence will certainly make this type of action even easier to carry out. WormGPT already gives us a glimpse of the possibilities offered by artificial intelligence, since it enables content generated by artificial intelligence to be implemented in other IT systems, which until now has been confined to an IT sandbox. 22

There is also the question of commission by omission. Most of the time, punishable behavior is committed by cybercriminals who seek to hinder the smooth running of the computer system in order to obtain something in return. However, it is also conceivable that the computer system may eventually cease to function properly because its administrator is not taking care of the necessary updates. In our view, the administrator of the computer system is punishable in such a case, since, by virtue of his function, he has a legal duty to act, and is therefore in a position of guarantor towards the rightful owner and users of the computer system. 23

In our view, the solution is identical in the case of the computer system administrator who fails to install a firewall and/or antivirus to protect the system, thereby leaving countless opportunities for third parties to attack it. 24

C. Serious interference with the operation of the computer system

25 To be guilty of system interference, it is not enough for the perpetrator to attack the integrity of the data contained in the computer system, as this would constitute data interference within the meaning of art. 4 CCC. The act must seriously hinder the operation of the computer system.

26 Impairment occurs when the computer system no longer functions optimally. The wording of art. 5 CCC is sufficiently neutral to protect multiple functions. It is therefore irrelevant which functions are impaired. It is also irrelevant whether the entire computer system is impaired or whether only certain functions are impaired.

27 The computer system is impaired when it is put out of action. It is also impaired when an application can no longer be used. This may occur because the program's computer code has been damaged or destroyed, or because data saved by the user has been erased, deleted or encrypted. The computer system may also be impaired as a result of reduced performance. This is the case, for example, when a cybercriminal takes remote control of a computer system and uses it as a zombie machine without the knowledge of its owner. In doing so, he or she uses part of the computer system's performance without the consent of the rightful owner, usually for malicious purposes. Finally, the smooth running of a computer system can be hampered by excessive demands. This is the case with denial-of-service or distributed denial-of-service attacks. The computer system itself functions normally, but is besieged by so many simultaneous requests that it cannot process them quickly enough, and eventually crashes.

28 Given the wording of the standard, obstruction must be the result of punishable conduct. Since the list in art. 5 CCC is exhaustive, hindrance must necessarily result from one of the enumerated behaviours in order to be punishable. Obstruction resulting from other conduct, such as moving data within the computer system, is not punishable.

29 As for the qualifier "serious", this has deliberately not been defined, to allow each State to define it freely. For some, serious hindrance may refer to the minimum damage caused by the hindrance. For others, it will be a question of the extent of the hindrance, such as the blocking of all external connections

to a computer system. The authors of the draft "have deemed 'serious' the sending to a computer system of data whose form, volume or frequency significantly prejudices the owner's or operator's ability to use the system in question or to communicate with other systems (this is the case of programs that undermine systems in the form of a 'denial of service', malicious code, such as viruses, which prohibit or significantly slow down the operation of the system, or programs which send a huge volume of e-mail to a recipient in order to paralyze the system's communication functions)".

D. Unlawfulness

To be punishable, the author must have acted without right. It is the rightful owner of the computer system who determines who has the right to administer and use the system. This means that anyone who has not been authorized to modify the operation of the computer system is liable to prosecution. On the other hand, persons who have been authorized, expressly or by contract, by the rightful owner to modify the operation of the computer system, or who are authorized to do so by law or by contract, are not liable to punishment. 30

Until the early 2000s, it was rare for an operating system or application to require updating. Over the past two decades, however, updates have become increasingly common. Today, they are even the rule. During an update, a new version of the program is installed in place of the old one. Existing data is erased, and new data is written to the storage medium. For the most part, updates contain application patches, bug fixes or new features. A priori, therefore, there is no impediment to the smooth running of the computer system. However, some updates may require more storage space on the hard disk, or take up more RAM or processor capacity. As a result, the computer system slows down. As a result, system performance is hampered. In most cases, this is not a problem, as the slowdown of the computer system is very slight or even insignificant. In exceptional cases, however, updates may cause the computer system to slow down, notably because the previous version of the application was already stretching available resources to the limit, and the update requires more resources than are available. In all cases, the user must be able to choose whether or not to install the update. In our view, the publisher of the application is punishable if he forces the user to install a new version of the application, failing which the computer system is impeded in its proper functioning, or the application is rendered unusable. 31

32 The behaviors listed in art. 5 CCC are also not unlawful when they have been contractually authorized. One example is the computer system administrator, whose task is to maintain the system. He is not punishable if he updates the programs installed in the computer system. On the other hand, he is liable to punishment if he takes advantage of his status to undermine the proper functioning of the computer system, for example by uninstalling programs or deleting data.

E. Intention

33 Undermining the integrity of a system must be intentional. Intention must cover all the objective elements of the offence. The perpetrator must therefore be aware of and intend to disrupt the proper functioning of a computer system without being authorized to do so.

IV. COMPARISON WITH SWISS LAW

34 There is no equivalent to art. 5 CCC in Swiss law. Admittedly, the different forms of conduct could give the impression of a similarity with the deterioration of data (art. 144bis ch. 1 CP). However, this is not the case, for three reasons.

35 Firstly, the assets legally protected by art. 5 CCC and art. 144bis ch. 1 CP are completely different. As explained above, art. 5 CCC protects the interest of the operator and users of a computer or telecommunications system in its proper functioning, whereas art. 144bis ch. 1 PC ensures a right of disposal over data. In other words, the former guarantees the proper functioning of a means of data processing, while the latter protects a specific right in rem.

36 Given that the legally protected goods are not the same, the persons harmed by these two offences are not identical either. The person harmed by the deterioration of data (art. 144bis ch. 1 CP) is the owner of the deteriorated data. On the other hand, undermining the integrity of the system (art. 5 CCC) affects the rightful owner of the computer system.

37 Secondly, although these two offences share many points in common, they cannot be equated. Indeed, system interference (art. 5 CCC) must in some way be seen as a special form of data deterioration (art. 144bis ch. 1 PC), as it requires that the data interference causes a serious hindrance to the function-

ing of the computer system. This is an additional constituent element not required under Swiss law.

Finally, certain forms of conduct fall within the scope of art. 5 CCC, even though they are not punishable under art. 144bis ch. 1 CP. This is the case, for example, of sending "data to a computer system, the form, volume or frequency of which is significantly prejudicial to the owner's or operator's ability to use the system in question or to communicate with other systems". Nor are these acts adequately punished by art. 179septies of the Swiss Penal Code (misuse of telecommunications equipment), for three reasons. Firstly, because art. 179septies CP requires a special purpose - namely malice or mischief - in addition to intent, which is not the case with art. 5 CCC. Secondly, because misuse of a telecommunications facility is merely a contravention, punishable only by a fine. However, art. 13 § 1 CCC expressly stipulates that the offences punishable under arts. 2 to 11 CCC must be punishable by penalties including deprivation of liberty. Thirdly, because aiding and abetting and attempting to undermine the integrity of the system are punishable under art. 11 CCC, whereas aiding and abetting and attempting to misuse a telecommunications facility is not punishable, as it is a contravention (cf. art. 105 para. 2 PC). 38

In view of the foregoing, it must be concluded that Swiss law does not comply with art. 5 CCC. It should therefore be adapted. 39

The technical IT concepts contained in this contribution were drafted with the help of Mr. Yannick Jacquey, ICT Manager with a federal diploma. Our warmest thanks to him.

BIBLIOGRAPHY

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/Crameri 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

MATERIALS

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)

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 6 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 6 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 6 CCC N. XXX.

Art. 6 Misuse of devices

[1] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a. i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

[2] This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

[3] Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

CONTENT

I. General 78
II. Legally protected property 78
III. Basic building blocks 79
A. Unlawful object 79
1. A device enabling the commission of an offence mentioned in articles 2 to 5 CCC 79
2. Data enabling access to a computer system for the purpose of committing one of the offences mentioned in art. 2 to 5 CCC. 80
B. Punishable conduct 80
1. Production, sale, obtaining for use, import, dissemination or other forms of making available 80
2. Possession 81
C. Unlawfulness 82
D. Intention 82
E. Special purpose 82
IV. Reservations 83
A. Punishable conduct 83
B. Illicit material 84
V. Comparison with Swiss law 84
Bibliography 86
Materials 86

I. GENERAL

1 The commission of the offences punishable under articles 2 to 5 CCC generally requires the use of computer tools. However, not all cybercriminals are capable of creating these tools themselves. They therefore seek to acquire them from third parties. Over time, this demand has led to the creation of a veritable black market, particularly on the dark net. Nowadays, almost anyone can acquire malware of any kind, rent bots-nets or even commission cybercriminals to carry out specific tasks. Given the risk that this black market represents for all IT systems and their legitimate users, the Parties have decided to penalize certain potentially dangerous acts upstream, before the commission of the offences referred to in art. 2 to 5 CCC. Art. 6 CCC is based on instruments adopted by the Council of Europe (European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access - ETS No. 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access), as well as on provisions adopted in certain countries in this area.

II. LEGALLY PROTECTED PROPERTY

2 By punishing all forms of trade in or possession of material intended for the commission of any of the offences punishable under articles 2 to 5 CCC, the Parties make punishable the acts preparatory to the commission of these offences. The aim is therefore to strengthen the protection of the legal assets protected by articles 2 to 5 CCC, namely the inviolability and proper functioning of computer systems, as well as the integrity, availability and confidentiality of data.

III. BASIC BUILDING BLOCKS

A. Unlawful object

1. A device enabling the commission of an offence mentioned in articles 2 to 5 CCC

The concept of a device is not defined either in the text of the convention or in its explanatory report. In our opinion, a device within the meaning of art. 6 CCC is a set of parts, elements or data designed to perform one or more specific functions. This is evidenced by the fact that the Parties expressly cite the computer program as an example of a device. As is clear from the addition of the words "including", the notion is intended to be much broader than computer programs alone. In addition to viruses, worms, Trojan horses, logic bombs and other malware, which are indisputably among the programs covered by this provision, there are also hardware devices such as microphones, cameras and robots. 3

However, the scope of the standard is limited to devices designed or adapted to commit one of the offences punishable under articles 2 to 5 CCC. These are devices or programs designed, for example, to alter or even destroy data, or to interfere with the operation of systems, such as virus programs, or programs designed or adapted to access computer systems. Devices which do not enable such acts to be performed are not covered by art. 6 § 1 let. a ch. 1 CCC. The same applies to devices which enable the commission of another offence, notably one of those punishable under art. 7 to 10 CCC. 4

During the drafting of the Convention, there was extensive discussion as to whether the devices covered should be those designed exclusively or specifically to enable the commission of offences, thus excluding dual-use devices, or whether the latter should also be included. The Parties finally concluded that criminal prosecution should not be limited to devices designed exclusively to commit offences, as this would have considerably reduced the number of cases to which the standard could be applied. However, the Parties also ruled out the possibility of extending the standard to all devices, including licit ones, which could in some way enable the commission of offences, as the commission of the offence would then be based solely on the perpetrator's intention. An intermediate solution has therefore been adopted. 5

6 Art. 6 § 1 let. a ch. 1 CCC thus covers devices primarily designed or adapted to enable the commission of one of the offences punishable under arts. 2 to 5 CCC. This wording excludes dual-use devices, unless the main purpose is to commit an offence.

2. Data enabling access to a computer system for the purpose of committing one of the offences mentioned in art. 2 to 5 CCC.

7 In order to cover all the means used by cybercriminals to commit one of the offences punishable under articles 2 to 5 CCC, the Parties have also made punishable acts aimed at making available passwords, access codes and similar computer data enabling access to all or part of a computer system (article 6 § 1 let. a ch. 2 CCC). The aim is to eliminate any loopholes. This approach is perfectly justified in view of the large number of passwords and other access data that have been stolen and are offered for sale on the dark net.

B. Punishable conduct

8 The Parties intended to punish all forms of making illicit objects available, as well as their possession. On the other hand, the mere provision of instructions - in the form of texts or videos, for example - on how to manufacture illicit objects is not punishable.

1. Production, sale, obtaining for use, import, dissemination or other forms of making available

9 Art. 6 § 1 let. a CCC lists a number of punishable acts relating to trade. This list is exhaustive. In order not to omit any conduct, it nevertheless ends with a general clause ("Auffangtatbestand").

10 "Production" is the manufacture of illicit material with a view to its use in the commission of one of the offences listed in art. 2 to 5 CCC. The term "production" includes all the steps required to produce the object. It therefore includes writing the malware code - in computer language - or decrypting a password.

11 Art. 6 § 1 let. a CCC then sanctions "sale". This term refers to the handing over of an illicit object mentioned in this paragraph in exchange for a sum of money. The currency in which the sum is paid is irrelevant. It can even be paid in

cryptocurrencies. However, the remittance must be expensive. It cannot be a donation.

"Obtaining for use" implies active behavior on the part of the person seeking to obtain prohibited material. It is necessary to have established contact with someone in possession of the prohibited material, and to have acquired it either free of charge or in return for payment. The manner in which the material is handed over is irrelevant. The transfer can be made electronically, by post or even by hand delivery. What is decisive is whether the perpetrator obtains the illicit material with the aim of using it to commit one of the offences punishable under articles 2 to 5 CCC. If the aim is to commit another offence, or simply to collect this type of material, the perpetrator is not punishable. 12

The fourth conduct mentioned in the list is "importation". This term refers to the act of introducing an illicit object into the country that sanctions this act. Importing prohibited material creates a significant risk that it will subsequently be passed on to third parties. To reduce this risk, simple introduction into the country is prohibited, even if the importer is only one link in the chain between the producer of the material and the end user. 13

Article 6 § 1 also punishes "dissemination". This is the transmission of illicit material to an indeterminate number of persons who have not necessarily requested it. Material can be sent by any means, whether by computer, post or hand delivery. 14

To avoid any gaps, the list ends with "other forms of provision". This assumption makes it possible to cover all cases which do not correspond exactly to the notions examined above, but which nevertheless enable the author to supply illicit objects to third parties. This expression includes, for example, the creation or compilation of hypertext links designed to facilitate access to illicit material. 15

2. Possession

Art. 6 § 1 let. b CCC punishes possession of any of the above-mentioned objects. As with the conduct listed in art. 6 § 1 let. a CCC, the perpetrator must possess the prohibited material with the intention of committing one of the offences punishable under arts. 2 to 5 CCC. If the perpetrator holds this material with the intention of committing another offence, or simply for collection purposes, he is not punishable. 16

17 The Parties have, however, left each State some leeway in determining whether possession of a single item is sufficient to commit the offence, or whether possession of a number of items is required. It has to be said, however, that this possibility seems to have been introduced mainly in favor of the United States of America, which was the only one to make use of it. However, they did not specify the minimum number of elements that had to be possessed in order to be punishable. They simply referred to the number stipulated in the applicable US federal law.

C. Unlawfulness

18 The requirement that the perpetrator must have acted without right enables the Parties to create exceptions to criminal repression. In particular, this allows them to exclude from the scope of art. 6 CCC prosecuting authorities who lawfully hold illicit material, in the form of sequestration, as part of their investigations.

19 Art. 6 § 2 expressly reserves the hypothesis that the perpetrator is not acting without right, i.e. the conduct listed in art. 6 § 1 let. a ch. 1 CCC is not punishable if it is not intended to commit an offence punishable under arts. 2 to 5 CCC. Thus, for example, test devices (also known as "cracking devices") and network analysis devices designed by professionals to assess the reliability of their IT products or check system security are manufactured for legitimate purposes, and their users are therefore considered to be acting "lawfully".

D. Intention

20 Device abuse is intentional. Intention must relate to all the objective elements of the offence. If the perpetrator possesses or provides an ordinary computer program to a third party without suspecting that it could also be used to commit one of the offences punishable under articles 2 to 5 CCC, he is not punishable.

E. Special purpose

21 In addition to intent, the perpetrator must have acted with the intention of committing one of the offences referred to in articles 2 to 5 CCC. It is therefore not sufficient for the perpetrator to intend to manufacture a malicious program solely for the technical challenge it represents, or to collect it. Simi-

larly, it is not sufficient for the perpetrator to use the malware or password for the purpose of committing an offence other than those punishable under articles 2 to 5 CCC.

The aim pursued by the perpetrator must be the commission, by himself or by a third party to whom he supplies the prohibited material, of one of the offences punishable under articles 2 to 5 CCC. Art. 6 CCC establishes an abstract endangerment offence. It is therefore not necessary for the illicit material to be actually used subsequently to commit one of these offences. It is sufficient if the punishable act is committed with the aim of committing one of the offences punishable under articles 2 to 5 CCC. 22

IV. RESERVATIONS

The only conduct which the parties must punish is the sale, distribution or other provision of a password, access code or similar computer data enabling access to all or part of a computer system. They may, however, limit the scope of application of this standard with regard to other punishable conduct and/or illicit objects. 23

A. Punishable conduct

The Convention allows Parties to limit criminal prosecution by refusing to prosecute the production, obtaining for use, import and possession of illicit material. 24

Georgia, Switzerland, Chile, Japan and Sri-Lanka have made use of this possibility to limit punishable conduct as far as possible. 25

The Principality of Andorra has indicated that obtaining the devices referred to in art. 6 § 1 let. a CCC for use is not punishable under its domestic law. 26

Azerbaijan stated that it would only prosecute the conduct listed in art. 6 § 1 CCC if serious damage occurred. 27

Ukraine explained that it would not punish the obtaining for use and other forms of making available of the items referred to in art. 6 § 1 let. a ch. 1 CCC, as well as the production and obtaining for use of the items referred to in art. 6 § 1 let. a ch. 2 CCC. 28

29 The United States of America has reserved the right not to prosecute the production, procurement for use, import and possession of illicit material designed or adapted to enable the commission of the offences punishable under art. 4 and 5 CCC.

30 Israel has declared that it will not prosecute the obtaining for use or importation of illicit material, nor the possession of a password, access code or similar computer data enabling access to all or part of a computer system.

31 Germany, the Principality of Andorra, Argentina and Peru have limited themselves to refusing to prosecute possession of illicit material (art. 6 § 1 let. b CCC).

B. Illicit material

32 The Convention also allows Parties to limit prosecution by refusing to consider as illicit devices, including computer programs, primarily designed or adapted to enable the commission of one of the offences punishable under articles 2 to 5 CCC.

33 Georgia, Norway, Switzerland, Japan and Sri-Lanka have also made use of this possibility to limit punishable material as far as possible.

34 Chile initially entered the same reservation as Georgia, Norway, Switzerland and Japan. However, it amended its legislation in 2022. In its new version, abuso de los dispositivos corresponds to art. 6 CCC. The reservation is therefore no longer necessary.

35 The United States has reserved the right not to prosecute devices, including computer programs, designed or adapted to enable the commission of the offences punishable under art. 4 and 5 CCC.

36 Germany has declared that a device, including a computer program, primarily designed or adapted to enable the commission of an offence punishable under art. 2 to 5 CCC is not punishable material under German law.

V. COMPARISON WITH SWISS LAW

37 In its Message on the approval and implementation of the Council of Europe Convention on Cybercrime, the Federal Council stated that art. 6 CCC was essentially covered by art. 144bis para. 2 of the Swiss Criminal Code, as well as

by the addition of a second paragraph to art. 143bis of the Swiss Criminal Code.

However, even if Switzerland has made use of all the possibilities afforded by art. 6 § 3 CCC to limit punishable conduct and illicit material to a minimum, the fact remains that Swiss law falls far short of the minimum requirements laid down by art. 6 CCC, for several reasons. 38

Firstly, art. 144bis ch. 2 al. 1 CP only applies to software. It does not apply to other devices, passwords, access codes or similar computer data. What's more, the software covered by art. 144bis ch. 2 al. 1 CP must be suitable or intended for committing an offence punishable under art. 144bis ch. 1 al. 1 CP. This raises two problems. On the one hand, art. 144bis ch. 1 al. 1 CP does not fully satisfy the minimum requirements of art. 4 CCC. On the other hand, art. 144bis ch. 2 al. 1 CP completely ignores software which is itself or is intended to commit an offence corresponding to those punishable under art. 2, 3 or 5 CCC. Such software is therefore not punishable under Swiss law. 39

The addition of art. 143bis para. 2 of the Swiss Penal Code closes only a small part of these important loopholes. Indeed, this provision only punishes the act of putting into circulation or making accessible a password, a program or any other data suitable or intended for committing the offence punishable under art. 143bis para. 1 PC. On the one hand, this standard does not meet the minimum requirements of art. 2 CCC. Secondly, it does not penalize the circulation or making available of a password, program or any other data suitable or intended for the commission of an offence other than that punishable under art. 143bis para. 1 of the Criminal Code. 40

In the final analysis, even assuming that art. 143bis para. 1 PC meets the requirements of art. 2 CCC, and that art. 144bis para. 1 para. 1 PC meets the minimum requirements of art. 4 CCC, punishability under Swiss law would be limited to circulating or making available a password, program or other data suitable or intended for committing the offence punishable under art. 2 CCC, as well as manufacturing, importing, putting into circulation, promoting, offering or otherwise making available software suitable for or intended to commit the offence punishable under art. 4 CCC. 41

In order to meet the minimum requirements of art. 6 CCC, art. 143 para. 1, art. 143bis para. 1 and art. 144bis ch. 1 para. 1 PC would therefore have to be adapted as indicated above; the equivalent of art. 5 CCC and complete each of 42

these provisions by adding a paragraph which would punish the sale, distribution or any other provision of a password, access code or similar computer data enabling access to all or part of a computer system, with the aim of committing one of these four offences.

BIBLIOGRAPHY

Trechsel Stefan/Crameri 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

MATERIALS

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

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 7 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 7 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 7 CCC N. XXX.

Title 2: Computer-related offences

Art. 7 Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

CONTENT

I. General 89
II. Legally protected property 89
III. Basic constituent elements 89
A. Computer data 89
B. Data relevant to legal relations 89
C. Punishable conduct 91
1. Data entry 91
2. Data alteration, deletion and erasure 92
D. Unlawfulness 93
E. Intention 93
IV. Optional additional constituent elements 93
V. Comparison with Swiss law 94
Materials 95

I. GENERAL

Given the omnipresence of information technology in society, forgery of computer documents is just as dangerous as forgery of paper documents. The purpose of this provision is therefore to establish an offence which is the counterpart of forgery of paper documents. It aims to close the loopholes in criminal law associated with classic falsification, which requires the visual legibility of statements contained in a document and does not apply to data recorded on electronic media. Manipulating recorded data with probative value can have consequences as serious as traditional acts of forgery, if they mislead a third party. Computer forgery consists in the unauthorized creation or modification of recorded data in such a way that it acquires a different probative value, so that the conduct of legal transactions, based on the authenticity of the information provided by this data, may be tainted by deception. 1

II. LEGALLY PROTECTED PROPERTY

The legally protected property of this standard is the security and reliability of electronic data, which may have consequences for legal relationships. 2

III. BASIC CONSTITUENT ELEMENTS

A. Computer data

According to art. 1 let. b CCC, "the term 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable for causing a computer system to perform a function". The notion of computer data is therefore very broad, encompassing in particular all letters, symbols or programming codes that can be entered, processed and stored by a computer system. 3

For further details on this concept, please refer to art. 1 CCC above. 4

B. Data relevant to legal relations

The use of the words "for legal purposes" means that art. 7 CCC does not apply to all computer data, but only to data that plays a role in legal relations. This means that it must be possible to prove a fact of legal significance, i.e. a 5

fact on which the creation, modification or extinction of a right depends. All data that is not relevant to legal relations is therefore excluded from the scope of this standard.

6 To be probative, it must be possible to establish the origin of the data. In the real world, this requirement means that the author of a title must be identifiable, and that this title contains the expression of a human thought. In practical terms, this means, for example, that the information must make sense, and that the document must be signed by its author. In the virtual world, guaranteeing the origin of data takes a very different form. Of course, the equivalent of a paper document signed by its author does exist. In this case, it's a computer document drafted by a human being, in which the handwritten signature is replaced by a qualified electronic signature. However, the virtual world offers many additional possibilities for producing data relevant to legal relationships.

7 Unlike securities issued in the real world, in the virtual world it is not mandatory for the author of the data to be a human being. Some data can be generated automatically by computer systems, without losing their probative value. Examples include a payment receipt created by an e-banking application, a salary certificate for the tax authorities automatically generated by a company's IT system for its employees at the end of the year, or a receipt sent automatically by an authority attesting to the filing of a legal deed by electronic means.

8 As art. 7 CCC expressly states, this provision extends to all data relevant to legal relationships, "whether or not they are directly legible and intelligible". Nor is it essential for the data to contain the expression of human thought. The data may well have been generated by a computer system. It simply has to be understandable by a human or a machine. Data can therefore take the form of a sequence of characters forming a code, a barcode or a QR code. The best recent example of this type of data is the computer-generated COVID certificate in the form of a QR code, which certifies that a person has been vaccinated against COVID and allows its holder access to certain places.

9 Ultimately, in the virtual world, for data to have probative value and be used in legal relations, it is sufficient that its origin can be established with certainty and that it can be understood by a human or a machine.

C. Punishable conduct

The definition of forgery varies considerably from country to country. A simple comparison of the definition given in Switzerland and its neighbouring countries is all that is needed. For some countries, the notion of forgery is based on the authenticity of the document's author, while for others, it is the veracity of the information contained in the document that is decisive. The Parties have therefore agreed that falsification must at least relate to the identity of the issuer of the data, irrespective of the accuracy or veracity of the content of the data. They are, however, free to extend the scope of their national provisions to include falsification of the information contained in the document. 10

The authenticity of the data as to its author implies that it actually comes from the person from whom it appears to originate. In this sense, the falsification of authentic data consists in the appearance of an author who is not the person from whom the data actually originates. The real author is therefore not the same as the apparent author. 11

As far as authenticity of data content is concerned, this means that the data has remained in its original state. Falsification therefore occurs when the data has been modified after it has been created. The modification referred to in art. 7 CCC is not the simple correction of a clerical error, but the modification of the meaning of the data. 12

Art. 7 CCC thus lists four punishable acts: introducing, altering, deleting or suppressing computer data. This list is exhaustive. The introduction of data punishes the creation of a false document, while alteration, deletion and suppression relate to the falsification of a true document. 13

1. Data entry

The introduction of data is the act by which the author introduces data from outside a computer system. This may involve the unauthorized introduction of accurate data or the addition of inaccurate data. 14

Art. 7 CCC only sanctions the introduction of data which leads to the creation of non-authentic data. Where the data introduced into the computer system is intended to hinder its proper operation, art. 5 CCC applies. 15

16 An example of the introduction of non-authentic data would be a company accountant who records a payment by a debtor in the accounting program, whereas the debtor in question has not in fact paid. Another example would be a person who uses a bank card that he has fraudulently copied to pay for his purchases, using the contactless function, thus making the vendor's terminal believe that the payment has been authorized and made by the legitimate holder of the copied card.

2. Data alteration, deletion and erasure

17 The alteration of data consists in damaging the integrity and/or content of the data. Data integrity refers to the reliability, accuracy and completeness of data. In the real world, the guarantee of data integrity could be compared to a parcel sent by post, where it is certified that it was really sent by the sender mentioned on the parcel, that it was sent on the date and at the place indicated on the postmark, and that the parcel was not opened during transit. As for the guarantee of contents, this could be compared to the certification that the contents of the parcel have not been altered after dispatch. In the case of data tampering, the perpetrator modifies the contents of the package and/or its packaging in order to deceive the recipient. Altering data content involves replacing the original data with other data. This is the case, for example, when the author modifies a text, changes bank details or replaces one image with another. On the other hand, the author alters the integrity of the data when he or she modifies the metadata. This is the case, for example, of someone who falsifies the sender's e-mail address to make it appear that a message has come from a certain person, when in fact it has come from someone else, or forges a qualified electronic signature to make it appear that a document has been drawn up by a certain person, when in fact this is not the case.

18 Data deletion involves withholding and concealing data. The author deliberately removes part of the data, so that the recipient is not aware of the entirety of the data. This is the case, for example, when the author deletes part of the clauses negotiated during transactional talks, with the aim of concluding a contract that is more favorable to him.

19 Unlike data deletion, data erasure is the definitive destruction of all or part of the data. The data no longer exists. Examples of this are when someone deletes parts of electronic conversations that are unfavorable to him, and then produces the redacted version as evidence in a court case, or when someone

deletes data from a computerized medical record to conceal a medical error he has made.

D. Unlawfulness

The author must act without right, i.e. without having been authorized to do so by the rightful owner. To act lawfully, a person must obtain the consent of the owner of the computer system to enter data, or of the owner of the data to modify it. 20

In today's society, many companies and public authorities work with IT systems. The majority of employees working for these entities are authorized to enter or modify data. All these people act lawfully as long as they follow the instructions they have been given. On the other hand, their actions become unlawful when they introduce or modify data in violation of the instructions they have received. This is the case, for example, of the person in charge of the cash register, who steals goods and then enters false sales into the computer system in an attempt to erase the traces of his crime. 21

E. Intention

Computer falsification is intentional. Intention must relate to all the objective elements of the offence. The perpetrator must therefore have the awareness and the will to create false data or to falsify authentic data with the aim of using them in legal relations. 22

IV. OPTIONAL ADDITIONAL CONSTITUENT ELEMENTS

The last sentence of art. 7 CCC allows Parties to require a special purpose in addition to intent. This special purpose may take the form of fraudulent intent or similar pernicious intent. The explanatory report contains no indication as to how the notion of fraudulent intent is to be understood. In our opinion, fraudulent intent refers to the perpetrator's intention to obtain an undue advantage for himself or for another person. This advantage need not be pecuniary in nature. It can be any advantage that improves one's personal situation or that of another. However, the advantage sought must be undue, i.e. contrary to law. 23

24 The United States of America has availed itself of the possibility offered by art. 7 in fine CCC and has indicated that it will only prosecute computer falsification if it is committed with fraudulent intent.

25 Germany and Peru have taken up the two purposes mentioned in art. 7 in fine CCC, namely that computer falsification must be committed with fraudulent intent or similar criminal intent.

26 Belgium, for its part, declared that it would only criminalize computer falsification when committed with fraudulent intent or malicious intent.

27 Switzerland decided that it would only prosecute computer falsification if it was committed with the intention of procuring for oneself or a third party an advantage or causing damage.

28 Finally, Chile had initially explained that it would only prosecute computer falsification if it was committed with fraudulent intent and caused damage to third parties. In our opinion, this statement was not in line with the text of art. 7 CCC, as a Party can only require additional special intent. It is not possible, however, to require the realization of a prejudice, whereas art. 7 CCC punishes an offence of endangerment. In 2022, Chile amended its legislation. In its new version, falsificación informática corresponds to art. 7 CCC. The reservation is therefore no longer necessary.

V. COMPARISON WITH SWISS LAW

29 The purpose of art. 7 CCC is to penalize forgery of computerized documents. Under Swiss law, this legal asset is protected by forgery of securities (art. 251 StGB), which has been extended to computerized securities (art. 110 para. 4 StGB) since January 1, 1995.

30 The conduct punishable under art. 7 CCC consists in falsifying data with probative value with the aim of deceiving others. The introduction of data corresponds to the creation of a false document. On the other hand, alteration, deletion and suppression are equivalent to the falsification of a document in the traditional offence of forgery.

31 Swiss law therefore complies with the requirements of Art. 7 of the Convention.

MATERIALS

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

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 8 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 8 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 8 CCC N. XXX.

Art. 8 Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

CONTENT

I. General 99
II. Legally protected property 99
III. Basic constituent elements 99
A. A computer system 99
B. Computer data 99
C. Punishable conduct 100
1. Data manipulation 100
a. Data entry 100
b. Alteration, deletion and erasure of data 100
2. Impairment of the computer system 101
D. Damage to property 101
E. Unlawfulness 102
F. Intention 102
G. A special design 102
IV. Comparison with Swiss law 103
Bibliography 104
Materials 104

I. GENERAL

The development of information technology and its penetration into all areas, especially money transfer, have transformed this sector into a veritable haven for economic crime. The ease with which offences can be committed and the virtual absence of risk of criminal prosecution have encouraged the transfer of "traditional" economic offences to the Internet. In order to combat this form of crime, art. 8 CCC criminalizes "any improper manipulation during data processing with a view to effecting an unlawful transfer of ownership". 1

II. LEGALLY PROTECTED PROPERTY

This provision protects computer systems against fraudulent manipulation with the aim of causing damage to the property of others and profiting from it. 2

III. BASIC CONSTITUENT ELEMENTS

A. A computer system

According to art. 1 let. a CCC, "the term 'computer system' means any isolated device or set of interconnected or related devices, which performs, or one or more of whose elements perform, automated data processing in execution of a program". The notion of computer system thus includes all hardwares (motherboard, processor, hard disk, screen, keyboard, printer, ...) and softwares (BIOS, operating system, software, updates, ...), as well as the devices that connect these different elements to each other (cables, router, wifi terminal, ...). 3

For further details on this concept, please refer to art. 1 CCC above. 4

B. Computer data

According to art. 1 let. b CCC, "the expression 'computer data' means any representation of facts, information or concepts in a form suitable for computer processing, including a program designed to cause a computer system to perform a function". The notion of computer data is therefore very broad, encompassing in particular all letters, symbols or programming codes that can be entered, processed and stored by a computer system. 5

6 For further details on this notion, please refer to art. 1 CCC above.

C. Punishable conduct

7 Art. 8 CCC lists a number of punishable acts and divides them into two categories. The first concerns the manipulation of data, while the second relates to interference with the functioning of the computer system.

1. Data manipulation

a. Data entry

8 Data input has the same meaning as in art. 4, 5 and 7 CCC. It therefore refers to the act whereby the perpetrator introduces into a computer system data originating from outside the system. However, art. 8 CCC does not penalize the introduction of just any data, but only that which is likely to cause proprietary damage.

9 In particular, data is introduced when the perpetrator, without authorization, inserts a debit card into an ATM and enters the personal identification number in order to make a cash withdrawal, or when the perpetrator logs on to an e-banking portal, in the place of a third party, using an ID and password that he has stolen, and wrongfully makes a money transfer.

b. Alteration, deletion and erasure of data

10 The concepts of data alteration, deletion and erasure are identical to those of art. 4, 5 and 7 CCC.

11 Data alteration occurs when the perpetrator undermines the integrity of the data, i.e. its reliability, accuracy and completeness. This is the case, for example, when the perpetrator alters the metadata of a payment during an online transaction, with the result that the bank's computer system redirects the funds to an account belonging to the perpetrator rather than to the account of the original recipient.

12 Data are also altered when the perpetrator attacks their content. A case in point is when the perpetrator changes the bank details or the amount of a payment order on an e-banking platform in the background, without the user noticing, so that the payment is higher than expected and/or is not credited to the intended account.

The author deletes data if he hinders free access to it. The author prevents the computer system from having full access to all the data to which it should have access. This is the case of the author who, having a credit limit with a credit card company, deletes the data relating to this limit from the company's computer system, in order to enable him to continue making credit payments, even though he knows he will not have the means to repay them. 13

Finally, data erasure is the definitive destruction of data. They no longer exist. We might think here of the author who accesses his creditor's computer system and deletes all data relating to the sum he owes, or of the person who, in the course of an online auction, deletes the highest bids and replaces them with his own bid at a much lower price. 14

2. Impairment of the computer system

To ensure that no fraudulent behaviour is overlooked, art. 8 let. b CCC also generally covers "any form of interference with the functioning of a computer system". This wording refers to acts such as manipulation of hardware, actions preventing printouts and acts affecting data records or data flows, as well as the order in which programs are executed. 15

In contrast to the behaviour punishable under art. 5 CCC, interference with the functioning of the computer system need not be serious. It must, however, be intended to cause financial loss. 16

An example of this would be the manipulation of a bank card payment terminal to confirm a payment to the seller, when in fact the payment has not been made to the account to be debited. 17

D. Damage to property

The above-mentioned behaviors are only punishable if they cause financial loss to others. This prejudice may be economic or material - a very broad concept which encompasses both liquid assets and tangible or intangible fixed assets of economic value. More generally, it can be defined as any injury to assets in the form of a decrease in assets, an increase in liabilities, a non-increase in assets or a non-decrease in liabilities. 18

The text of art. 8 CCC does not set a minimum amount for the pecuniary damage caused. Even a minimal loss is sufficient. 19

20 Nor is it required that the loss be definitive. A temporary or provisional loss may suffice. A fraudulent banking transaction which causes financial loss to the account holder who has been debited, but which is subsequently corrected when the fraud is revealed, constitutes an offence.

E. Unlawfulness

21 The perpetrator must act without right, i.e. without having been authorized to do so by the rightful owner, by law or by contract.

22 A person entrusted by a rightful claimant with a login and password to make an e-banking payment is not acting without right, as long as he or she is merely carrying out the instructions he or she has received. If, on the other hand, he uses his access rights to increase the amount of the transfer or change the identity of the beneficiary, he is acting without right.

23 The administrator of an e-banking portal or online store, whose task is to maintain it, is not liable to prosecution if he modifies data or temporarily prevents the website from functioning. On the other hand, if he takes advantage of his access, for example to modify data in a customer's account, he is guilty of computer fraud.

F. Intention

24 Computer fraud is intentional. Intention must cover all the objective constituent elements, i.e. both the punishable conduct and the occurrence of financial loss.

G. A special design

25 In addition to intent, art. 8 CCC requires that the author act in a drawing to procure for himself or a third party an economic benefit. In our view, the notion of economic benefit should not be understood in the narrow sense in which it is used in accounting. On the contrary, it encompasses all economic advantages that lead to enrichment. In other words, it refers to any improvement in a company's financial situation.

26 We are thinking primarily of an increase in assets, a decrease in liabilities, a non-decrease in assets or a non-increase in liabilities. In these cases, the enrichment corresponds, for example, to the price of goods delivered but not

paid for, to the sum diverted from a bank account, or to the amount of the service obtained at someone else's expense.

In our opinion, the notion of economic benefit is even broader, and also extends to any patrimonial advantage. This is the case of the author who can use a paid streaming platform without having to pay for it, of the person who, when booking online, provides a third party's credit card number as a guarantee so as not to have to bear the risk of having his or her credit card debited in the event of a late cancellation, or of the person who uses the contact details of a third party, such as a student or pensioner, to obtain - at a reduced price - services that he or she would have had to pay the full price for. 27

The economic benefit intended by the author must also be obtained free of charge. If the author has or believes he has a pecuniary claim corresponding to the enrichment obtained, he is not acting without right and is therefore not punishable. Similarly, competing commercial activities which may cause economic harm to one person and benefit to another, but which are not carried out with fraudulent or dishonest intent, such as the use of information-gathering programs to leverage competition on the Internet, do not constitute computer fraud. 28

IV. COMPARISON WITH SWISS LAW

In Swiss law, the provision that comes closest to art. 8 CCC is art. 147 of the Swiss Criminal Code. However, this provision does not meet the requirements of art. 8 CCC in several respects. 29

Firstly, the legal assets protected by the two provisions are different. Art. 8 CCC protects computer systems against fraudulent manipulation with the aim of causing damage to the property of others and profiting from it. Art. 147 of the Swiss Criminal Code, on the other hand, protects only assets, to the exclusion of the computer system operator's interest in ensuring that the system is used correctly. 30

With regard to punishable conduct, art. 147 of the Swiss Criminal Code penalizes the incorrect, incomplete or improper use of data. These largely overlap with the concepts of introducing, altering, deleting or suppressing computer data, mentioned in art. 8 CCC. However, Art. 147 PC leaves a significant loophole open, as it does not penalize the deletion of data that should have been in the computer system. 31

32 Finally, art. 147 of the Criminal Code only punishes computer fraud caused by data manipulation. The conduct referred to in art. 8 let. b CCC is therefore not covered by art. 147 PC. This point is particularly problematic, as many acts escape punishment, even though Switzerland has undertaken to prosecute them.

33 It has to be said that Swiss law does not comply with art. 8 CCC and should therefore be adapted.

BIBLIOGRAPHY

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

MATERIALS

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à https://rm.coe.int/168

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 9 CCC (Convention on Cybercrime)

A commentary by Jérémie Müller

SUGGESTED CITATION

Jérémie Müller, Commentary of art. 9 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Müller, art. 9 CCC N. XXX.

Title 3: Content-related offences

Art. 9 Offences related to child pornography

[1] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another person;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.

CONTENT

I. General information 108
II. Legally protected property 109
III. Basic constituent elements 109
A. A child pornographic representation 109
1. The medium of representation 109
2. Pornographic nature 109
3. The notion of minor 110
4. The notion of child pornography 110
B. Punishable conduct 111
C. Unlawfulness 113
D. Intention 114
IV. Reservations 114
A. With regard to the age of minors depicted 114
B. Punishable conduct 115
C. Objects of representation 116
V. Comparison with Swiss law 116
Bibliography 116
Materials 117

I. GENERAL INFORMATION

1 The advent of the Internet has enabled the longest, fastest and most efficient exchanges known to mankind. However, it has also provided high-performance communication tools for criminals who were previously often isolated. For example, people producing child pornography have been able to make contact with child pornographers all over the world. The exchange of ideas, fantasies and advice between paedophiles has helped to support, encourage or facilitate sexual offences against children.

2 As well as facilitating the exchange of child pornography, the virtual world has also guaranteed a degree of anonymity for perpetrators, and consequently a form of impunity. It is therefore not surprising that this type of crime has developed rapidly with the spread of the Internet.

3 Art. 9 CCC therefore responds to the concern expressed by the members of the Council of Europe at their 2nd Summit in 1997, and reflects an international trend in favor of the prohibition of child pornography, as confirmed by the recent adoption of the Optional Protocol to the United Nations Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, as well as the European Commission's recent initiative on combating the sexual exploitation of children and child pornography (COM2000/854).

4 This provision aims to strengthen protection measures for children, particularly against sexual exploitation, by modernizing criminal law to restrict more effectively the use of computer systems in the commission of sexual offences against children.

5 In the years following the adoption of the Convention on Cybercrime, child pornography and, more broadly, the sexual exploitation of children remained very important issues. This led to the drafting of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, adopted in Lanzarote on October 25, 2007. Art. 20 of this treaty is largely inspired by art. 9 CCC.

II. LEGALLY PROTECTED PROPERTY

Art. 9 CCC protects two different legal assets. Art. 9 § 2 let. a CCC directly protects the sexual integrity of children. As for art. 9 § 2 let. b and c CCC, they protect their sexual integrity indirectly by prohibiting any behavior which, without necessarily causing harm to the "child" represented in the material in question, could nevertheless encourage or incite children to participate in such acts. These provisions thus fall within the context of a subculture advocating child abuse. 6

III. BASIC CONSTITUENT ELEMENTS

A. A child pornographic representation

1. The medium of representation

Art. 9 CCC - like Art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse - refers exclusively to visual representations of child pornography. This includes all representations that can be perceived by sight, in particular photos, drawings, sketches, paintings, engravings, sculptures, videos and films. Audio recordings and texts are not covered. 7

Under the Convention on Cybercrime, repression is limited to visual representations in digital form. The medium on which they are recorded is irrelevant. It is therefore irrelevant whether they are stored on a hard disk, USB stick, DVD or even in the cloud. 8

2. Pornographic nature

The notion of pornography is not defined either in the Convention on Cybercrime or in the explanatory report. The Explanatory Report simply states that the concept must be interpreted in accordance with domestic law, which deals with the classification of representations as obscene, incompatible with public morality or otherwise having a perverse effect. 9

In Switzerland, pornography is defined as anything intended to arouse the consumer sexually, where sexuality is so detached from its human and emotional components that the person is reduced to a pure sex object to be disposed of at will. Sexual behavior is crude and overemphasized. Pornography 10

includes the insistent and repetitive representation of acts such as fellatio, cunnilingus and masturbation. This definition seems neither licentious nor particularly chaste. On the contrary, it seems balanced and can therefore easily be adopted internationally. The cardinal elements of this definition are also to be found in art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse - largely inspired by art. 9 CCC - which defines child pornography in paragraph 2 as any material that visually depicts a child engaged in real or simulated sexually explicit conduct, or any depiction of the sexual organs of a child for primarily sexual purposes. This definition can therefore be retained.

11 Although the text of art. 9 CCC does not expressly mention it, material of artistic, medical or scientific interest is not considered pornographic.

12 Determining what is artistic and what is not is complicated, especially in the context of an international convention concluded between states with very diverse cultures. In our opinion, artistic character must be assessed on a case-by-case basis. Generally speaking, however, it can be said that material must be qualified as artistic when the artist presents something in an original way, is intended to convey a message and is the fruit of genuine research. This is in contrast to a crude, trivial or vulgar representation of reality.

13 As for medical or scientific materials, these are necessary for training or research.

3. The notion of minor

14 Although the national laws of certain Parties to the Convention provide for a higher age of majority (e.g. Canada, Japan and the United States of America), the Parties agreed that the notion of a minor should in principle be taken to mean any person under the age of 18 (art. 9 § 3 CCC). As will be seen in section IV below, the Parties may, however, make reservations to require a lower age limit. In all cases, however, the age limit must be at least 16.

4. The notion of child pornography

15 Art. 9 § 2 CCC defines the notion of child pornography by providing a list of three types of punishable representations. This list is exhaustive.

16 The first type of depiction is that of a minor engaged in sexually explicit conduct. The term "sexually explicit conduct" refers above all to sexual relations,

including genital-genital, oro-genital, ano-genital or oro-anal. To be punishable under art. 9 § 2 let. a CCC, they must involve at least one minor. On the other hand, it is irrelevant whether they take place only between minors or with one or more adults. The gender or sexual orientation of each of the participants is also irrelevant.

The term "sexually explicit conduct", however, is broader than just sexual relations. It also includes zoophilia committed with a minor, masturbation of a minor, sado-masochistic violence in a sexual context committed on a minor, or lascivious exhibition of a minor's genitals or pubic area. 17

In all of the above cases, it is irrelevant whether the behavior depicted is real or simulated. The perpetrator cannot therefore escape conviction simply because the sexually explicit behavior did not actually take place. 18

The second type of representation covered by art. 9 § 2 CCC concerns pornographic images showing a person who appears to be a minor engaging in sexually explicit behavior (art. 9 § 2 let. b CCC). These are images depicting people who have just come of age, but who are being passed off as minors, or who are clearly of age, but who, through their clothing, make-up or accessories, give the appearance of minors. 19

Lastly, art. 9 § 2 let. c CCC refers to realistic images depicting a minor engaged in sexually explicit behavior. This last hypothesis concerns comic strips or mangas, photomontages or even images created from scratch by computers, as can be done by artificial intelligence. 20

B. Punishable conduct

Art. 9 § 1 CCC lists five punishable acts. This list is exhaustive. 21

The first is the "production", i.e. manufacture, of a child pornography representation with a view to disseminating it by computer. The term "production" encompasses all the acts required to produce representations of child pornography. This obviously refers primarily to the fixing of images on an image carrier. However, it also includes the preparation of the location and equipment needed to produce the images, the retouching of the images once they have been fixed on an image carrier, the editing of photographs or films, or even the creation of computer-generated images. In other words, this behavior covers all forms of visual media creation or editing. In all cases, however, the 22

material must be intended for computer distribution. The creation of digital images for one's own consumption is not punishable as production, but only as possession (art. 9 § 1 let. e CCC).

23 Art. 9 § 1 let. b CCC then punishes the offering or making available of child pornography via a computer system. The term "offer" refers to commercial conduct whereby the author informs his customers that he has one or more products available and proposes that they acquire them. The type of contract (sale, exchange, donation, etc.) is irrelevant. Making available" is a broader concept than "offering", as it does not necessarily mean that the author is taking any active steps to offer a product to his customers. In fact, it refers to any act that enables or facilitates access to a child pornography representation by computer. This includes putting child pornography online, for example by creating websites, as well as creating or compiling hyperlinks to sites containing child pornography.

24 Another punishable offence is disseminating or transmitting child pornography via a computer system. Both concepts refer to data transmission. Dissemination" is the distribution of child pornography to an indeterminate number of people who have not necessarily requested it. Transmission", on the other hand, is the sending of material to one or more specific persons who have requested it. The child pornography representation may be sent by any electronic means, including e-mail, instant messaging or peer-to-peer transfer.

25 Art. 9 let. d CCC also refers to "procuring child pornography by means of a computer system". This involves actively obtaining child pornography, for example by downloading. The data must therefore have been transferred to the author's computer system, or by the author to the computer system of a third party. There must be a transfer of possession. The data must be obtained by computer. Hand delivery or sending by post are therefore not covered by the convention.

26 Finally, the last punishable conduct is "possession of child pornography in a computer system or computer data storage medium" (art. 9 § 1 let. e CCC). The classic notion of possession presupposes both physical control over the object and a willingness to exercise this control. In the virtual world, the objective requirement of physical control over the object must, in our view, be relaxed in the sense that it is sufficient for the possessor to be freely able to access its data at any time. This is obviously the case if the data is stored on a

computer system belonging to the owner, on a data storage medium such as an external hard drive or USB stick, or on the memory card of a camera. However, the author is also in possession of the data if he saves it on a remote server to which he has access, or if he saves it in the cloud.

For some reason, the fact of consulting child pornography directly online, without appropriating it, has not been mentioned and is therefore not punishable. The absence of any mention of this conduct in the list in art. 9 § 1 CCC seems particularly surprising. Given the stated aim of combating child pornography, the repression of consumption seems just as important as criminalizing the production of child pornography. Fortunately, this oversight has been corrected in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Indeed, the explanatory report mentions that the conduct referred to in art. 20 para. 1 let. f is intended to enable prosecution of those who view images of children on child pornography sites but, by not downloading them, escape criminal prosecution. 27

C. Unlawfulness

The perpetrator must act without right. This constitutive element enables the Parties to create exceptions to criminal repression for authors acting in an interest worthy of protection, similar to artistic, medical or scientific interests. 28

This expression also makes it possible to exclude from the scope of art. 9 CCC prosecuting authorities who lawfully hold images of child pornography in the form of sequestration in the investigations they are investigating and trying. 29

The omnipresence of smartphones, even in the hands of minors, has led to a number of abuses. It is not uncommon these days for people - particularly among the younger generation - to send each other photographs of their private parts during the seduction phase. This practice poses a problem when the sender of such a photograph is a minor, as he or she produces child pornography by photographing his or her genital area, transfers it when sending it via an instant messaging system, and even possesses it if he or she keeps a copy on his or her smartphone. In this situation, the minor is paradoxically both perpetrator and victim of the offence punishable under art. 9 CCC. In the context of art. 9 § 2 let. a CCC, we believe that the Parties could provide 30

that a minor who takes a photograph with a sexual connotation of himself, transmits it or possesses it is not acting without right. On the other hand, the recipient of a mailing who asks to receive such an image, knowing the age of the sender, is clearly acting without right.

31 With regard to Art. 9 § 2 let. b CCC, the expression "without right" could also allow a Party to provide, for example, that a person is not punishable if it is established that the individual depicted is not "a minor" within the meaning of this provision.

D. Intention

32 The offence must be intentional. Intention must relate to all the objective elements of the offence. The perpetrator must therefore have the knowledge and intent to produce, offer, make available, disseminate, transmit, procure or provide to a third party, or to possess child pornography.

33 Parties may, however, adopt a more specific standard, in which case the latter would apply. Liability could, for example, be imposed if there is "knowledge and control" of the information transmitted or stored. It is not enough, for example, for a service provider to act as an intermediary for the transmission of this representation, via a website or chat room, among other means, in the absence of the requisite intent. Furthermore, a service provider is not obliged to monitor content to avoid criminal liability.

IV. RESERVATIONS

34 Art. 9 § 3 and 4 CCC allow Parties to restrict punishability in three different ways, namely in relation to the age of minors, punishable conduct and the objects of the performance.

A. With regard to the age of minors depicted

35 In the process of drafting the Convention, the Parties agreed that it was important to set the age of majority in a uniform manner. They therefore decided that the term "minor" should refer to any person under the age of 18. This limit was set in the light of the definition of "child" given in article 1 of the United Nations Convention on the Rights of the Child. It should be stressed, however, that this age refers to the exploitation of children as sexual objects. It must therefore be distinguished from the age of consent to sexual relations.

Given that some States have set a lower age limit in their national legislation concerning child pornography, the last sentence of paragraph 3 allows Parties to set a different age limit, which in any case must not be lower than 16. 36

The only State to have made use of this possibility is Switzerland. It has set the age limit at 16, in line with the wording of the former article 197, paragraphs 3 and 3bis of the Swiss Criminal Code. However, on June 16, 2010, Switzerland signed the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Article 20 of this convention punishes offences relating to child pornography. The notion of "child" mentioned therein is defined in art. 3 let. a as any person under the age of 18. As no reservation could be made with regard to the age limit, Art. 197 PC had to be adapted. The new wording of this provision came into force on July 1, 2014. It now corresponds to the general definition contained in art. 9 § 3 CCC. The reservation made by Switzerland at the time of ratification of the convention is therefore no longer relevant. 37

B. Punishable conduct

The Convention also authorizes Parties to restrict criminal prosecution by refusing to prosecute the procurement or provision to a third party of child pornography images and/or the possession thereof. 38

At the time of ratifying the convention, Ukraine, Japan and Sri Lanka made use of this possibility not to prosecute obtaining and possessing child pornography. In 2014, Japan amended its legislation and penalized possession of child pornography, as well as procuring it for others. Obtaining it for oneself, however, is still not punishable. 39

Israel specified that it refused to prosecute the obtaining of child pornography. 40

Argentina stated that possession of child pornography was not punishable under its national law. 41

Other States have expressed reservations regarding the punishability of obtaining or possessing child pornography under certain specific conditions. 42

Denmark, for example, has declared that it will not punish the possession of pornographic images involving children aged at least 15, if the minor concerned has consented to such possession. 43

44 At the time of ratification of the Convention, Montenegro specified that obtaining and possessing child pornography was not punishable when the person appearing in such material was at least fourteen years old and had given his or her consent. This exception has since been abolished.

C. Objects of representation

45 Finally, the Convention allows Parties to limit criminal prosecution by refusing to consider as unlawful images depicting a person who appears to be a minor engaged in sexually explicit conduct and/or realistic images depicting a minor engaged in sexually explicit conduct.

46 The Principality of Andorra, Great Britain, Argentina, Chile, the United States of America, Japan, Peru and Sri Lanka have declared that they will not prosecute the representations mentioned in art. 9 § 2 let. b and c CCC. At the time of ratification of the Convention, Iceland had entered a reservation to the same effect. This reservation no longer applies, however, as the Act of June 25, 2012 introduced a new Art. 210a into the Icelandic Penal Code, which also punishes the representations referred to in Art. 9 § 2 let. b and c CCC.

47 Denmark, Hungary, Montenegro, Switzerland and Israel have indicated that they will refrain from punishing visual depictions of a person who appears to be a minor engaging in sexually explicit behavior (art. 9 § 2 let. b). France entered a similar reservation, stating that it would not prosecute images depicting a person who is of age at the time the image is taken, but who appears to be a minor and is engaged in sexually explicit behavior.

V. COMPARISON WITH SWISS LAW

48 The conduct and the various representations punishable under the Convention find their equivalent in Swiss law in art. 197 paras. 4 and 5 of the Swiss Criminal Code. Swiss law fully complies with art. 9 CCC.

BIBLIOGRAPHY

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

Trechsel Stefan/Crameri 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

MATERIALS

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)

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 11 CCC (Convention on Cybercrime)

A commentary by Julian Mausbach

SUGGESTED CITATION

Julian Mausbach, Commentary of art. 11 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Mausbach, Art. 11 CCC N. XXX.

Title 5 Ancillary liability and sanctions

Article 11 Attempt and aiding or abetting

[1] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

[2] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.

[3] Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

CONTENT

I. Scope of application 122
II. Criminal liability for participation (Art. 11 para. 1) 122
III. Attempted criminal liability (Art. 11 para. 2 and para. 3) 123
Materials 124

I. SCOPE OF APPLICATION

1 The purpose of Art. 11 is to establish the principle of criminal liability for attempt and participation in relation to the offenses defined in the Convention. Para. 1 assumes that intentional participation in an intentional criminal offense pursuant to Art. 2-10 is punishable and sanctionable both in the sense of aiding and abetting and incitement.

2 Para. 2 already limits this to Art. 3-5 as well as Art. 7, 8 and 9 para. 1 lit. a and c of the Convention. This limitation of attempted criminal liability to the listed offenses can be implemented by the contracting parties in such a way that attempted criminal liability is waived in whole or in part (para. 3).

3 Switzerland has not made use of the possibility of limiting para. 3 and therefore provides for attempted criminal liability by linking it to the General Part of the Criminal Code.

II. CRIMINAL LIABILITY FOR PARTICIPATION (ART. 11 PARA. 1)

4 Art. 11 para. 1 provides for criminal liability for participation for Art. 2-10. Unlike in the General Part of the SCC (Art. 24 and 25 SCC), no distinction is made between incitement and aiding and abetting. Since the implementation of para. 1 was carried out directly via the provisions of the General Part of the SCC, the form taken there, for example with regard to attempted criminal liability (Art. 24 para. 2 SCC), also applies to the scope of application of the Convention and the corresponding implementation. Objective requirements that go beyond Art. 24 and 25 SCC are not given and therefore the implementation via these articles is also congruent here.

5 The double intent to participate provided for in para. 2 with regard to the act of participation and the main offense is also required by the provisions of the General Part, so that no additions were necessary here.

6 Reference should be made to the addition to the criminal provision of Art. 143bis SCC. For details, please refer to the corresponding commentary on Art. 6. With regard to the question of participation and attempt, it should be emphasized that even after the addition of Art. 143bis SCC, attempted aiding and

abetting of a principal offence that has not (yet) been attempted remains unpunishable.

III. ATTEMPTED CRIMINAL LIABILITY (ART. 11 PARA. 2 AND PARA. 3)

Para. 2 provides for the obligation to extend attempted criminal liability to the named provisions. Neither objective criteria are mentioned, nor is a general attempt punishability provided for. The latter in particular is due to the fact that the legal systems of some contracting parties do not stipulate a general, but a graduated attempted criminal liability. The provision thus promises an implementation option that can be (and has been) implemented without major distortions in the fundamental legal concepts of the contracting states. 7

The implementation of attempted criminal liability was carried out via Art. 22 in conjunction with Art. 10 para. Art. 10 para. 2 and para. 3 SCC. It thus extends to all of the offenses named in para. 2. This follows from the fact that their implementation is in turn carried out by means of criminal offences in the Special Part of the SCC, which are themselves at least offences within the meaning of Art. 10 para. 2 SCC. 8

Although para. 2 does not contain any obligation to extend the criminalization of attempts to provisions not named in para. 2, the implementation via articles of the Criminal Code means that there is also criminalization of attempts in Switzerland with regard to Art. 2, Art. 9 as a whole and Art. 10 CCC. In particular, by including the documentary offenses (Art. 251 et seq. SCC), the offenses for the protection of postal and telecommunications secrecy (Art. 321ter SCC) and the pornography article (Art. 197 SCC), which in turn are at least structured as misdemeanors, an implementation took place that entails attempted criminal liability for Art. 2-10. Therefore, there is no dissonance with the principle of attempted punishment for misdemeanors and felonies in Swiss criminal law. 9

Para. 3 provides for the possibility of the contracting parties to waive attempted criminal liability in whole or in part. This provision is intended to counter any implementation difficulties on the part of the contracting parties. The scope for implementation granted in this way should, where possible, allow ratification to take place without fundamental changes to the respective legal system. In Switzerland, no use has been made of this possibility, not even with 10

regard to individual elements or parts thereof. This is convincing in terms of content, as it does not involve a break with the understanding of attempted criminal liability in Switzerland. The provision in para. 3, which is ultimately to be understood as a concession to the practicability of implementation with regard to the legal systems of the contracting parties, has therefore been left without consequence in Switzerland.

MATERIALS

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)

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 12 CCC (Convention on Cybercrime)

A commentary by Ugur Gürbüz

SUGGESTED CITATION

Ugur Gürbüz, Commentary of art. 12 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Gürbürz, art. 12 CCC N. XXX.

Article 12 – Corporate liability

[1] Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a. a power of representation of the legal person;

b. an authority to take decisions on behalf of the legal person;

c. an authority to exercise control within the legal person.

[2] In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

[3] Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

[4] Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

CONTENT

I. Introduction 128
II. Scope of application and objectives 128
A. Paragraph 1: For acts committed by persons in a leadership position 129
B. Paragraph 2: Breach of the duty of supervision 130
C. Paragraph 3: Type of responsibility 131
D. Paragraph 4: Individual liability 131
III. Comparable criminal law norms in Switzerland 131
A. Criminal sanctions and measures under the SCC 131
B. Art. 102 para. 1 SCC: Subsidiary liability 132
C. Art. 102 para. 2 SCC: Primary liability 133
D. Provisions in administrative criminal law 134
1 Art. 6 VStrR: Principal's liability 134
2 Art. 7 VStrR: Corporate liability 135
IV. Implementation of the criminal law aspect in Switzerland 135
V. Comparable civil and administrative law standards in Switzerland 136
VI. Implementation of the civil and administrative law aspect in Switzerland 137
Bibliography 138
Materials 138

I. INTRODUCTION

1 For decades, the principle of "**societas delinquere non potest**", which originated in Roman law, was regarded in continental Europe as an immutable rule that focused criminal law on the individual and exempted companies from criminal liability. This notion of a legal system without direct corporate criminal liability became obsolete as the economy became increasingly characterized by more complex business structures and global divisions of labour, thereby increasing the potential for abuse and the danger and harmfulness of any corporate misconduct. In Europe, the Netherlands in 1976, France in 1994 and Denmark in 1996 implemented corporate criminal liability in their criminal codes. In Switzerland, corporate criminal law has been regulated in the Criminal Code since October 1, 2003, but Switzerland is still considered one of the pioneering countries internationally when it comes to the introduction of criminal liability for legal entities. Even before its introduction in the Criminal Code, Articles 6 and 7 of the Administrative Criminal Law Act (VStrR) could be invoked from 1974 in the case of infringements in business operations in accordance with Art. 26 UWG (Federal Act against Unfair Competition). However, these provisions were regarded as exceptions to the then generally recognized principle that legal persons are not liable to prosecution and were not included in criminal law.

2 As part of the intended effectuation of criminal prosecution with the introduction of the Cybercrime Convention of the Council of Europe, the contracting parties were - following the **European trend** - given identical rules on the liability of legal persons in Art. 12 CCC as in the largely identical criminal law provisions of the Criminal Law Convention on Corruption, namely to provide for liability for infringements by their bodies and other employees. The contracting states were also obliged under Art. 12 CCC to ensure that legal persons are subject to appropriate sanctions or measures, including monetary sanctions. The principle that companies cannot make themselves liable to prosecution was also protected by the Cybercrime Convention.

II. SCOPE OF APPLICATION AND OBJECTIVES

3 The **liability of legal entities** pursuant to Article 12 aims, on the one hand, to hold companies liable for criminal acts committed by persons in a manage-

rial position, provided that these acts are carried out for the benefit of the legal entity (paragraph 1). On the other hand, the provision provides for liability for persons in a managerial position who have failed to supervise or control employees or agents and this failure facilitates an offense by employees or agents as defined by the Convention (paragraph 2). The Convention leaves it to the contracting parties to decide whether they wish to regulate the liability of the legal person under civil, administrative or criminal law (paragraph 3). It also states that the liability of a legal person shall not prevent the possible criminal liability of a natural person who has committed the offense (paragraph 4).

A. Paragraph 1: For acts committed by persons in a leadership position

Art. 12 para. 1 CCC obliges the contracting parties to establish the liability of the legal person for offenses committed by persons with a leading position within the company or who participate in them as instigators or accomplices. The provision establishes **causal liability** and comprises **four elements**: 4

a) The Convention requires a **violation of the criminal norms formulated in Articles 2-10 of the Convention**, namely unlawful access (Art. 2), unlawful interception (Art. 3), interference with data (Art. 4), interference with a system (Art. 5), misuse of devices (Art. 6), computer-related counterfeiting (Art. 7), computer-related fraud (Art. 8), offenses related to child pornography (Art. 9) and infringement of copyright and related rights (Art. 10). 5

b) Criminal liability under the Convention text is limited to offenses **committed for the benefit of the legal person**. The criterion "for the benefit of*the*legal person" establishes a link between the offense and the legal person. The scope of application is limited to criminal offenses that are committed for the benefit of a legal entity. This benefit can be financial or otherwise. Direct financial advantages include, among other things, proceeds that are obtained from criminal offenses and either enrich the legal entity or save it an expense. A benefit of another kind exists if the benefit to the legal entity is not (primarily) financial, for example if the legal entity receives orders as a result of bribery. The Convention does not contain a legal definition of the term legal entity. In defining Article 12, the historical and European interpretation of the term "legal person" was used, according to which it includes any legal entity that has the status of a legal person under the applicable law, with the excep- 6

tion of states or other public bodies in the exercise of sovereign rights and public international organizations.

7 c) In accordance with the principles of private law that legal persons can only act through their organs, that the acts of the organs are direct acts of the legal person and that the legal person is liable for the acts of the organs vis-à-vis injured third parties, the Convention presupposes the **commission of the offense by a natural person** who holds a **leading position** within the legal person. According to the list in lit. a to c, this includes those natural persons who derive their management and leadership function from a power of representation, decision-making or control. The Convention text thus requires the liability of legal persons to be defined as a special offense, without presupposing a formal executive function on the part of the perpetrator.

8 d) Furthermore, the Convention requires the contracting states to ensure that the natural person acts within the scope of the authority vested in him in the **performance of an authorized business activity**, i.e. within the scope of the power of representation, decision-making or control vested in him in the legal person, in order to trigger the liability of the legal person pursuant to Art. 12 para. 1 CCC.

B. Paragraph 2: Breach of the duty of supervision

9 Art. 12 para. 2 CCC obliges the contracting states to hold companies accountable

a) if the natural persons named in para. 1 lit. a to c **violate their duty to supervise** subordinate employees **through a lack of supervision and control**,

b) who then commit a criminal offense as a causal consequence of this violation within the meaning of **Art. 2-10 CCC**

c) for the **benefit of the legal person** .

10 Paragraph 2 thus extends the liability of the legal entity to acts committed by persons who commit an offense as employees **without a management position** in the legal entity and the offense was made possible by the fact that the manager did not adequately supervise the subordinate employee.

Failure to supervise can be assumed if suitable and appropriate measures were not taken to prevent criminal acts in favor of the legal entity by employees or agents. The type and intensity of the duty of supervision depends on the type of company, its size, security standards and business practices. The duty of supervision does not give rise to a general monitoring obligation. 11

C. Paragraph 3: Type of responsibility

Art. 12 para. 3 CCC was included in the Convention in order to take into account the national legal principles of the contracting states as far as possible. According to this provision of the Convention, the **liability of legal persons** may be **criminal, civil or administrative**. When regulating accordingly, States Parties must ensure that their criminal or non-criminal sanctions or measures against legal persons meet the criteria of Art. 13 para. 2 CCC, according to which they must be effective, proportionate and dissuasive and include monetary sanctions. 12

D. Paragraph 4: Individual liability

Art. 12 para. 4 CCC clarifies that the liability of legal persons **does not exclude the individual liability of a natural person**. This provision does not oblige the contracting states to introduce parallel criminal liability. 13

III. COMPARABLE CRIMINAL LAW NORMS IN SWITZERLAND

A. Criminal sanctions and measures under the SCC

Corporate criminal liability was introduced into the Swiss Criminal Code on October 1, 2003. The motives for this were the fear of organized crime, the fear of man-made major dangers and the signing of the "Convention on Combating Bribery of Foreign Public Officials in International Business Transactions". By ratifying this **OECD Convention**, Switzerland undertook, in accordance with Art. 2, to take the necessary measures to establish the liability of legal persons for the bribery of a foreign public official in accordance with its legal principles. 14

B. Art. 102 para. 1 SCC: Subsidiary liability

15 According to Art. 102 para. 1 SCC, felonies or misdemeanours - but not misdemeanours - are attributed to a company if a felony or misdemeanour is committed in the "company in the exercise of business activities within the scope of the company's purpose" and "this act cannot be attributed to a specific natural person due to deficient organization of the company". The company is therefore liable to subsidiary prosecution in the event of defective **organization**.

16 The accusation directed against the company is that

a) a **felony or misdemeanor** under Swiss law within the meaning of Art. 10 SCC was committed **as an instigating offence**

b) the offence was committed **within a company** and the offender must be hierarchically or organizationally integrated into the company

c) the predicate offense was committed "**in the course of business**", which requires a functional connection between the predicate offense and the business activity, i.e. a minimal economic activity that is related to the activities of the company and thus includes the action with power of representation, decision-making or control required in Art. 12 CCC,

d) the offense was committed **within the scope of the purpose of the company**, which, according to the prevailing opinion, justifies a restriction to typical company risks,

e) and the company is responsible for the fact that the criminal prosecution authorities are **unable to** identify a **responsible natural person** due to inadequate organization.

17 As long as the responsibility of legal persons

- on the one hand, in accordance with Art. 12 para. 1 of the Convention, the aim is to hold companies liable for criminal acts committed by persons in a managerial position, provided that these acts are carried out for the benefit of the legal person,

- and on the other hand, according to Art. 12 para. 2 CCC, persons in a managerial position who have failed to supervise or control employees or agents and this failure facilitates an offense by employees or agents as described in the Convention,

both types of offense find a far-reaching equivalent in the subsidiary corporate liability under criminal law pursuant to Art. 102 para. 1 SCC. The provision covers **all offenses under the Cyber Convention** without explicitly enumerating them.

The Convention is limited to offenses under Art. 2-10 CCC that are committed for the benefit of the legal entity and by its representatives. Liability under the SCC, on the other hand, applies to any crime or misdemeanor committed by a person in the course of business within the scope of the corporate purpose. Compared to the Convention text, liability under the SCC thus extends further because the SCC **does not require a criminal offense committed for the benefit of the legal entity as a criterion** for corporate liability. 18

Art. 102 para. 1 SCC, according to which the legal person can only be punished if the act cannot be attributed to a natural person, and Art. 12 para. 4 CCC, according to which the criminal liability of the legal person should not affect the liability of the perpetrator, do not contradict each other because **criminal liability of the natural persons acting is not excluded by the subsidiary corporate liability**. In Switzerland, it is even possible to punish the natural person as well as the legal entity if the defective organization of the company is the fault of a natural person and this person can only be identified after the company has been convicted. 19

Art. 102 para. 1 SCC provides for a **fine of up to five million Swiss francs** as a penalty, which corresponds to the Convention text of Art. 13 para. 2, according to which states parties must impose monetary sanctions. 20

C. Art. 102 para. 2 SCC: Primary liability

Irrespective of the criminal liability of natural persons, since 1.10. 2003, a **company is primarily held liable** if it commits an offence under Articles ^{260ter} SCC (criminal organization), ^{260quinquies} SCC (financing of terrorism), ^{305bis} SCC (money laundering), ^{322ter} SCC (bribery of Swiss public officials), ^{322quinquies} SCC (granting of advantages), ^{322septies} paragraph 1 SCC (bribery of foreign public officials) or ^{322octies} SCC (bribery) and the company has not tak- 21

en all necessary and reasonable organizational precautions to prevent such an offence. The **breach of duty** lies in the disregard of organizational duties that facilitate the offences listed exhaustively. Punishment is imposed in accordance with Art. 102 para. 2 SCC in addition to any punishment of a natural person.

22 None of the offenses under Art. 2-10 CCC are included in the catalog of offenses under Art. 102 para. 2 SCC, which is why the liability of legal persons under Art. 12 CCC remains meaningless in relation to primary criminal corporate liability. It follows that, in accordance with the existing legal provisions, **no direct attribution of third-party fault to a company is possible** in Switzerland in connection with the criminal norms formulated in Art. 2-10 CCC.

D. Provisions in administrative criminal law

23 Before the introduction of corporate criminal liability and the attribution provision (Art. 29 SCC) in core criminal law and also before ratification of the Cybercrime Convention, natural and legal persons in Switzerland were held liable for offenses in business operations under the Federal Act on Administrative Criminal Law. Corresponding provisions in administrative criminal law **continue to apply**: Art. 6 VStrR punishes natural persons who have a special relationship to the business operation. Art. 7 VStrR deals with the criminal liability of legal persons. Overlaps between the provisions of the SCC and the VStrR are possible. Art. 6 and 7 VStrR are applicable as long as laws either explicitly refer to one of the provisions or to administrative criminal law as a whole.

1 Art. 6 VStrR: Principal's liability

24 The subject of criminal liability under Art. 6 VStrR is always an **individual person**. If offences are committed in the course of managing the affairs of a legal entity, general or limited partnership, sole proprietorship or partnership without legal personality or otherwise in the performance of business or official duties, paragraph 1 states that the criminal provision applies to the natural person who committed the offence. Paragraphs 2 and 3 specify that the principal, employer, principal, representative or even the organ and member of the organ, the managing partner, liquidator and the person actually in charge are to be held liable as long as they have intentionally or negligently failed to

avert an infringement by the subordinate, agent or representative or to nullify its effects in breach of a legal duty. Article 6 is an offense of omission in violation of a legal duty. The administrative criminal liability of the principal arising from Article 6 considerably limits the scope of the subsidiary criminal liability of the company pursuant to Art. 102 para. 1 SCC and leads to the exoneration of the company because it enables the attribution to a natural person.

2 Art. 7 VStrR: Corporate liability

Art. 7 VStrR provides for subsidiary criminal liability of the legal person in administrative criminal law. The provision aims to reduce the investigative effort of the prosecution authorities **in the case of minor offenses** in accordance with the moderate opportunity principle. At the same time, it contradicts the principle of investigating the material truth and the principle of legality. According to Art. 7 VStrR, the prosecution of a natural person can be dropped and the legal entity, general or limited partnership or sole proprietorship can be sentenced to pay a fine in their place if the following conditions are met: 25

a) the offense is committed in the course of business

b) a maximum fine of CHF 5,000.00 is possible and

c) the investigation of the individual perpetrator would entail a disproportionate investigation effort.

If a natural person is identified as the perpetrator, the application of Art. 7 VStrR is excluded. The provision also does not replace Art. 102 para. 1 SCC in administrative criminal law. Due to their different regulatory content, both standards can be applied.

IV. IMPLEMENTATION OF THE CRIMINAL LAW ASPECT IN SWITZERLAND

Due to the **extensive coverage of the content of the Convention** by Art. 102 para. 1 SCC, the legislator has rightly refrained from imposing primary corporate criminal liability in connection with Art. 12 CCC and the associated extension of the scope of application. Although the Convention enshrines a parallel responsibility of the company, which in Switzerland can only be en- 26

sured at the criminal law level through primary criminal corporate liability in accordance with Art. 102 para. 2 SCC, it does not require the contracting states to regulate the criminal liability of companies. Article 12 of the Convention does not require the creation of a criminal provision in the narrower sense; rather, in para. 3, it leaves it to the contracting states to regulate the liability of the legal person under civil or administrative law as an alternative. Since the subsidiary liability under Art. 102 para. 1 SCC covers all offenses under Articles 2-10 CCC, especially since it ensures that crimes and offenses committed for the benefit of a company do not go unpunished, the legislator correctly assumed that a more comprehensive primary liability would go beyond the minimum required by the Convention. Due to Art. 2 VStrR, according to which the provisions of corporate criminal law of the SCC also apply to administrative criminal law, unless the VStrR itself or the individual administrative law provides otherwise, but also due to Art. 7 VStrR, according to which staff associations can be punished instead of individual offenders who are difficult to identify, the liability of legal persons is also ensured in the case of criminal offenses for violations of federal laws such as the Copyright Act.

27 **Contrary** to the wording and purpose of Art. 12 para. 1 CCC, the Swiss legislator has not designed Art. 102 SCC as a causal liability provision. While Art. 12 para. 1 CCC states that a legal person bears the risk of liability for a tort within the company regardless of fault, Art. 102 SCC presupposes organizational fault for the criminal liability of the legal person. Despite this difference, Switzerland nevertheless complies with the requirements of Art. 12 CCC because "liability" within the meaning of the Convention does not necessarily mean criminal liability of the legal person (cf. Art. 12 para. 3 CCC).

V. COMPARABLE CIVIL AND ADMINISTRATIVE LAW STANDARDS IN SWITZERLAND

28 The Swiss legal system recognizes various instruments of liability for damages and the prevention of future harm under civil and administrative law. In addition to the **liability regulations and organizational measures** in civil law, reference should also be made to the **supervisory instruments** of the authorities.

Specifically, these instruments include the following (not exhaustive): 29

- Dissolution of the association by the court in accordance with Art. 78 CC if the purpose of the association is unlawful or immoral;
- Dissolution of the foundation by the competent federal or cantonal authority in accordance with Art. 88 CC if the purpose of the foundation has become unlawful or immoral;
- Liability of the company arising from principal's liability pursuant to Art. 55 CO;
- Liability of the company for auxiliary persons pursuant to Art. 101 CO;
- Liability of the company for damages arising from tortious acts committed by a shareholder in the performance of business activities pursuant to Art. 567 para. 3 CO;
- Liability of the company for damages arising from tortious acts committed by a liquidator in the performance of business duties pursuant to Art. 586 CO and Art. 743 CO;
- Liability of the company for damages arising from tortious acts committed by a person authorized to manage or represent the company in the performance of their business duties pursuant to Art. 722 CO and Art. 817 CO;
- Dissolution of the company in the event of existing deficiencies in the organization pursuant to Art. 731b CO;
- Liability of the cooperative for damages arising from unlawful acts committed by a person authorized to manage or represent the company in the course of their business activities pursuant to Art. 899 CO;
- Administrative sanctions imposed by the Swiss Financial Market Supervisory Authority in accordance with the Financial Market Supervision Act.

VI. IMPLEMENTATION OF THE CIVIL AND ADMINISTRATIVE LAW ASPECT IN SWITZERLAND

Swiss civil and administrative law provides for a **large number of sanctions and measures** against companies for unauthorized acts in the course of a business. As long as companies are managed to operate a business and not exclusively to commit criminal offenses, the sanctions and measures under civil 30

and administrative law are generally sufficient to ensure the effective and dissuasive sanctions required by Art. 13 para. 2 CCC.

BIBLIOGRAPHY

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.

MATERIALS

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.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 16 CCC (Convention on Cybercrime)

A commentary by Ugur Gürbüz

SUGGESTED CITATION

Ugur Gürbüz, Commentary of art. 16 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Gürbüz, art. 16 CCC N. XXX.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

[1] Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

[2] Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and

maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

[3] Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

[4] The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

CONTENT

I. Introduction 144
II. Scope and objectives 144
A. Para. 1: Immediate securing of computer data 145
B. Paragraph 2: Preservation of data by means of a preservation order 146
C. Paragraph 3: Duty of confidentiality 147
D. Paragraph 4 147
III. Implementation in Switzerland 147
A. Securing by law enforcement authorities 148
B. Request for preservation from individuals 149
C. Lack of legal provisions regarding orders to retain data 149
D. Securing of data blocked by the Federal Supreme Court despite valid application for sealing 151
Bibliography 152
Materials 152

I. INTRODUCTION

1 The fact that professional and skilled cybercriminals are increasingly using the latest technologies and the internet for their illegal purposes poses growing challenges for authorities. However, the technical possibilities for abuse do not guarantee permanent and absolute security for criminals as long as authorities take targeted action. This is because **traces are left behind on data carriers and on the internet**: every action carried out online, such as visiting a website, posting on social media, or shopping online, generates data that can be stored and tracked. By creating images of seized data carriers, deleted and unoverwritten data can be recovered. Such data, even if only stored temporarily, can be useful to law enforcement agencies in investigating crimes, solving crimes, or carrying out surveillance measures, provided it is secured in a timely manner.

2 Whether **computer data** has been **stored** and is still **available** at the time of the ongoing investigation depends, on the one hand, on the deletion behavior of the data owner and, on the other hand, on the data protection regulations of the respective contracting state.

II. SCOPE AND OBJECTIVES

3 Due to their volatile nature, computer data is easy to manipulate, modify, and delete. The risk of data loss or destruction is therefore high in practice. In order to ensure that the securing of such computer data and connection data in domestic criminal proceedings does not depend on lengthy evidence-gathering processes, but rather to prevent the deletion and alteration of evidence-relevant data in a timely manner by means of a preservation order through swift and effective measures, thereby increasing the effectiveness of the prosecution of the offenses described in more detail in the Cybercrime Convention, the Contracting States have undertaken to take the necessary legislative measures at the domestic level. The procedure for securing stored computer data immediately and in a timely manner is known in practice as the "**quick freeze procedure**." The quick freeze procedure should not be confused with the immediate securing of data in a cross-border context, known as a preservation request, which is regulated in Article 29 CCC.

Art. 16 CCC regulates the **immediate securing of data**, but does not entitle the contracting states per se to order the disclosure of the data or to view its content unless expressly permitted by domestic law. The disclosure of data is regulated in Art. 18 CCC, while search and seizure are dealt with in Art. 19 CCC. 4

A. Para. 1: Immediate securing of computer data

Art. 16 para. 1 CCC guarantees the rapid securing of computer data within a contracting state in order to counteract the risk of obfuscation due to the volatility of computer data. Data should be protected "*from anything that would cause its current quality or condition to change or deteriorate*" and thus comprehensively protected against changes, deterioration or deletion. Preservation refers to the **temporary storage of data** and not the denial of access to the data. Legitimate users should continue to be able to use the data or copies thereof as long as they are not subject to seizure under Art. 19 CCC. 5

Art. 16 CCC does not oblige Contracting States to restrict the provision or use of services or to introduce new technical means for the storage and collection of data. The provision therefore does not lead to an obligation to retain data. It is merely intended to ensure that contracting states can arrange for the **accelerated securing** of stored computer data at the national level in order to support each other at the international level. 6

The specific **form of** the safeguards is left to the contracting parties. In practice, two options are available as safeguarding methods: safeguarding the original data and creating identical copies of the data. 7

According to the wording of Art. 16 para. 1 CCC, the safeguarding concerns "*certain computer data, including traffic data, stored by means of a computer system*." This covers all types of computer data that have already been collected and stored by data owners or service providers, known as "**stored computer data**." Connection and traffic data, known as "traffic data," are also explicitly mentioned. The reference to traffic data serves to establish a link between the measures in Art. 16 and Art. 17 CCC. The latter provision provides for certain special features for traffic data. Future-oriented real-time collection of computer data and data retention are not covered. These are regulated in Articles 20 and 21 CCC. 8

The securing of data may be ordered or effected in a similar manner. 9

a) "**Ordering**" includes both a court or official order to secure data and an obligation on the part of the addressee of the order to actively cooperate. The latter is to be achieved by the addressee of the order securing the data unchanged and without loss (see Art. 16 para. 2 CCC).

b) The wording "**or effect in a similar manner**" allows the Contracting States to organize the preservation of data flexibly and with their own resources in accordance with their procedural law.

10 Preservation measures should be specified by the Contracting States in particular where there is reason to believe that computer data are particularly **susceptible to loss or alteration**. This may refer, for example, to situations where the data are subject to a short retention period in accordance with business policy, are deleted at regular intervals or are stored in an insecure manner.

B. Paragraph 2: Preservation of data by means of a preservation order

11 Art. 16 para. 2 CCC stipulates that in cases where computer data is preserved pursuant to Art. 16 para. 1 CCC by order against another person, the Contracting States may take measures and introduce "**preservation orders**" to ensure the integrity of such computer data for a limited period of time. However, Contracting States are not obliged to take such measures. Contracting States must ensure that their investigating authorities – regardless of the procedure chosen – can order or effect immediate/prompt preservation.

12 Persons who are either in possession of stored computer data or who have control over the data are considered to be **addressees of orders**.

13 The Contracting States may, in their domestic law, as a measure within the meaning of Art. 16 para. 2 CCC, oblige the addressees of the order to preserve the integrity of the computer data that is the subject of the order for as long as necessary, but for no longer than 90 days. However, they may also provide for an extension of this **retention period**. The setting of a time limit as a measure serves to give the competent authorities sufficient time to obtain the necessary authorizations and to initiate legal steps such as search, seizure, securing, or issuing a surrender order, so that they can then, in a second step, obtain knowledge of the content of the data, in particular also within the framework of mutual legal assistance within the meaning of Art. 29 CCC.

C. Paragraph 3: Duty of confidentiality

Art. 16 para. 3 CCC requires the contracting states to take the necessary legislative measures to ensure that, in the event of an order addressed to the **depositary or a third party**, they are obliged to carry out the data preservation in a confidential manner for a period specified in domestic law. This measure takes into account, on the one hand, the requirements of the law enforcement authority that suspects and third parties cannot learn of the investigations and, on the other hand, protects the privacy of the persons concerned, in particular those who are mentioned or identifiable in the data. 14

D. Paragraph 4

Through the **references** in Art. 16 para. 4 CCC, the Contracting States undertake to ensure that the powers and procedures referred to in Art. 16 CCC are subject to the conditions and safeguards laid down in Art. 14 and Art. 15 CCC. 15

III. IMPLEMENTATION IN SWITZERLAND

The securing of stored computer data in accordance with Art. 16 CCC is an important **investigative tool** for combating computer and IT-related crime. The Contracting States – including Switzerland – are obliged to create the necessary legislative and organizational framework conditions for this. 16

Switzerland has not incorporated the "quick freeze procedure" provided for in Art. 16 CCC as a separate measure into the applicable Swiss Criminal Procedure Code. Instead, **Swiss law** already complies with the requirements of Art. 16 CCC in general in that **providers of telecommunications services** are obliged, on the one hand, **pursuant to Art. 21 para. 2 and Art. 22 para. 2 BÜPF**, to ensure that identification data is collected when the customer relationship is established and that this data remains accessible throughout the customer relationship and for six months after its termination, and, on the other hand, **pursuant to Art. 26 para. 5 BÜPF**, to store edge data for six months. 17

Even when considered specifically, the applicable Swiss law meets the requirements of the Convention provision under Art. 16 CCC. Under the Swiss Criminal Procedure Code, computer data can either be secured by a written order of the public prosecutor's office in the context of a search under **Art.** 18

246 ff. CrimPC or added to the case file by means of a disclosure order under **Art. 265 CrimPC**. The securing of stored computer data in Switzerland can be divided into two categories: securing by law enforcement authorities and requests for securing to individuals. Both measures may also be taken by the police without a public prosecutor's order if there is imminent danger, thereby ensuring that stored computer data is secured in an expedited and proportionate manner.

A. Securing by law enforcement authorities

19 In Switzerland, temporary securing of data material is ordered by the public prosecutor's office (or, where applicable, the court hearing the case) in accordance with Art. 198 in conjunction with Art. 241 para. 1 and **Art. 246 CrimPC** in order to search records. This order ensures that data can be examined in terms of its content or nature in order to determine its admissibility as evidence and, if necessary, to seize it. Such searches and the securing of data are ordered by the police in accordance with Art. 312 CrimPC. The police then carry out a search in accordance with the instructions of the public prosecutor's office (or the court hearing the case) and either take the data carrier with them for safekeeping or make a forensic copy of the data stored on the data carriers found and to be searched (known as “data mirroring”). Mirroring ensures that data is copied to an external data carrier and protected against manipulation. In economic criminal proceedings in particular, this ensures that data within the meaning of Art. 16 para. 1 CCC can be secured immediately. On the other hand, this allows the persons affected by the search to continue using their devices to carry out their business activities, taking into account the principle of proportionality, as long as the devices do not have to be seized for the purpose of confiscation in accordance with Art. 263 CrimPC in conjunction with Art. 69 para. 1 SCC.

20 In order to ensure the **security of data on digital servers or in the cloud**, it is essential to immediately create a data mirror on site to prevent this data from being altered or deleted through alternative means of access. The legal basis for making copies of such records and data in the context of a search is Art. 247 para. 3 CrimPC.

B. Request for preservation from individuals

With regard to the search and seizure of data material, the public prosecutor's office (and, where applicable, the court of jurisdiction) also has the option, within the meaning of Art. 263 and Art. 265 CrimPC, to order the surrender and seizure of data by means of an order namely to specifically oblige the owner, under threat of punishment under Art. 292 SCC and within a specified period, to surrender the electronic data carriers and data in the original or in copy as evidence. This process is referred to as **edition** and **editing**. However, such an order to surrender data is only possible if the holder is not the accused person, a person with the right to refuse to give evidence or a company that could be held criminally or civilly liable if the data were surrendered (Art. 265 para. 2 CrimPC). A further prerequisite for issuing an order to produce evidence is that the order must be addressed to the actual holder of the data with a Swiss domicile, otherwise the route of international mutual assistance in criminal matters must be pursued. 21

If a person is obliged under Art. 2 BÜPF as the data holder to transmit the peripheral data available to them on a person under surveillance, Art. 269 ff. CrimPC apply. Provided that the conditions under Art. 269 para. 1 lit. b and c CrimPC are met and approval has been obtained from the coercive measures court, seizure based on Art. 263 CrimPC is not an option, but **telecommunications service providers** based in Switzerland, as owners of the peripheral data, may be required to back up the data in accordance with Art. 273 CrimPC. The procurement of inventory data is not a coercive measure and does not require the approval of the coercive measures court. 22

C. Lack of legal provisions regarding orders to retain data

In Switzerland, only telecommunications service providers are required by law to retain identification and peripheral data for a period of six months in accordance with Art. 2 BÜPF. In connection with this stored data, various federal and cantonal authorities are granted the right under **Art. 15 BÜPF** to obtain information on telecommunications services under Art. 21 BÜPF and on the identification of perpetrators under Art. 22 BÜPF. Such disclosure of information is equivalent to an obligation to surrender data under Art. 265 CrimPC. This does not constitute a “preservation order” within the meaning of Art. 16 para. 2 CCC. 23

24 By ratifying the Cybercrime Convention, Switzerland did not commit itself to introducing "preservation orders" into domestic law. Currently, the Swiss Criminal Procedure Code also does not provide **any legal basis** for ordering data holders and service providers to protect data from loss or alteration and to keep it available for law enforcement authorities without having to disclose it immediately. The message assumes that the possibility of obliging anyone to retain data by means of an order would go too far and would hardly be compatible with the principle of proportionality. This assessment is no longer in line with the times: due to the ongoing development of digitalization, even private individuals now have considerable storage capacity on their data carriers. Numerous trustworthy and cooperative companies voluntarily store data relevant for evidence purposes, such as customer data and technical data (not covered by the FIPCA), in accordance with Swiss data protection regulations (FADP) without being bound by any retention period. Ordering the holders of such data to extend the retention period to a maximum of 90 days is a much less severe measure than ordering the search of records at the relevant data holders (see N. 19 f. above) or requiring them to surrender the complete data immediately (see N. 21 f. above). In view of the technical possibilities available today, extending the retention period does not impose a disproportionate burden on the addressees of the order, and there is a public interest in ensuring that data collected voluntarily by private individuals can be secured as evidence for the purpose of establishing the truth before it is deleted.

25 Under the current Swiss Criminal Procedure Code, the storage of data in the possession of persons not covered by the BÜPF can also be ensured by means of a graduated order in accordance with the legal principle of **argumentum a maiore ad minus**: An order within the meaning of Art. 263 ff. CrimPC may be issued, whereby the data holder is first obliged, under threat of punishment for disobedience under Art. 292 SCC, to provide information, store the data and maintain confidentiality, in order to collect the data relevant to the investigation for the investigation files in a second step. Such a step-by-step obligation does not contradict the principle of numerus clausus for coercive measures (Art. 197 para. 1 lit. a CrimPC), because the first obligation to retain the data is already for the purpose of requesting the evidence-relevant data at a later date in accordance with Art. 263 CrimPC. Such a step-by-step obligation interferes less with the rights of the data holder than the search order under Art. 246 ff. CrimPC or a disclosure order under Art. 265 CrimPC. The retention period of no more than 90 days provided for in Art. 16 para. 2 CCC must

be observed so that the measure does not go beyond the text of the Convention.

D. Securing of data blocked by the Federal Supreme Court despite valid application for sealing

In recent years, the Federal Supreme Court has had to rule several times on cases where, after electronic devices had been secured despite being sealed, a forensic backup copy (mirror image) of the data stored on them was made by the investigating authorities or by a specialist agency commissioned to do so. The Federal Supreme Court considers it inadmissible for an investigating authority to arrange for the mirroring of data after a request for sealing has been made or to transfer this task to a person or authority commissioned by it and bound by its instructions. Instead, after sealing the data carriers, the investigating authority must submit a request for mirroring to the coercive measures court, even if mirroring is urgently necessary to protect against data loss. The request may be submitted together with the application for unsealing or, in cases of urgent necessity, on a super-provisional basis. After sealing, the order to make a copy is the sole responsibility of the coercive measures court. 26

This ruling has rightly been met with considerable **criticism**. It also proves to be contrary to international law in light of the Cybercrime Convention. The Federal Supreme Court is ignoring the fact that Switzerland has committed itself to ensuring that computer data relevant to evidence is secured immediately in domestic proceedings in order to prevent the loss of evidence. With its ruling, the Federal Supreme Court is not only introducing a previously unknown super-provisional procedure before the coercive measures court, but also a procedure in which, even in the case of a coercive order, the collection of evidence-relevant data can be significantly jeopardized within a few hours: As long as the investigating authority cannot make or have a copy of the data made during an on-site search and must instead apply to the coercive measures court and wait for its decision, in current practice there is a considerable risk that persons with access rights will alter or delete the data stored on digital servers or in the cloud before the coercive measures court issues its decision on mirroring. New developments also offer increased protection against access by authorities, provided that immediate action is not taken. Just recently, one of the largest technology companies introduced a security feature on its (mobile) devices that blocks the USB port 60 minutes after the device is 27

last unlocked, with the result that data cannot be read from that point on, nor can software be installed on the device that would enable subsequent reading. It can be assumed that other companies will follow suit. Consequently, certain risk scenarios – both new ones and those considered in the Explanatory Report – can only be prevented by immediate intervention by the investigating authority or the police or person appointed by it during the on-site search. The procedure established by the Federal Supreme Court, which requires a super-provisional mirroring application to be filed with the coercive measures court after sealing, significantly increases the risk of evidence being lost. This cannot be said to be more effective prosecution as intended by the Cybercrime Convention.

BIBLIOGRAPHY

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

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

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

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

MATERIALS

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

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2010/813/de, besucht am 4.5.2025.

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

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 18 CCC (Convention on Cybercrime)

A commentary by Damian K. Graf

SUGGESTED CITATION

Damian K. Graf, Commentary of art. 18 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Graf, art. 18 CCC N. XXX.

Title 3 – Production order

Article 18 – Production order

[1] Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

[2] The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

[3] For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

CONTENT

I. General 158
II. Order to disclose computer data (para. 1 lit. a) 159
III. Order to disclose inventory data from providers (para. 1 lit. b) 161
IV. Reference to Art. 14–15 CCC (para. 2) 165
V. Definition of inventory data (para. 3) 165
VI. Requirements for permissible data collection under Swiss criminal procedure law 166
Bibliography 168
Materialis 169

I. GENERAL

1 In Section 2 ("Procedural law") of Chapter 2 ("Measures to be taken domestically"), Article 18 CCC, under Title 3 ("Ordering disclosure"), deals with the **disclosure of data** by the competent criminal authorities. A distinction is made between two scenarios: on the one hand, the disclosure of computer data by a person located in the territory of the Contracting State concerned (para. 1 lit. a), and on the other hand, the disclosure of inventory data by service providers offering their services in the Contracting State (para. 1 lit. b). Since the latter are not based in the contracting state concerned and the inventory data does not have to be stored there, Art. 18 CCC contains an **extraterritorial** element (see n. 9 f.).

2 Issuing an order to disclose data is the **lesser measure** compared to coercive measures, which interfere more profoundly with the rights of the persons concerned (who are often not themselves accused). In accordance with the principle of proportionality, the possibility of an order to disclose data must always be examined before resorting to more far-reaching coercive measures (such as a house search) (see also Art. 265 para. 4 CrimPC). An important consideration in this balancing of interests is the risk of collusion and loss of evidence if the data is not immediately secured by members of the law enforcement authorities.

3 In terms of content, Art. 18 CCC is limited to the disclosure of **specifically identified or identifiable, existing or stored data in the context of criminal proceedings**. This does not necessarily have to be a cybercrime within the meaning of Articles 2–11 CCC or another crime committed using a computer system; it is sufficient that the evidence available in electronic form is intended to prove any crime (Article 14 para. 2 CCC). This also means that the requested evidence must at least be **potentially relevant**, i.e., it must be of significance for the criminal investigation or must not appear to be obviously unsuitable, which already follows from the generally applicable principle of proportionality (requirement of an "appropriate" state measure).

4 Based on the wording of the Convention ("each Party shall take the necessary legislative or other measures to empower its competent authorities"; similarly Art. 14 para. 1 CCC), Art. 18 CCC is **not a "self-executing" norm** that becomes directly applicable upon ratification of the Convention. Rather, it es-

tablishes an obligation under international law to adopt corresponding domestic provisions. Unlike Art. 32 CCC, Art. 18 CCC cannot therefore be directly invoked as a basis for criminal proceedings.

However, the Federal Council stated in its message that Swiss law already complies with the requirements of Art. 18 CCC. In this respect, both the wording of Art. 18 CCC and the related materials – in particular the Explanatory Report on the CCC and Guidance Note # 10 of the Cybercrime Convention Committee ("T-CY") of the Council of Europe – can be used as **interpretative aids** for the application of domestic provisions, primarily Art. 265 CrimPC. In Switzerland, it is also a general principle that standards must be interpreted in accordance with the convention as far as possible. 5

Art. 18 CCC does not specify how the measures are to be implemented in the respective domestic law; rather, it merely outlines the minimum content of the national enabling provisions and leaves it to the individual contracting states to integrate the convention requirements into their systems of evidence-gathering measures. Art. 18 para. 2 CCC refers to the further minimum guarantees of Art. 14–15 CCC, which must also be observed in this context. 6

Nor does Art. 18 CCC regulate whether and, if so, to what extent data must be stored, nor does it specify retention periods. In particular, it does not contain any obligation for providers to keep records of their subscribers, to ensure that these are accurate, to verify the identity of users or to prevent the use of pseudonyms. Such obligations may arise from domestic regulations at the level of law or ordinance. 7

II. ORDER TO DISCLOSE COMPUTER DATA (PARA. 1 LIT. A)

In **substantive terms**, the request for disclosure may extend to "computer data" defined in Art. 1 lit. b CCC as "any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program that can trigger the execution of a function by a computer system." This term includes **all types of data**, in particular inventory, connection, and content data (see n. 24 ff.). Art. 18 CCC merely requires that the data in question may be requested, without commenting on jurisdiction or specific domestic procedures. For this reason, it is, for example, entirely compatible with Art. 18 and Art. 15 CCC that the disclosure of connection data under Swiss law is subject to stricter requirements than the disclosure of inventory or content 8

data and that the approval of the coercive measures court must also be obtained (see n. 27 f.).

9 **In personal terms**, Art. 18 para. 1 lit. a CCC applies, according to its express wording, to all legal and natural persons who, at the time of the order, have their seat, domicile or even only their temporary residence in the contracting state. The internal relationship required under sovereignty law is defined here – in contrast to Art. 32 CCC, is not defined by the location where the data is stored, but **is linked to the person in whose possession or under whose control the data to be collected is located.** Art. 18 para. 1 lit. a CCC also covers **providers** based in Switzerland; not only inventory data (cf. Art. 18 para. 1 lit. b CCC) but also content and connection data can be made available from them.

10 The
location where the data is stored is irrelevant in this context. Accordingly, **data stored abroad** may also be edited if it is "in the possession or under the control" of a domestic person ("computer data in that person's possession or control"). Art. 18 para. 1 lit. a CCC therefore allows, like Art. 32 CCC, a form of extraterritorial evidence gathering. This is in line with the Federal Supreme Court's case law on Art. 18 CCC and Art. 265 CrimPC, according to which these provisions **allow the disclosure of all data to which the addressee of the order has access or is permitted to have access** ("avoir un pouvoir de disposition, en fait et en droit, sur ces données").

11 The pair of terms "possession or control" refers, on the one hand, to the **physical possession** of the data in question within the territory of the issuing Contracting State (data sovereignty) and, on the other hand, to situations in which the data of interest is not in the custody of the addressee of the disclosure order but the latter has **free control** over its disclosure (right of disposal). This includes, for example, a person who has stored data with a third-party provider, such as in a cloud—in this case, the third-party provider is in possession of the data and the user is in control of it, and both can be held liable as addressees of the order. Ownership and control may differ in this respect. However, according to the Explanatory Report, it is not sufficient to merely have the technical ability to access remotely stored data; rather, the data must be under the legitimate control of the addressee of the disclosure. "Control" thus cumulatively requires both the possibility of access and the authorization to access this data. This must be clarified in detail. The addressee must **coop-**

erate in providing evidence if it claims that it lacks control or access to the requested information.

In **group structures**, it cannot be assumed without further ado that a subsidiary can access data belonging to its parent company or sister companies. Conversely, parent companies within a group are often likely to have either de facto or de jure control over the data within the group due to their position. If data remains with national subsidiaries for regulatory or data protection reasons and the parent company demonstrably lacks access to it, the data can only be requested from the national subsidiary. If internal or external storage or archiving solutions or data centers are used, the right of control remains with the outsourcing party, while the storing company "owns" the data because it is within its sphere of control. Therefore, subsidiaries or partner companies of foreign providers based in Switzerland that store data in Switzerland (e.g., in server farms) are also subject to a disclosure obligation. 12

The decisive factor is the actual or legal ability to access the data **at the time of the order**. Restricting access after receiving a request would not only be an abuse of rights, but could also constitute a criminal offense (see Art. 305 SCC [aiding and abetting]) depending on the legal situation in the contracting states. 13

As seen (n. 9 f.), Art. 18 para. 1 lit. a CCC does not directly refer to the location where data is stored. However, a domestic disclosure order may cover data stored in Switzerland regardless of whether the persons entitled to the data are located abroad (e.g., if a person residing abroad stores data in Switzerland or operates a data center). If only the data is located in Switzerland, but not the persons entitled to the data, the only question that arises is how the disclosure request can be transmitted to the person residing abroad – an issue that also arises under lit. b (see n. 20 f.). 14

III. ORDER TO DISCLOSE INVENTORY DATA FROM PROVIDERS (PARA. 1 LIT. B)

Art. 18 para. 1 lit. b CCC refers to the disclosure of **inventory data** by **service providers** within the meaning of Art. 1 lit. c CCC who offer their **services in the territory of the contracting state**. The article is thus both narrower and broader than lit. a in that it is limited to service providers and the submission of inventory data ("subscriber information") – e.g., the identity of the cus- 15

tomer or details of payment transactions (see n. 24 ff.) – but also covers not only Swiss but also foreign providers (see n. 17 f.). The necessary domestic connection to Switzerland is understood here, similar to the concept under antitrust law, in the sense of the **effect principle**, which is why foreign service providers are also covered if they are active on the Swiss market. The prerequisite here is also that the data is **in the possession or under the control** of the addressee of the order (see n. 11 ff.).

16 In contrast to Art. 32 CCC, which is based on voluntary compliance and requires, among other things, authorization in the general terms and conditions or similar for legally compliant data delivery by providers, a request for disclosure is **binding** and must be implemented by the addressed service providers if it complies with the domestic requirements of the contracting state in which the services are offered and which issued the order. Facilitated and more efficient access to inventory data appears appropriate, as 80–90% of the data required internationally is inventory data; Art. 18 para. 1 lit. b CCC thus contributes to relieving the burden on the international mutual assistance system.

17 On the question of when a service is **"offered"** in a contracting state, there is already case law in European states in other contexts: it is necessary that the activities of the service provider are directed at users in that state, i.e., the service provider intends that users in that state use its services. The mere accessibility of a website or the possibility of logging in from another country is not sufficient for this purpose. Indications that a service is being "offered" include the use of languages or currencies other than those customary in the country of establishment, the use of top-level domains or a telephone area code of a country. For example, the highest Belgian court ruled that Yahoo! Inc. could be compelled to disclose inventory data under threat of criminal penalties because Yahoo! Inc. actively participated in Belgian economic life as a provider of a free webmail service. This was evident, among other things, from the use of the domain "www.yahoo.be," the use of the national language, the placement of advertisements based on the location of users, and the establishment of a complaint form and an FAQ section for Belgian users. Finally, the new Art. 3 no. 4 of Regulation (EU) 2023/1543 on European production orders and European preservation orders for electronic evidence in criminal proceedings and for the enforcement of custodial sentences following criminal proceedings of July 12, 2023 ("e-Evidence Regulation") requires that the

criterion of "providing services in the EU" be met cumulatively by (a) the creation of a possibility for natural or legal persons in a Member State to use the services, and (b) a substantial connection with that Member State, which is deemed to exist, for example, if the service provider has a registered office or a branch in that Member State. cumulatively (a) the creation of a possibility for natural or legal persons in a Member State to use the services, and (b) a substantial connection to that Member State, which is deemed to exist, for example, if the service provider has an establishment or a significant number of users in that Member State or if its activities are directed toward that Member State. Such criteria can also be applied to Art. 18 CCC.

If foreign providers are active with a service in the market of a contracting state, they are obliged to disclose the inventory data relating to the users of that specific service in the respective contracting state. This is the case, for example, if someone registers via the service provider's ".ch" address, has indicated Switzerland as their place of residence or registered office, or has used a Swiss IP address at the time of registration or at a later date. 18

Within the Council of Europe bodies, too, the prevailing view is that **domestic providers** may be required to disclose inventory data stored on a data processing system **abroad** (provided that it is under their control, see also n. 11 ff.) and that orders may be addressed directly to a **foreign provider**. Both are also in line with the wording of Art. 18 CCC. 19

The Federal Supreme Court has also already dealt with these two questions and issued a differentiated ruling: In a judgment of November 16, 2016, it held that Art. 18 CCC and Art. 265 CrimPC permit the disclosure of all data provided that the addressee of the order has factual and legal access to it ("avoir un pouvoir de disposition, en fait et en droit, sur ces données"), including data stored abroad. In a ruling dated January 14, 2015, however, it stated that, on the basis of Art. 18 CCC, a foreign provider cannot be approached directly by means of a disclosure order, even if it offers its services in Switzerland – Art. 32 CCC therefore conclusively regulates direct cross-border access, and Art. 25 para. 4 sentence 1 CCC stipulates that international legal assistance must follow the usual instruments unless a different provision is "expressly" provided for in the CCC. At least the Federal Supreme Court stated that subsidiaries or partner companies of foreign providers based in Switzerland that store data in Switzerland (such as server farms) are subject to Swiss law. However, it did not address the wording of Art. 18 CCC, the Explanatory Report, or the mes- 20

sage, according to which the legislature specifically assumed that domestic law complies with the requirements of Art. 18 CCC. It is not the task of the Federal Supreme Court to override the clear intention of the legislature. Furthermore, there is no apparent violation of sovereignty when services are offered in Switzerland, as in this case there is a sufficient internal connection to Switzerland. A restriction to service providers based in Switzerland would also render Art. 18 para. 1 lit. b CCC obsolete, as providers based in Switzerland are already covered by Art. 18 para. 1 lit. a CCC (see n. 9) and are therefore required to disclose not only inventory data but also content and connection data. Therefore, on balance, Art. 18 para. 1 lit. b CCC can also be used as a basis for the current practice in Switzerland, which is primarily based on Art. 32 CCC, according to which law enforcement authorities address **direct requests to foreign providers** ("information requests"). This also applies in reverse – Swiss providers offering their services in foreign markets may be requested directly by those authorities to disclose data, and since they are generally subject to a disclosure obligation, they are not liable to prosecution under Art. 271 SCC ("Prohibited acts for a foreign state") if they disclose the data.

21 With regard to the **delivery** of disclosure orders, larger providers make so-called "law enforcement portals" available, through which Swiss law enforcement authorities can also register and submit their requests directly. In the case of smaller service providers, requests for disclosure can be sent via the police (via Interpol) or, if accepted, directly (e.g. by email). Art. 18 para. 1 lit. b CCC allows the formal mutual assistance procedure to be waived and permits the contracting states to serve such disclosure orders directly on providers in other contracting states. This is permissible and appropriate, as the requirement for service of the disclosure order by mutual legal assistance would negate the simplifications that Art. 18 para. 1 lit b CCC is specifically intended to enable. Only direct service ensures that the criminal prosecution authorities can access the necessary inventory data efficiently and quickly without having to go through the often lengthy and bureaucratic mutual legal assistance procedure. The fact remains, however, that the lack of cooperation cannot be enforced directly, but only through the formal mutual legal assistance procedure by means of coercive measures going beyond Art. 18 CCC.

22 Since the request for disclosure is a **domestic measure of evidence**, it is not the law of the contracting state in which the provider is based that is decisive, but the law of the contracting state in which the provider offers its services.

IV. REFERENCE TO ART. 14–15 CCC (PARA. 2)

States may, within the framework of Art. 15 CCC, lay down **conditions and safeguards** and exclude data from the scope of Art. 18 CCC. For example, it is justified to restrict the disclosure of connection data to certain offenses and to require that authorization be obtained from the coercive measures court (Art. 273 CrimPC). Furthermore, it is permissible to link disclosure orders to prohibitions on disclosure, as implemented in Swiss law (Art. 73 para. 2 CrimPC). 23

V. DEFINITION OF INVENTORY DATA (PARA. 3)

Inventory data includes all information – other than connection or content data – stored by a service provider in connection with a user or subscriber of its services. The main purpose of requesting inventory data is to determine the **identity** of the subscriber or user and to identify the services used by the user. In addition, commercial information such as billing and payment data may also be relevant, particularly in connection with cyber fraud and other property offences. 24

According to Art. 18 para. 3 CCC, inventory data includes all information relating to (a) the type of communication service used, the technical measures taken for this purpose and the duration of the service; (b) the identity of the subscriber, their postal or home address, telephone and other access numbers, and billing and payment details available on the basis of the contract or agreement relating to the service; and (c) other information about the location of the communication equipment available on the basis of the contract or agreement relating to the service. In Switzerland, the information that may be disclosed pursuant to Art. 22 para. 1 BÜPF is specified in Articles 36–38 of the Ordinance on the Surveillance of Postal and Telecommunications Traffic of November 15, 2017 ("VÜPF," SR 780.11). In particular, inventory data includes addressing elements such as the assignment of names, telephone numbers, and addresses of users to a known IP address, as well as original contracts and copies of identification documents presented when the contract was concluded, and technical information relating to telecommunications. 25

Inventory data must be distinguished from **content data**, which comprises the content of communications or stored files, and from connection or **traffic data**, which is generated in connection with a communication and reveals the origin, destination, route, time, date, scope, or duration of the communication 26

(Art. 1 lit. d CCC). The Federal Supreme Court differentiates between inventory data and peripheral data based on the criterion of whether the law enforcement authorities already know an Internet connection or an e-mail address that only needs to be assigned to a specific person; if so, it is a query of inventory data. If, on the other hand, the law enforcement authorities are only aware of criminal Internet communication activities and the assigned IP addresses and registered customers are to be determined from the connection peripheral data of the communication in question, this constitutes a (permit-requiring) retroactive collection of peripheral data within the meaning of Art. 273 CrimPC. According to case law, this should also apply across the board to requests for the disclosure of IP history. The distinction must be made according to whether it is a question of who communicated with whom and when (connection data within the meaning of Art. 273 CrimPC) or rather who used a specific service at a known point in time (inventory data within the meaning of Art. 22 para. 1 BÜPF). **Registration IP addresses** for an already known account must therefore be clearly regarded as inventory data and not as traffic data, as they serve exclusively to identify a participant and have no connection to subsequent communication via the account. Other **"access data"** (e.g., the IP history of logins to a service not intended for communication, such as logging into a crypto wallet or a cloud) cannot correctly be considered connection metadata either. This data does not directly or indirectly concern communication between people and its surveillance. In such cases, IP addresses are more comparable to traces left at the scene of a crime, similar to a fingerprint or DNA, and do not constitute connection data in the context of human communication, but rather inventory data. The Federal Supreme Court's ruling on the classification of IP histories as traffic data within the meaning of Art. 273 CrimPC is insufficiently differentiated in this respect.

VI. REQUIREMENTS FOR PERMISSIBLE DATA COLLECTION UNDER SWISS CRIMINAL PROCEDURE LAW

27 For **inventory data** within the meaning of Art. 18 para. 3 CCC – i.e. in particular (also retroactive) information about who is or was registered as the owner or billing addressee of the connection with service providers subject to Swiss law (see n. 24 ff.) – a simple query pursuant to Art. 22 para. 1 BÜPF may be submitted to the service provider responsible for monitoring postal and

telecommunications traffic (ÜPF service). Such information may also be obtained through disclosure (Art. 265 CrimPC), in particular if the foreign provider offering its services within the meaning of Art. 18 para. 1 lit. b CCC in Switzerland is not subject to the BÜPF. The request for information via the PTPS is merely a procedural requirement; neither the CrimPC nor the PTPA or the associated ordinance stipulate that information not communicated via the PTPS is inadmissible. A request for inventory data requires a suspicion that a criminal offense (felony, misdemeanor, or violation) has been committed via the Internet (Art. 22 para. 1 BÜPF), that the information requested is potentially relevant to the investigation or admissible as evidence, and that the measure is proportionate. No ordinary legal remedy is available against a request for inventory data; in particular, sealing (Art. 248 CrimPC) is not applicable, as it is not apparent from the outset to what extent the requested inventory data could be subject to a prohibition of seizure under Art. 264 CrimPC. Providers are subject to a duty to provide information; if they refuse to do so, an administrative fine or a fine pursuant to Art. 292 SCC may be imposed (provided they have been informed of this in advance), or coercive measures may be taken (analogous to Art. 265 para. 3 and 4 CrimPC). For foreign providers offering their services in Switzerland, the threat of criminal penalties under Art. 292 SCC should also be permissible, but coercive measures to enforce the request for inventory data would have to be requested from the relevant state through mutual legal assistance.

28 For content and connection data, both of which may be requested under Art. 18 para. 1 lit. a CrimPC, a distinction must then be made: **Content data** that may be relevant for evidentiary purposes must be disclosed under Art. 265 CrimPC if it is stored ("in storage") at the time of the order and is not still in transit ("in traffic"). Relevant in practice are, for example, content data from webmail operators, such as the email account of an "@bluewin.ch" address at Swisscom. The prerequisites for the disclosure of content data are sufficient suspicion of any criminal offense, the potential evidential value or relevance of the disclosed records for the criminal proceedings, and compliance with the principle of proportionality. The disclosure order may be linked to a prohibition of disclosure pursuant to Art. 73 para. 2 CrimPC, which means that the account holder may not be notified by the service provider until further notice. The owners and other authorized persons may appeal against disclosure orders by applying for sealing (Art. 248 CrimPC), at least insofar as they can assert their own interests in confidentiality. Although the provider is for-

mally entitled to request sealing, it cannot do so on behalf of its customers and is unlikely to be able to invoke its own prohibition of seizure under Art. 264 CrimPC. For **connection or marginal data** (see n. 26), the public prosecutor's office must not issue a disclosure order, but rather an order pursuant to Art. 273 CrimPC, which is subject to stricter requirements: (1) There must be urgent suspicion of a crime or offense; (2) the seriousness of the offense must justify the surveillance; (3) the investigative measures taken to date must have been unsuccessful or the investigation would otherwise be futile or disproportionately difficult (Art. 273 para. 1 in conjunction with Art. 269 para. 1 CrimPC). The order must also be approved by the coercive measures court (Art. 274 CrimPC), otherwise the evidence obtained is absolutely inadmissible (Art. 277 para. 2 CrimPC). The approval of the coercive measures court may be challenged by the person under surveillance, or, where applicable, by the provider, by means of an appeal under Art. 393 ff. CrimPC (Art. 279 para. 3 CrimPC).

BIBLIOGRAPHY

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

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

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

Graf Damian K., Kommentierung zu Art. 32 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter https://onlinekommentar.ch/de/kommentare/cc-c32, besucht am 31.3.2025 (zit. OK).

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

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

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

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

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

Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 2014.

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

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

MATERIALIS

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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 25 CCC (Convention on Cybercrime)

A commentary by Miro Dangubic

SUGGESTED CITATION

Miro Dangubic, Commentary of art. 25 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Dangubic, Art. 25 CCC N. XXX.

Title 3 General principles relating to mutual assistance

Article 25 General principles relating to mutual assistance

[1] The Parties shall afford one another mutual assistance to the widest extent possible for thepurpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

[2] Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

[3] Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of

communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying

CONTENT

I. Introduction 174
II. The material scope of application of the CCC in relation to local mutual assistance 174
A. Criminal offense as a connecting factor 175
B. Evidence in electronic form as a connecting factor 175
III. Legal sources in mutual legal assistance 175
A. Mutual assistance provisions 175
B. Subsidiary procedural law in Switzerland 176
IV. Obligation to provide legal assistance 176
V. Principle of maximum accommodation 176
VI. Forms of transmission in mutual legal assistance 177
VII. Structure of the principle of double criminality 178
A. Principle of double criminality 178
B. Principle of double criminality within the scope of application of the CCC 178
VIII. Breaking through the fiscal reservation 179
IX. Legislative mandate to the contracting states 179
A. General 179
B. Implementation in Switzerland 179
Bibliography 180
Materials 181

I. INTRODUCTION

1 Art. 25 CCC summarizes under the heading "General Principles of Mutual Legal Assistance" various provisions relating to small-scale mutual legal assistance within the scope of application of the CCC. Specifically, the article contains provisions concerning

- the material scope of application of the CCC (para. 1),
- the relevant legal sources in legal assistance proceedings (para. 4),
- the obligation to provide minor legal assistance (para. 1),
- the principle of maximum accommodation (para. 1),
- the possible forms of transmission in mutual legal assistance proceedings (para. 3),
- the structure of the principle of double criminality (para. 5) and
- the breach of the fiscal reservation (para. 4).

2 Furthermore, Art. 25 para. 2 CCC contains a legislative mandate to the contracting states.

3 The CCC is intended to supplement existing bilateral or multilateral treaties and agreements between the contracting parties (in particular the EUeR) and thereby accelerate and simplify mutual legal assistance procedures. Its conception as a supplementary convention has a strong impact on the regulatory content and the density of regulation relating to small-scale mutual assistance.

II. THE MATERIAL SCOPE OF APPLICATION OF THE CCC IN RELATION TO LOCAL MUTUAL ASSISTANCE

4 The substantive scope of application of the CCC for small-scale mutual assistance is governed by Art. 25 para. 1 CCC and has two alternative connecting factors: On the one hand, it can be linked to the offense under investigation ("offenses related to computer systems and data") and, on the other hand, to the evidence to be collected ("evidence in electronic form").

A. Criminal offense as a connecting factor

On the one hand, the material scope of application applies if there is a suspicion that an offense described in Art. 2-11 CCC has been committed. On the other hand, the material scope of application applies to offenses committed by means of a computer system - regardless of the actual offense committed. The offence "computer systems" is defined in Art. 1 lit. a CCC as follows: "a device or a group of interconnected or related devices which, individually or in combination, perform automatic data processing on the basis of a program". 5

In the prima facie examination of this material scope of application by the mutual legal assistance authorities, the following must be taken into account in particular: Certain elements of the material scope of application are in principle part of the legally relevant facts to be clarified in the context of the foreign criminal investigation; in some circumstances, it is precisely these points that the requested measures of evidence are intended to clarify. Accordingly, no high demands are to be placed on the description of these factual elements. 6

B. Evidence in electronic form as a connecting factor

If evidence is to be collected in the context of mutual assistance in criminal matters which is presumed to be in electronic form, the material scope of application of the CCC applies irrespective of the offense under investigation. Evidence in electronic form may, in particular, be data. 7

III. LEGAL SOURCES IN MUTUAL LEGAL ASSISTANCE

A. Mutual assistance provisions

Mutual assistance proceedings within the scope of the CCC are primarily governed by the relevant international treaties and the CCC. Insofar as these international treaties do not expressly or implicitly regulate certain issues, the national provisions apply (Art. 25 para. 4 CCC). In Switzerland, the IMAC and the IMAC Ordinance are authoritative for mutual assistance in criminal matters (Art. 1 para. 1 IMAC). The principle of favorability - also enshrined in Art. 25 para. 1 CCC - states that the national provisions apply even if they impose less stringent requirements for mutual assistance. Consequently, the provisions of the CCC only apply in mutual legal assistance proceedings if they 8

represent the most favorable norm from the perspective of the requesting state.

B. Subsidiary procedural law in Switzerland

9 If the mutual assistance provisions lack relevant procedural provisions, the CrimPC and the APA apply mutatis mutandis in mutual assistance proceedings in Switzerland. The CrimPC is authoritative in mutual assistance proceedings if the IMAC refers to it directly or in connection with criminal procedural acts within the meaning of Art. 63 et seq. IMAC. In other cases, the APA serves as subsidiary procedural law.

IV. OBLIGATION TO PROVIDE LEGAL ASSISTANCE

10 Based on Art. 25 para. 1 CCC, the requested state is obliged, if all the conditions for mutual assistance are met, to provide minor mutual assistance if it is requested to do so by a contracting party. However, this obligation does not mean that the requesting state has the status of a party or the right to appeal within the framework of the legal assistance proceedings. Any divergent positions of states with regard to the question of whether the conditions for mutual assistance in criminal matters are met and whether mutual assistance should be provided shall be resolved at diplomatic level.

11 In the case of non-contractual mutual assistance in criminal matters, there is no entitlement to intergovernmental cooperation in criminal matters (see Art. 1 para. 4 IMAC).

V. PRINCIPLE OF MAXIMUM ACCOMMODATION

12 Art. 25 para. 1 CCC obliges the requested state to comply with requests for mutual assistance within the scope of application of the CCC "to the greatest extent possible" (so-called principle of maximum accommodation).

13 The principle of maximum accommodation is a generally recognized principle of mutual assistance in criminal matters that is not merely programmatic in nature. The principle includes the above-mentioned principle of favorability. In practice, the principle of favorability applies in all mutual legal assistance proceedings - even if there is no obligation to do so under international treaties. It states that national law may not make legal assistance in criminal

matters more difficult than overriding international treaty law, but it may make it easier.

The principle of maximum accommodation also relates to the scope of the legal assistance to be provided. It allows the measures requested in a request for mutual assistance to be interpreted generously and all potentially relevant evidence for the foreign criminal proceedings to be handed over to the requesting authority - even if the requesting authority has not explicitly requested this. 14

VI. FORMS OF TRANSMISSION IN MUTUAL LEGAL ASSISTANCE

According to the IMAC, requests for mutual legal assistance addressed to Switzerland must generally be sent in writing to the Federal Office of Justice. However, several European treaties also permit direct communication between the competent judicial bodies (usually public prosecutors' offices) as well as alternatives to written correspondence. 15

Within the scope of application of the CCC, Art. 25 para. 3 CCC permits the use of "rapid means of communication, including fax or electronic mail" in urgent cases. This applies not only to requests for mutual legal assistance, but to all mutual legal assistance. The purpose of this provision is to speed up mutual assistance proceedings and, in particular, to enable evidence to be secured quickly in order to counteract the risk of evidence being lost. A request for mutual assistance must be submitted in writing at the explicit request of the requested state. 16

Temporal urgency is given if there is a risk of loss of evidence with the transmission in written form. This is particularly the case if data needs to be collected for the purposes of mutual legal assistance. 17

There is no numerus clausus with regard to the means of communication that may be used. In practice, e-mail, fax and state file-sharing platforms are used in particular. However, requests for legal assistance may also be made by telephone. 18

The relevant security and authentication standards are derived from the national legal systems or the guidelines and practice of the relevant authorities. 19

VII. STRUCTURE OF THE PRINCIPLE OF DOUBLE CRIMINALITY

20 Art. 25 para. 5 CCC regulates the structure of the principle of dual criminality.

A. Principle of double criminality

21 Double criminality is a classic principle of international cooperation. It states that mutual assistance in criminal matters is only granted with regard to offenses that are punishable under the law of both the requesting and the requested state. The principle of dual criminality is part of public policy in Switzerland and has been ensured accordingly in all bilateral treaties and (by means of reservations) in multilateral mutual legal assistance agreements - including for the scope of application of the CCC.

B. Principle of double criminality within the scope of application of the CCC

22 If measures requiring procedural coercion are to be applied in the context of mutual assistance proceedings, the principle of double criminality applies within the scope of application of the CCC. However, there are also exceptions to this principle.

23 According to the general principles, criminal liability under the law of the requesting state - also within the scope of application of the CCC - is not to be examined in principle in mutual assistance proceedings here, subject to cases of obvious abuse.

24 On the question of double criminality under Swiss law, the executing authority examines whether the set of facts described in the request for mutual assistance can prima facie be subsumed under a Swiss criminal provision. Art. 25 para. 5 CCC states on the one hand that it is sufficient if the facts described in the request for mutual assistance can be subsumed under a single criminal offense under Swiss law - it is not necessary to further examine whether other offenses could also be fulfilled. On the other hand, it stipulates that dual criminality does not require identical criminal provisions in the requesting and requested state. Consequently, the content of para. 5 already corresponds to the current practice in Switzerland.

VIII. BREAKING THROUGH THE FISCAL RESERVATION

Traditionally, numerous sources of law - both national and international - contain a so-called fiscal reservation. For example, Art. 3 para. 3 IMAC stipulates that accessory legal assistance in proceedings for the evasion of fiscal duties is also excluded in principle. 25

Sentence two of Art. 25 para. 4 CCC is intended to ensure that any fiscal reservations do not stand in the way of mutual legal assistance within the scope of application of the CCC if criminal offenses within the meaning of Art. 2-11 CCC are being investigated. Since the offenses described in Art. 2-11 CCC are not fiscal offenses, the practical relevance of this provision is likely to be rather limited. At best, one could consider constellations of ideal competition: The perpetrator commits both a fiscal offense not eligible for mutual assistance and a criminal offense within the meaning of Art. 2-11 CCC through a single act or through a uniform, related act. In this case, the fiscal reservation would always be breached. 26

IX. LEGISLATIVE MANDATE TO THE CONTRACTING STATES

A. General

Art. 25 para. 2 CCC obliges the Contracting States to ensure, when drafting their national legal systems, that national instruments exist to implement the provisions of Art. 27-35 CCC. This norm therefore primarily represents a so-called legislative mandate under international law. 27

The obligation is fundamentally directed at the legislature and requires active action on the part of the state party - if domestic law does not (yet) meet the requirements. States parties that already have the necessary legal instruments do not have to take legislative action. 28

B. Implementation in Switzerland

As we understand it here, the provisions of Art. 27-35 CCC are generally to be qualified as self-executing. With regard to their domestic applicability and enforceability, the legislator only saw a need for action with regard to Art. 30 and 33 CCC. 29

30 To implement Art. 30 CCC (Immediate disclosure of secured traffic data) and Art. 33 CCC (Mutual legal assistance in the collection of traffic data in real time), Art. 18b IMAC was inserted into the law with the marginal note "Electronic data" by federal decree of March 18, 2011.

BIBLIOGRAPHY

Böhi Simon, Kommentierung zu Art. 18*b* 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 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.

MATERIALS

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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 27 CCC (Convention on Cybercrime)

A commentary by Jan Reinhardt

SUGGESTED CITATION

Jan Reinhardt, Commentary of art. 27 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Reinhardt, art. 27 CCC N. XXX.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

[1] Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

[2] a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

[3] Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

[4] The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

[5] The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

[6] Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

[7] The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be

given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

[8] The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

[9] a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

CONTENT

I. General 187
II. Relationship to other provisions 187
III. Requirements for mutual legal assistance 189
A. Establishment of authorities (para. 2) 189
B. Requirements regarding the manner of implementation (para. 3) 190
C. Objections to execution 191
1. Additional grounds for refusal (para. 4) 191
2. Postponement of mutual legal assistance (para. 5) 193
3. Condition as a minimum requirement for refusal and postponement (para. 6) 193
D. Obligation to provide information (para. 7) 194
E. Confidentiality (para. 8) 194
F. "Accelerated procedure" (para. 9) 197
IV. Legal protection 197
Bibliography 198
Materials 199

I. GENERAL

Art. 27 CCC supplements the general mutual legal assistance requirement of Art. 25 para. 1 CCC and guarantees a **minimum institutional framework** for minor mutual legal assistance. The provision prevents the need to resort to non-contractual mutual legal assistance between two contracting parties and thus serves the principle of effectiveness under Art. 25 para. 1 CCC. 1

In addition to the obligation to designate certain authorities, the provision contains a more detailed **obligation to execute requests for legal assistance**. In this respect, it is self-executing according to the Swiss monistic understanding. However, as in the case of non-treaty legal assistance under the IMAC, there must be a basis for authorization in national procedural law for the individual measures requested. It also follows from Art. 25 para. 2 CCC that the contracting states must adapt their legal systems so that they do not conflict with the procedure under the articles of this section. No need for this was seen with regard to Art. 27 CCC. 2

II. RELATIONSHIP TO OTHER PROVISIONS

Art. 27 CCC merely establishes a procedure for requests for legal assistance. The prerequisite is the opening of the scope of application specified in Art. 25 para. 1. This includes all proceedings in connection with computer systems and data as well as the collection of evidence in electronic form, including for other criminal offenses. The latter in particular creates a **broad scope of application**. The Second Additional Protocol to the CCC contains several partial references to Art. 27 CCC, namely in Art. 3 para. 2 lit. a, Art. 7 para. 5 lit. a, Art. 8 para. 8, Art. 10 para. 7 and Art. 11 para. 2 lit. b. However, Switzerland has not yet signed or ratified this Additional Protocol. 3

Art. 25 CCC regulates the scope of application and the principles of mutual assistance under the CCC. In paras. 2 and 4, it refers primarily to the provisions of the CCC and, subsidiarily, to national law, in Switzerland primarily to the IMAC, and secondarily to the APA and the CrimPC. Art. 27 CCC therefore takes precedence over national law within its scope of application from the perspective of the CCC. The extent to which this precedence also applies from the perspective of national law is a matter for national law. For Switzerland, Art. 27 CCC can be assumed to take precedence in principle. In view of 4

the very fundamental, primarily organizational provisions in Art. 27 CCC, conflicts between this provision and national law are unlikely. Rather, it creates a minimum standard that does not preclude detailed and more extensive regulation by national law.

5 Art. 27 para. 1 sentences 1 and 2 CCC stipulate, in accordance with the heading of Title IV – "Procedure for requests for legal assistance **without an applicable international agreement**" that the provisions of the article are only applicable to individual requests for legal assistance if there is no (bilateral) legal assistance treaty or (multilateral) agreement in force between the requesting and requested states, or if the parties agree to apply Art. 27 CCC in whole or in part despite existing contractual legal assistance. Beyond the wording, another agreement limited to a specific area would not suffice. What is meant here is rather a general mutual legal assistance agreement that also guarantees contractual (minor) mutual legal assistance within the scope of application of Art. 25 para. 1 CCC. If such an agreement exists, Art. 27 CCC is not applicable, even in part, subject to an agreement between the contracting parties, for example with regard to the additional grounds for refusal in Art. 27 para. 4 CCC. This makes it clear that Art. 27 CCC merely sets a minimum standard that does not preclude **further commitments by the contracting states in other agreements**. This is not an essential provision of the CCC, such as Art. 25 para. 4 sentence 2 CCC or Art. 29 CCC, which are not flexible according to the system of the Convention.

6 The actual scope of application of Art. 27 CCC is limited for Switzerland, as it is for many other contracting states. It is significantly restricted by the European Convention on Mutual Assistance in Criminal Matters of April 20, 1959. This provides comprehensive and superseding rules between the signatory member states of the Council of Europe. In addition, there are bilateral mutual assistance treaties concluded by Switzerland, for example with the United States of America, Canada, and Peru. These treaties comprehensively regulate mutual legal assistance in criminal matters and also do not provide for the supplementary application of Art. 27 CCC, so that it does not apply. The regulation is **primarily applicable for Switzerland in relation to many African and Latin American countries and between Switzerland and Japan**. Countries without an applicable agreement or bilateral treaty are currently (as of April 12, 2025) the following: Argentina, Benin, Brazil, Cape Verde, Costa Rica, Côte d'Ivoire, the Dominican Republic, Fiji, Ghana, Grena-

da, Japan, Cameroon, Kiribati, Colombia, Morocco, Mauritius, Nigeria, Panama, Senegal, Sierra Leone, Sri Lanka, Tonga, and Tunisia. Finally, the procedure under the CCC is also likely to apply in relation to Paraguay. In this respect, there is only an extradition treaty, but no comprehensive treaty on minor mutual legal assistance. With regard to the taking and securing of evidence, only Articles 16 and 17 of the treaty contain provisions on the examination of witnesses. In addition, the scope of application of the extradition treaty is limited in Article 2, to which reference is made in the other articles, to certain listed offenses. The list includes, for example in the form of fraud covered by Article 2(18) of the treaty, only a small proportion of the offenses punishable under Articles 2 et seq. of the CCC, which is not surprising given that the treaty was concluded in 1906. Article 27 of the CCC is also likely to apply in relations between Switzerland and Rwanda. Articles 13 and 14 of the extradition treaty between Switzerland and Belgium, which remain applicable in this respect, contain only rudimentary provisions on minor mutual assistance through diplomatic channels. The purpose of Article 27 CCC, which is to ensure an effective minimum standard within its scope, also requires the application of the more extensive provisions of this article in this respect.

Conflicts of norms within the CCC would have to be resolved in accordance with the general principles of interpretation, in particular the *lex specialis* principle. 7

III. REQUIREMENTS FOR MUTUAL LEGAL ASSISTANCE

A. Establishment of authorities (para. 2)

The communication via central authorities that is customary in the field of mutual legal assistance is intended to provide the requesting party with a **central point of contact** and thus serve to speed up international criminal prosecution, which is particularly important in the case of cybercrime. At the same time, equal treatment of incoming and outgoing requests should be ensured. Communication via central authorities avoids the inefficient communication via diplomatic channels that would otherwise be necessary in the case of non-contractual mutual legal assistance. 8

The Federal Council has designated the **Federal Office of Justice** as the competent authority. Thus, there is no deviation from Art. 27 para. 2 IMAC for requests for mutual legal assistance based on the CCC. The current list of 9

competent authorities of all contracting states can be found in English on the Council of Europe website.

B. Requirements regarding the manner of implementation (para. 3)

10 Para. 3 largely corresponds to Art. 65 IMAC and provisions in bilateral mutual assistance treaties. The provision is intended to ensure that evidence obtained through mutual assistance can be used in criminal proceedings in the requesting state. The criminal procedure law of the individual contracting states differs considerably in some respects with regard to the requirements for the taking of evidence. One example is the general requirement that witness statements be sworn, see also Art. 65 para. 1 lit. a IMAC. If the requested state, which does not have such a requirement, were to apply only its own procedural law, there would be a risk that the evidence would be **inadmissible in the requesting state** and the mutual assistance would fail to achieve its purpose. This is because the requested state regularly applies its own criminal procedure law, see Art. 12 and Art. 63 para. 1 IMAC.

11 However, the principle of effective mutual assistance is not guaranteed in absolute terms. Rather, the execution of the request in the procedure specified by the requesting state is subject to **compatibility with the law of the requested state**, see also Art. 65 para. 2 IMAC. The latter may therefore – without prejudice to any possibility of refusing mutual assistance altogether – apply its own procedural law insofar as the procedure specified by the requesting state is incompatible with its national law. Taking into account the wording of the English ("except where") and French ("sauf lorsqu'elle") language versions and the stated purpose of the exception, this should always refer only to individual requirements. The requested state may therefore not apply its national procedure as a whole because a single requirement is incompatible with its law. In accordance with the wording cited above, the principle laid down in Art. 25 para. 1 CCC and the legal principle underlying Art. 27 para. 6 CCC, it would even be appropriate to reduce the incompatible requirement to the extent possible to the still compatible extent and thus maximize the likelihood of its usability in the requesting state. A practical solution lies in consultation via the competent authorities designated in para. 2.

12 It
is very important to distinguish between a manner of implementation that is

incompatible with national law and one that is **merely not provided for** in national law, as refusal cannot be based solely on the latter fact. In any case, provisions of constitutional rank, such as those on secularism in relation to religious oath requirements, justify refusal. Conversely, the mere fact that national ordinary law provides for a different rule is naturally not sufficient. This must be distinguished, by interpretation in each individual case, from provisions of ordinary law that expressly preclude the specific implementation measure. The decisive factor is likely to be whether the required formality constitutes an additional significant interference with individual rights for which there is no legal basis.

The intention of the contracting states is likely to be to apply para. 3 more strictly than Art. 65 para. 2 IMAC. This is also reflected in the fact that the additional broad criterion of substantial disadvantage is not contained in the CCC. In addition, Art. 25 CCC also provides for a stricter mutual assistance regime for the particularly internationalized area of cybercrime. 13

At the same time, a comparison with para. 4 lit. a shows that the reduction to a pure *ordre public* reservation for the limited right of refusal under para. 3 is not intended. In this respect, the reservation is to be classified between the broad provision of Art. 65 para. 2 IMAC and a pure *public policy* principle, as contained, for example, in § 73 sentence 1 of the German IRG. Accordingly, a request can and must be refused if its execution would require **significant interference with individual rights** without a legal basis and contrary to the legislative balancing of interests. 14

Insofar as national procedural law imposes **further requirements** on the measure to be taken, these must in principle be complied with by the executing authorities of the requested state, see also Art. 12 para. 1 IMAC. 15

C. Objections to execution

1. Additional grounds for refusal (para. 4)

In proceedings under Art. 27 CCC, Art. 25 para. 4 CCC applies first. In this respect, too, reference is made to the grounds for refusal under national law or an applicable mutual assistance treaty, whereby refusal is inadmissible *solely* on the basis of classification as a fiscal offense. Art. 27 para. 4 CCC refers to Art. 25 para. 4 CCC and specifies two additional grounds for refusal: the pros- 16

ecution of **political offenses** and the *ordre public* **principle**. The requested state may therefore invoke these grounds for refusal even if they are not provided for in national law. However, in the case of an applicable international agreement, Art. 27 CCC does not apply in principle, in accordance with para. 1.

17 Against the background of the CCC system, according to which the grounds for refusal under national law regularly apply in the case of Art. 27 CCC, it is not entirely clear at first glance what practical added value the additional grounds for refusal offer. A state that does not provide for these restrictions in its national law will not normally invoke them in proceedings under the CCC either, as refusal under para. 4 is at the discretion of the requested state. The significance of this is likely to be that, in applying the principle of maximum mutual assistance, the states have agreed to make use of the grounds for refusal under national law that are not mentioned in para. 4 only in exceptional cases within the scope of application of the CCC. Against this background, para. 4 has a **clarifying and symbolic effect**. The provision shows that the grounds for refusal mentioned remain valid as an expression of national ideology. However, the agreement not to apply other grounds for refusal as a rule is likely to be primarily politically binding, not least because it was not included in the text of the Convention.

18 For Switzerland, in addition to the IMAC, there may be a **limited scope** for the additional grounds for refusal in direct application of para. 4. In the case of political offenses, the ground for refusal under Art. 3 para. 1 IMAC applies. It can be assumed that Art. 27 para. 4 lit. a CCC also covers both absolute and relative political offenses. In view of the cautious provision in the CCC, which refers extensively to national law, and the subjective classification of an act as political or non-political, which varies between states, no autonomous interpretation should be made. Rather, the formulation of the ground for refusal should be left to the requested state, subject to abuse of rights. In the event of exclusion pursuant to Art. 3 para. 2 IMAC, refusal pursuant to Art. 27 para. 4 lit. a CCC is also not to be expected.

19 The *ordre public* reservation is partially expressed in Art. 2 IMAC. As a general principle of international law and in view of the constitutional interpretation of the IMAC, in particular the general clause of Art. 2 lit. d IMAC, it must also be assumed that it already applies under national law. Art. 27 para. 4 lit. b CCC simplifies the justification for refusal in this respect. The *public policy*

reservation also applies to the failure to guarantee basic data protection standards, whereby high requirements must be met. Priority should be given to mutual legal assistance subject to a corresponding assurance.

2. Postponement of mutual legal assistance (para. 5)

Para. 5 allows the requested state, i.e. the competent authority, to postpone the execution of the request for legal assistance and thus to deviate from the **requirement of prompt execution** expressed in Art. 25 para. 1 CCC, the preamble to the Convention and the possibility of an urgent procedure under Art. 27 para. 9 CCC. Conversely, this means that if the conditions of para. 5 are not met, the request must be executed within a reasonable time. Since this is a less severe means of refusal, there is no fixed maximum period. Rather, the execution of the request may be postponed for as long as the conditions of para. 5 are met. 20

The prerequisite for postponement is the risk that immediate execution would impair the requested state's own criminal investigations or proceedings. Impairment is not limited to the frustration of the investigation, for example in the case of long-term covert investigations by the requesting state. Rather, the **delay of an imminent taking of evidence** that would otherwise be expected to result from the surrender of the evidence to the requesting state is sufficient grounds for refusal. Nevertheless, in the interests of comprehensive and expeditious mutual legal assistance, the possibility provided for in para. 5 should only be used with restraint. 21

According to the system of Article 27 CCC, **refusal and postponement** are independent of each other due to their different prerequisites and legal consequences, so that the decision on refusal could be postponed until the end of the period under para. 5. However, an overall assessment must in any case be made when deciding under para. 6 and should also be in line with the requirement of effective mutual assistance. 22

3. Condition as a minimum requirement for refusal and postponement (para. 6)

Para. 6 implements the principle of effective and comprehensive mutual legal assistance in accordance with Art. 25 para. 1 CCC. The requesting state should not be forced to elaborate detailed main and subsidiary requests. Rather, it is incumbent on the requested state to comply with the request as far as possible 23

and to consult the requesting state if it has any reservations. This means that objections should be limited to separable parts of the request, as far as possible. The part not affected should then be dealt with immediately. As a second option for ensuring prompt execution, para. 6 provides for execution subject to conditions. These conditions primarily concern the use of the evidence transferred in the requesting state. Appropriate assurances must be obtained before the evidence is handed over. A common condition is that the evidence may only be used for the proceedings in question and not for any further proceedings. If, on the other hand, there are concerns about the legality of the execution in the requesting state, efforts should be made during the consultation to adapt the request. If this is not done, the request must be rejected in whole or in part, or the procedure set out in para. 3 must be followed. In the interests of effective mutual assistance, the rights of the requested state under para. 6 should also be exercised with restraint.

D. Obligation to provide information (para. 7)

24 Para. 7 contains notification requirements regarding the results of the execution and the reasons for a refusal or postponement. This serves to inform the requesting State so that it can make **future requests** to the same State more effective. A separate notification of the reasons for a condition is not required. It is apparently assumed that the reasons are either sufficiently apparent from the condition itself or that they will be discussed with the requesting State in the context of a consultation under para. 6.

E. Confidentiality (para. 8)

25 Para. 8 allows, beyond para. 3, a requirement for the execution of the request that does not serve the usability in the requesting state but other **investigative or political interests**. The wording "unless the execution of the request requires otherwise" in the German translation is misleading: the English ("except to the extent necessary") and French ("sauf dans la mesure nécessaire") versions make it clear that this clause elaborates on the concept of confidentiality and does not in principle restrict the possibility of proceeding under para. 8. Confidential within the meaning of para. 8 also includes, in particular, a measure that necessarily becomes known to the person concerned, such as the bank of the accused.

In view of the restrictive wording and the requirement for the most comprehensive mutual legal assistance possible, structural factual deficiencies cannot be used to justify inability to comply, such as problems with corruption within the competent authorities. The exception should rather be interpreted in accordance with para. 3, second half-sentence, and thus concern **legal obstacles**. Confidentiality cannot therefore be observed if the measures that are the subject of the request, including the fact that they are based on a request for mutual assistance, must be disclosed under mandatory national law. 26

The interest of the requesting state is usually to prevent the **accused** from becoming aware of the request. The same applies to the person **affected** by the measure, provided that this person is close to the accused and the measure can in principle be carried out secretly. Confidentiality is not guaranteed in any case if the accused is directly informed or if the information is likely to be disclosed by the person concerned. Furthermore, confidentiality is naturally not guaranteed if the fact that a request has been made or the content of that request becomes known to the public, i.e., to an indefinite number of persons who are not connected by any special characteristics. 27

This conflicts with the right of the person affected by the measure to **effective legal protection**: if the results of the measure are transmitted to a foreign state that is not bound by Swiss law, the consequences of a violation of the IMAC can no longer be remedied. The human rights of the accused and the person affected must be reconciled with the legitimate confidentiality interests of the requesting state. The balance of interests achieved by the IMAC tends to be favorable to the persons concerned. 28

Art. 80m IMAC regulates the service of decisions by the executing authority and thus presupposes the **service of both the decision on admissibility and the final decision**, as well as any interim decisions. The time of service is not regulated. Conversely, Art. 63 para. 2 IMAC provides for minor mutual legal assistance measures that would be frustrated by prior notification. This applies in particular to the search of persons and premises. Furthermore, the subject matter of legal protection and thus the primary point of reference for the right to be heard under Art. 12 IMAC in conjunction with Art. 29 APA is not the decision to initiate proceedings, but rather the final decision under Art. 80e para. 1 IMAC. It is therefore permissible to notify the person concerned of the decision to initiate proceedings only together with the final decision. 29

30 This ensures that measures which, by their nature, are not known to the person concerned – such as questioning – remain confidential with regard to the existence and content of the request. However, before the results of the measure are transmitted to the requesting state, the **legal validity of the final decision** must be awaited in accordance with Art. 80d in conjunction with Art. 80l para. 1 IMAC. Early transmission, which preserves confidentiality vis-à-vis the person concerned in the longer term, is only possible under the extremely narrow conditions of Art. 80d^{bis} IMAC, which requires, in particular, a case of organized crime or terrorism. In this case, notification to the person concerned is postponed in accordance with Art. 80d^{bis} para. 5 IMAC, but must be made subsequently. Complete confidentiality vis-à-vis the data subject regarding the existence of a request cannot therefore be guaranteed in any case.

31 If the data subject learns of the measure – through the disclosure of a decision or otherwise – they are entitled to the rights under Art. 80b para. 1 IMAC, namely the **right to inspect the files** and the right to **participate in enforcement measures**. This jeopardizes the confidentiality of the content of the request for mutual assistance. In this respect, however, Art. 80b para. 2 lit. a and b IMAC offer the extensive possibility of complying with the request for confidentiality regarding the content of the request.

32 Pursuant to Art. 80n para. 1 IMAC, the person concerned is also entitled in principle to **inform** his client or customer, usually the accused, about the mutual assistance measure. Confidentiality can then no longer be guaranteed vis-à-vis the latter either. However, Art. 80n para. 1 clause 2 IRSG allows the competent authority to prohibit the disclosure of information to the client or customer under penalty of law, which is sometimes done in the case of disclosure orders against banks (Art. 73 para. 2 CrimPC in conjunction with Art. 292 SCC). This ensures confidentiality, at least from a legal perspective.

33 Confidentiality can therefore be guaranteed in certain respects under various individual provisions. However, there is no general provision allowing mutual legal assistance requests to be handled confidentially with the same effectiveness as domestic measures. It is questionable whether this satisfies the **requirement for adaptation under Art. 25 para. 2 CCC** in every case.

34 Para. 2 leaves the requesting state with the power to decide on non-confidential processing if the requested state cannot comply with confidentiality.

F. "Accelerated procedure" (para. 9)

Para. 9 provides for the transmission of requests without the direct involvement of the central authorities in accordance with para. 2 in "urgent cases." Communication takes place either directly between the executing authorities (lit. a and d) or via Interpol (lit. b). However, Switzerland has made use of the option provided for in lit. e and stipulates that incoming requests must – in accordance with the wording of the Convention "for reasons of efficiency" – be addressed **exclusively to the central authority**, the Federal Office of Justice. This relieves the executing authorities in Switzerland of the burden of immediately processing incoming requests. For requesting foreign states, this simplifies matters (only) insofar as they do not have to communicate via their central authority. Instead, a subordinate foreign authority may address a request to the Federal Office of Justice or the request may be forwarded to it via Interpol. 35

The purpose of Art. 27 CCC is to establish a minimum procedure between the contracting states that goes beyond non-contractual mutual legal assistance. Under no circumstances should the requesting state be placed in a worse position than if it had proceeded under its national IMAC. Requests under Art. 27 CCC may therefore also be made via the **communication channels of Art. 29 IMAC**. This includes a procedure under Art. 29 para. 2 alt. 2 IMAC, according to which the request is not addressed directly to the subordinate authority, but a copy can be sent to it at least at the same time as the request is sent to the Federal Office of Justice. 36

Para. 9 lit. e does **not** contain a **reciprocity reservation**. Subordinate Swiss authorities may therefore transmit outgoing requests under the CCC directly to subordinate authorities of other states, provided that these states have not themselves made a declaration under para. 9 lit. e. However, this does not correspond to the usual procedure in Switzerland (subject to the scope of application of international treaty provisions). 37

IV. LEGAL PROTECTION

For citizens affected by the measures that are the subject of the request, the legal protection options under Art. 25 para. 4 CCC are governed by the **national law of the requested state**. If Switzerland is requested, legal assistance must therefore be appointed under Art. 21 IMAC in certain circum- 38

stances, and the final decision may be appealed under Art. 80e IMAC. If Switzerland requests legal assistance from another state, legal protection against the measures as such is governed by the procedural law of that state. The person concerned may only appeal against the Swiss request under the conditions set out in Art. 25 para. 2 IMAC, which will not be met within the scope of Art. 27 CCC.

39 Art. 27 CCC is binding between the requesting and requested states and, if the conditions are met, creates an obligation to execute the request for legal assistance. Enforcement is governed by Art. 45 CCC, which provides primarily for a solution at the diplomatic level and, subsidiarily, for a decision by a body to be determined between the parties, namely the European Committee on Crime Problems (CDPC), an arbitral tribunal, or the International Court of Justice.

BIBLIOGRAPHY

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/cc-c25, 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., Zürch 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).

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).

MATERIALS

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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 28 CCC (Convention on Cybercrime)

A commentary by Julian Mausbach

SUGGESTED CITATION

Julian Mausbach, Commentary of art. 28 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Mausbach, art. 28 CCC N. XXX.

Article 28 – Confidentiality and limitation on use

[1] When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

[2] The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a. kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b. not used for investigations or proceedings other than those stated in the request.

[3] If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

[4] Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

CONTENT

I. Purpose 204
II. Scope (Art. 28 para. 1) 205
III. Restrictive conditions (Art. 28 para. 2) 206
IV. Impossibility of compliance with conditions (Art. 28 para. 3) 207
V. Information on use (Art. 28 para. 4) 207
Materials 208

I. PURPOSE

1 Article 28 aims to ensure mutual legal assistance while imposing **restrictions on the use of information or material.** This enables the requested party to provide particularly sensitive information or material only on a protected basis. This protection may extend to restricting the use of the information to the purpose for which the assistance is granted or to defining the recipients by stipulating that the information or material provided may not be disseminated beyond the law enforcement authorities of the requesting party. In this sense, Article 28 is to be understood as a classic mediating norm, which is committed on the one hand to the fundamental purpose of mutual legal assistance and on the other hand to the legitimate interests in the protection (of data) of the information and materials in question.

2 The mediating approach is ensured by the fact that Article 28 contains a **confidentiality obligation**. According to this, the receiving authority must treat information received from another state as confidential. This means that the information may not be made public or passed on to unauthorized third parties.

3 Furthermore, there is the **principle of purpose limitation**. According to this principle, the receiving state may only use the information for the purposes for which it was originally transmitted. This means that information may not be used for other purposes or in other proceedings without the consent of the transmitting state.

4 This is supplemented by the fact that **exceptions to the purpose limitation** are themselves subject to consent. If the receiving state intends to use the information for purposes other than those covered by the purpose limitation, it must obtain the consent of the transmitting state for this extension of purpose. This ensures that control over the use of the information remains in the hands of the state that originally provided it.

5 Art. 28 can thus be understood as a central component of international cooperation in the fight against cybercrime. It ensures that information exchanged between states is treated confidentially and used only for the intended purpose. Art. 28 thus creates a basis for the trustworthy international exchange of information and supports compliance with national and international data protection guidelines.

II. SCOPE (ART. 28 PARA. 1)

Art. 28 applies only if **there is no mutual legal assistance treaty** or agreement based on uniform or reciprocal legal provisions between the requesting and requested parties. The existing conventions and mutual assistance treaties, with regard to the taking of evidence, in particular the Convention of November 8, 1990, on money laundering, investigation, seizure, and confiscation of the proceeds of crime, the European Convention of 20 April 1959 on Mutual Assistance in Criminal Matters or the Second Additional Protocol of 8 November 2001 to the European Convention on Mutual Assistance in Criminal Matters, must be observed with regard to para. 1 and result in Art. 28 being superseded by these for quite a few mutual assistance proceedings. 6

If such a treaty or agreement is in force, its provisions on confidentiality and restrictions on use shall apply in place of Art. 28. This shall apply in any case unless the parties have expressly agreed to apply Art. 28 paras. 2 to 4. For the majority of mutual assistance proceedings involving the Swiss authorities, it can be assumed that mutual assistance within the meaning of para. 1 will be handled in accordance with the relevant conventions and mutual assistance treaties. 7

Whether and in what way there is otherwise an agreement between Switzerland and other states not party to the aforementioned mutual assistance agreements which excludes the applicability of Art. 28, establishes its own confidentiality rules or nevertheless refers to Art. 28 paras. 2 to 4 must be examined on a case-by-case basis for each country. The list of bilateral and multilateral treaties in the field of international mutual assistance in criminal matters maintained by the Federal Office of Justice is useful for this purpose. 8

If there is an agreement between the parties, only that agreement applies. Overlaps with other existing bilateral and multilateral mutual assistance treaties and similar agreements are thus avoided by the clear provision in para. 1, so that the competent authorities can adhere to the usual rules in practice and there is no need to resolve conflicts between competing or even contradictory agreements. 9

III. RESTRICTIVE CONDITIONS (ART. 28 PARA. 2)

10 Para. 2 allows the requested Contracting Party to impose two types of conditions. It may first make the information or documents available on condition that they remain **confidential** if and to the extent that the request cannot otherwise be complied with (lit. a; comparable to the confidential treatment of the identity of an informant).

11 Furthermore, the condition may be imposed that the information or documents provided may **not be used for investigations or proceedings other than those specified in the request** (lit. b).

12 The restriction on the use of the information and documents provided must be expressly requested by the requested Contracting Party. This must also apply in the same way to the condition of confidential treatment, as is already clear from the wording of the provision when it states that the transmission is made subject to a condition and that action is therefore expected from the requested party.

13 If no express statement of the condition is made, there is no such restriction on the requesting party.

14 In particular, the second condition reflects the principle of speciality enshrined in Article 67 IMAC, which is of central importance in practice, in Article 28. According to this principle, documents and information transmitted may not be used in the requesting State in proceedings for offences for which mutual assistance is not admissible, either for investigations or as evidence. In Switzerland, this prohibition also extends in particular to acts which, in the Swiss view, are of a political, military, or fiscal nature.

15 During the negotiations on the Cybercrime Convention, **two exceptions** to the possibility of restricting use were recognized. These are therefore implicitly contained in the provisions of the paragraph and are themselves restrictive in the sense that these exceptions do not carry a restriction on use.

16 The first restriction arises from the fundamental legal principles of many states, which require that information and material constituting evidence that exonerates an accused person must be disclosed to the defense or to a judicial authority. If the information or material provided constitutes such evidence, no violation of fundamental legal principles can be expected or demanded.

Similarly, a restriction does not extend to **public court proceedings.** Material transmitted under mutual legal assistance arrangements and intended for use in court proceedings that are normally public cannot be subject to a restriction on use. 17

IV. IMPOSSIBILITY OF COMPLIANCE WITH CONDITIONS (ART. 28 PARA. 3)

Para. 3, in turn, establishes an obligation on the requesting party to respond immediately to a condition if it cannot comply with it. The requesting party must **immediately inform** the requested party of this circumstance. The latter, in turn, is entitled to examine and decide whether it nevertheless wishes to provide the information, and thus in the knowledge that the condition cannot be met, i.e., ultimately unconditionally. In this context, adherence to the principles of mutual legal assistance may be required and assumed, which, in view of the decision, means that, in the interests of fairness to the requested party, it is entitled to exercise any discretion available to it in this regard. 18

If no immediate notification is given that a condition cannot be met, that condition shall remain in force as a binding condition, as in the case of express acceptance of the condition. 19

V. INFORMATION ON USE (ART. 28 PARA. 4)

Para. 4 represents a **control level**. The party sending the information or material is enabled to obtain an overview of how the information and materials provided under a condition in para. 2 have been used. To ensure this, the requested party may require the requesting party to provide information on the use of the information or documents. This information must be sufficiently detailed and comprehensive to enable compliance with the conditions to be verified. 20

Ultimately, this not only serves to monitor the requesting party, but also ensures that the requested party can fulfill its obligations – in particular, the obligation to ensure that there is no violation of Art. 67 IMAC. 21

MATERIALS

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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 29 CCC (Convention on Cybercrime)

A commentary by Simon Bächtold

SUGGESTED CITATION

Simon Bächtold, Commentary of art. 29 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Bächtold, art. 29 CCC N. XXX.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

[1] A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

[2] A request for preservation made under paragraph 1 shall specify:

a. the authority seeking the preservation;

b. the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c. the stored computer data to be preserved and its relationship to the offence;

d. any available information identifying the custodian of the stored computer data or the location of the computer system;

e. the necessity of the preservation; and

f. that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a. the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b. the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall

promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

[7] Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

CONTENT

I. Introduction 213
A. Multinational and collaborative prosecution of cybercrime 213
B. Practical significance and related articles 213
II. Condition of double criminality (Art. 29 para. 3 and 4 CCC), exclusion of political prosecution (Art. 29 para. 5 lit. a CCC) and violation of public policy (Art. 29 para. 5 lit. b CCC) 215
III Securing and collecting data abroad 216
A. Making a preservation request 216
1. the requesting authority (lit. a.) 216
2. The offense that is the subject of the criminal investigation or proceedings and a nutshell statement of the facts (lit. b.) 216
3. The stored computer data to be secured and the connection between them and the offense (lit. c.) 217
4. All available information to identify the custodian of the stored computer data or the location of the computer system (lit. d.) 217
5. The necessity of the preservation (lit. e.) and the intention of the contracting party to submit a request for mutual legal assistance (lit. f.) 217
B. Forwarding and processing of the preservation request 218
C. Distinction from the Information Request 219
D. Prosecution by means of letters rogatory 220
E. Best practices for letters rogatory to the USA 220
IV. Execution of Preservation Requests by Swiss authorities 222
A. Procedure and responsibilities 222
B. Implementation under Swiss law 222
Bibliography 225
Materials 225

I. INTRODUCTION

A. Multinational and collaborative prosecution of cybercrime

Criminals use the **Internet** to commit crimes for two main reasons. On the one hand, to remain anonymous. On the other hand, to scale their criminal business model cost-effectively, i.e. to reach a large number of potential victims (especially cyber fraud). In addition, there are those computer crimes in the narrower sense that are inconceivable in the analog world (e.g. hacking, DDOS attacks, etc.). 1

In line with the nature of the Internet as a global communication network, cybercrime always takes place **internationally**. As a rule, organized criminal groups operate worldwide, or at least - from a Swiss perspective - Europe-wide, and in some cases only in specific language regions (e.g. German-speaking countries). This means that no state can fight cybercrime alone. Cyber investigations almost always have to be conducted internationally or have cross-border aspects. Large and complex investigations are referred to as international criminal prosecutions. The contrast to this in (Swiss) criminal prosecution could not be clearer. Due to the primary responsibility of the cantons for criminal prosecution, a great deal of resources are still lost in this country to clarify national jurisdiction. A national situational picture of cybercrime phenomena exists at best in rudimentary form. 2

Anyone investigating in the cyber area will generally not be able to avoid Art. 29 CCC (Preservation Request / immediate seizure of data). 3

B. Practical significance and related articles

Art. 29 CCC, together with Art. 32 lit. b CCC, is one of the most practically relevant provisions of the Cybercrime Convention, at least from the perspective of law enforcement authorities. 4

The Preservation Request is intended to solve the problem that electronic data is volatile and is often stored abroad, but legal assistance proceedings are regularly very lengthy. From the point of view of law enforcement, this is aggravated by the fact that many countries do not have a so-called "data retention policy", which can lead to data relevant to investigations being lost before a request for mutual legal assistance can even be made. Preservation requests 5

are therefore intended to enable data relevant to criminal prosecution to be **secured** abroad quickly and easily so that the requesting state has time to make the data available through mutual legal assistance channels.

6 In contrast to the information request pursuant to Art. 32 lit. b CCC, which can be submitted at a low threshold and without disadvantages or costs for the requesting state, the requesting state, which invokes Art. 29 CCC, undertakes to actually request the data secured abroad later by means of a **request for** mutual legal assistance. A request for mutual legal assistance involves a certain amount of effort for the requesting public prosecutor's office, so that the public prosecutor's office will not make preservation requests lightly.

7 The question of the **legal nature** of a preservation request arises time and again. This is the case, for example, if it is still unclear after a criminal complaint has been filed whether there is sufficient initial suspicion to open criminal proceedings (Art. 309 para. 1 lit. a CrimPC). Only then are coercive measures by the public prosecutor possible and justified. If the preservation request were not a coercive measure, it would be possible for the police to submit a preservation request on their own initiative, which would be welcome in terms of the intention, because the faster a data preservation is carried out, the more successful it is likely to be. The question of the legal nature of the request is not answered by the Cybercrime Convention itself, but is governed by the law of the requested state (Art. 25 para. 4 CCC). The answer can therefore vary. For Switzerland, it is argued that the police may not, in principle, submit a preservation request without the consent of the public prosecutor's office, because the latter is then obliged to submit an international request for mutual legal assistance at a later date (which is only possible if criminal proceedings have been opened). The request for immediate data preservation also results in a temporary seizure of records, which would constitute a coercive measure in domestic proceedings. In fact, a preservation request must therefore be treated in the same way as a **coercive measure in criminal proceedings**. As a consequence, a preservation request must be ordered by the public prosecutor's office, whereby the execution can be delegated to the police. In domestic cases, however, a temporary seizure by the police is permitted as an exception if there is "imminent danger" and the public prosecutor's office cannot be informed in good time (not even verbally) (Art. 263 para. 3 CrimPC). In such exceptional cases, the police may also make requests autonomously in accordance with Art. 29 CCC.

Mention should also be made of Art. 16 CCC, which requires member states to create the necessary legislative and organizational conditions so that preservation requests from foreign states can be complied with in accordance with Art. 29 CCC. In the course of implementing the Convention, Switzerland decided not to enact any new criminal procedure law in this regard (see below, n. 32). 8

II. CONDITION OF DOUBLE CRIMINALITY (ART. 29 PARA. 3 AND 4 CCC), EXCLUSION OF POLITICAL PROSECUTION (ART. 29 PARA. 5 LIT. A CCC) AND VIOLATION OF PUBLIC POLICY (ART. 29 PARA. 5 LIT. B CCC)

The Cybercrime Convention strives to promote international cooperation in the prosecution of cybercrime as much as possible. For this reason, the Convention itself does not contain a requirement of dual criminality, but leaves it up to the contracting states to provide assistance if only the requesting state criminalizes a corresponding offence (Art. 29 para. 3 CCC). States parties are free to make a reservation at the time of ratification that double criminality is a prerequisite. In this case, the requested state may refuse a preservation request if it is already clear at this point that the data requested for preservation cannot be released by way of mutual legal assistance (Art. 29 para. 4 CCC). Of the 70 states that have ratified the Convention, 23 have made a corresponding reservation, including Switzerland and the United States of America. Because the USA and its federal states do not have a criminal offense analogous to our **defamation offenses**, legal assistance in this regard is always excluded and consequently no preservation request is accepted. 9

Irrespective of the question of double criminality, the Cybercrime Convention excludes the Preservation Request for politically motivated prosecution (persecution) (Art. 29 para. 5 lit. a CCC), which should be self-evident from a Swiss perspective. The same applies if the requested contracting party is of the opinion that the execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests (Art. 29 para. 5 lit. b CCC). 10

III SECURING AND COLLECTING DATA ABROAD

11 From a Swiss perspective, Art. 29 CCC is particularly relevant for the collection of computer data abroad (see below, n. 12 et seq.). However, the article also applies to requests from foreign states to Switzerland (see below, n. 31 et seq.).

A. Making a preservation request

12 The Convention text itself provides quite detailed instructions on how to formulate a preservation request. The following requirements are explicitly stated:

1. the requesting authority (lit. a.)

13 In practice, this will usually be a **public prosecutor's office** (see also n. 7 above). From the Convention's point of view, however, there is nothing to prevent the police from submitting a preservation request in close consultation with the public prosecutor's office (which must later submit the request for mutual legal assistance). Since the aim is to secure volatile data in good time, this may even make sense. The implementation of the preservation request or its legal qualification depends on the national law of the requested state (Art. 25 para. 4 CCC). In many requested states, the implementation of the preservation request (seizure of data at the storage location) will be qualified as a coercive measure, so that a request - or at least a (co-)signature - from a public prosecutor is often required. Overall, the handling is very inconsistent.

2. The offense that is the subject of the criminal investigation or proceedings and a nutshell statement of the facts (lit. b.)

14 The point here is for the requested state to be able to recognize whether **double criminality** is fulfilled (see above, n. 9) and whether the request, which may well involve considerable effort, is proportionate (purpose/means relationship). In the case of common phenomena, however, a description of two or three sentences is sufficient to meet the requirement.

3. The stored computer data to be secured and the connection between them and the offense (lit. c.)

It must be substantiated which specific data is to be secured (e.g. registration data, log files/edge data or even content data, if possible and reasonable also stating the file formats). In particular, however, reasons should be given as to *why* this data actually has a **connection to the** facts giving rise to the **suspicion**. This criterion is similar to the so-called potential relevance of evidence in the context of a domestic search pursuant to Art. 246 CrimPC (according to which "it is to be assumed" that the records in question contain information that can be seized); here, the data only has to be "potentially relevant" or not appear "obviously unsuitable". *Fishing expeditions* are frowned upon. The criterion is taken very seriously and careful justification is required. It should be borne in mind that in other countries the authority to seize and/or hand over data does not lie with the public prosecutor's office, but must be ordered by a compulsory measures court. For example, in practice-relevant dealings with the USA, the Department of Justice must apply to a court in order to order the surrender of data from a service provider by means of a search warrant. This requires a substantiated and (depending on the circumstances) substantiated presentation of the offense connection with the essential documents (in English). The level of substantiation required here goes well beyond what Swiss public prosecutors are used to under national criminal procedure law. In practice, the US authorities at least consult with the requesting authority if the level of substantiation of the request is not yet sufficient and provide the opportunity to substantiate the preservation request in more detail. 15

4. All available information to identify the custodian of the stored computer data or the location of the computer system (lit. d.)

As a rule, this should simply refer to the **company** to which the specific addressing element is assigned. For example, Google for @gmail email addresses, Meta (for Facebook, Instagram and WhatsApp) etc. 16

5. The necessity of the preservation (lit. e.) and the intention of the contracting party to submit a request for mutual legal assistance (lit. f.)

The request must explicitly state that the request is **necessary** (in terms of subsidiarity and proportionality) and it must be confirmed that the requesting 17

authority is willing to follow up on the preservation request by means of a request for mutual legal assistance.

B. Forwarding and processing of the preservation request

18 Irrespective of the wording of the Cybercrime Convention, in practice there are **two ways** in which a preservation request can or must be submitted. The typical route is via the 24/7 network in accordance with the Convention text (Art. 35 CCC). Each signatory state has undertaken to operate a contact point that is ready to receive preservation requests around the clock, seven days a week. In Switzerland, this role is assumed by the Federal Office of Justice together with the Federal Office of Police (fedpol).

19 For reasons of efficiency (avoidance of media disruptions, automation), however, many large providers of internet-based communication services have started to operate their own Law Enforcement Request Systems (LERS), which the law enforcement authorities can use to record their requests directly in a standardized manner and track progress without having to involve other state authorities (e.g. Federal Office of Justice / Department of Justice). It makes sense, and has been implemented in some cantons, for a central office
at the police or public prosecutor's office to manage access to all available **LERS portals**, and to submit and administer preservation and information requests on behalf of the case managers. In this way, experience in dealing with the various service providers can be collected and evaluated centrally and case managers have competent contacts to discuss the prospects of success of the corresponding requests in advance.

20 Alternatively, law enforcement authorities have the option of sending their requests to the **Federal Office of Police** (fedpol) by e-mail (encrypted and authenticated). The requests are checked there, supplemented by queries if necessary, translated and forwarded to the competent authority abroad. English is generally recommended as the language for preservation requests worldwide. The fedpol coordination office can also be asked whether other Swiss law enforcement authorities have already submitted the same Preservation Request, which can provide valuable information with regard to the coordination of ongoing investigations (or the possibility of submitting a request for jurisdiction to the other canton).

C. Distinction from the Information Request

What is the difference between a preservation request and an information request pursuant to Art. 32 lit. b CCC? In this regard, reference should first be made to the commentary on Art. 32 CCC. In a nutshell, the information request involves the **voluntary disclosure** of data to a CCC partner state directly by the service provider. In practice, "voluntariness" refers to the service provider and only indirectly to the user/customer of the service. Users will regularly stipulate in their terms of use that data may be forwarded to law enforcement authorities; in specific cases, the customers concerned are no longer asked. Voluntariness on the part of users is relative in that many services simply cannot be used without consent to the terms of use (and thus to the forwarding of data to law enforcement). 21

Although the Cybercrime Convention does not recognize this restriction, according to the national law of the relevant partner states, an information request can generally only include registration data (also: "subscriber information") in accordance with Art. 18 para. 3 lit. b CCC (e.g. name, date of birth, address, user name, billing address, e-mail addresses, IP address at registration) and marginal data ("traffic data", e.g. the IP history), but generally **no** content data. The term "content data" refers to the content of a communication, e.g. a message, a post, media files, etc. Registration data is by far the most frequently clarified. Information and preservation requests are often made at the same time, as it is uncertain which data the service provider will provide voluntarily. 22

In practice, information requests are made at a much lower threshold because this does not oblige the public prosecutor's office to issue a request for mutual legal assistance. Such a request is also not necessary because the disclosure of the data is voluntary and is answered directly by the service provider. The **willingness** of service providers to cooperate depends heavily on the type of offense. The services are regularly particularly willing to cooperate in the case of sexual offenses, especially those involving children. Offenses against property are more problematic. At the lower end of the scale are defamation offenses, where cooperation regularly fails due to the requirement of double criminality (see above, n. 9 and n. 14). 23

D. Prosecution by means of letters rogatory

24 As already mentioned several times and also explicitly stated in the Convention text, the public prosecutor's office undertakes with the Preservation Request to request the seized data by means of mutual legal assistance. There are certainly cases where it turns out in retrospect that data that was initially secured has since become obsolete. There are also no direct consequences of **not requesting mutual legal assistance** (e.g. there are no cost implications). However, it is generally expected that public prosecutors' offices comply with this obligation under Convention law in order not to jeopardize good cooperation between Convention states.

25 The data is frozen for **at least 60 days** (see Art. 29 para. 7 CCC). The specific duration is specified in the written confirmation of the preservation request and is usually longer. The requesting authority can usually also request an extension of the deadline. The request for legal assistance must be formally submitted within the deadline.

E. Best practices for letters rogatory to the USA

26 Due to their great practical importance, the best practices for letters rogatory to the USA are discussed below. The following explanations are based on the "Practical Guide for Requesting Electronic Evidence Across Borders", published by UNODC, CTED and IAP, as well as on our own experience.

27 Requests for mutual legal assistance addressed to foreign authorities in cybercrime cases must contain the following information:

- Language of the request: requests for mutual legal assistance should ideally be entered directly in English, otherwise they should be translated;
- Facts of the case: must be described briefly but in a nutshell, stating the place of the crime (or the place where it was committed), the exact time of the crime and the manner in which it was committed;
- Any modus operandi: must be described in detail;
- Legal description of the offense, including the wording of the applicable articles of law;
- Reasons for the request, in particular showing the connection between the proceedings being conducted and the requested measures;

- The evidence sought or actions requested must be specified in detail (e.g. handing over the account statements relating to account X for the period A to B, obtaining documents from provider Y from which the registration data and log files for the remote ID 12345678 for the period between A and B can be seen, etc.);
- Explanations regarding any preservation request already submitted, whereby all reference numbers communicated following the preservation request must be listed in the request (CCIPS and reference numbers of fedpol, the requested foreign police authority and the requested foreign public prosecutor's office).

In order to obtain content data from US service providers, the Department of Justice must obtain a search warrant under US law from a court. The standard of proof is "*probable cause*". This means that the court must be convinced that the user account in question probably still contains evidence relevant to the offense (unless the data has already been provisionally seized on the basis of a preservation request). There must also be a solid foundation of evidence for the assumption that an offense has been or will be committed and that the evidence of the offense will be found in the requested user account. The sources of the submitted evidence must be trustworthy (e.g. police reports, trustworthy private sources). Central evidence should be provided. If circumstantial evidence is provided, it must be translated into English. In summary, it must be explained why the account holder is a target of the investigation, why it is assumed that the user account in question belongs to this person, and what evidence is expected to be obtained from this user account. 28

The request for mutual legal assistance must be sent either through diplomatic channels via the Federal Office of Justice or - if agreed and provided for - directly to the public prosecutor's office abroad. The legal assistance guide of the Federal Office of Justice contains more detailed information on the specific transmission channels. 29

Note: 30

- For requests for mutual legal assistance in cybercrime cases, the CCC must also be entered as the legal basis (provided the target country has ratified the Convention).

- The presentation of the facts, the subsumption of the facts under the elements of the offense and the reasons for the request are the be-all and end-all of a request for international legal assistance.
- Detailed information on mutual legal assistance can be found in the Federal Office of Justice's Guide to Mutual Legal Assistance, with templates in various languages and a country index.
- A request for mutual legal assistance following a preservation request must be made as soon as possible, at the latest within the deadline for the sequencing of requests (Art. 29 para. 7 CCC).

IV. EXECUTION OF PRESERVATION REQUESTS BY SWISS AUTHORITIES

A. Procedure and responsibilities

31 All states that have ratified the Cybercrime Convention have indicated which of their authorities acts as the central point of contact for requesting states ("24/7 network", Art. 35 CCC). According to Switzerland's declaration, this is primarily the Federal Office of Justice. However, the Federal Criminal Police (fedpol) is responsible for matters relating to the Cybercrime Convention, in particular for preservation requests (the Federal Office of Justice forwards such requests to fedpol). Fedpol receives around **200 requests** per year from abroad, which it in turn forwards to the cantonal police forces for processing.

B. Implementation under Swiss law

32 The process by which a foreign preservation request is processed in Switzerland is **not regulated by law**. It is remarkable how little the dispatch on the implementation of the Cybercrime Convention deals with procedural and practical issues. It merely mentions that the contracting states are not obliged to create further legal instruments in addition to seizure and disclosure.

33 Swiss criminal procedure law **does not recognize "Preservation Orders"** in the sense of the Cybercrime Convention. A preservation order would be an official order to a service provider to keep data available for a certain period of time (typically in the sense of a back-up). As this instrument is not provided for in the Criminal Procedure Code, the long-term availability of the data must be ensured in another way, which can only be done by means of an edi-

tion (Art. 265 CrimPC). As the cantonal police forces have no authority to edit data, they must forward the corresponding requests they receive from fedpol to the competent public prosecutor's office, which then issues an editing order. While the Code of Criminal Procedure has no basis for preservation orders, the legally prescribed retention of data in the telecommunications sector has been implemented in a similar way. It is the telecommunications service providers themselves who must retain their customers' registration and communications edge data for the prosecution authorities for a period of 6 months (Art. 21 para. 2, Art. 22 para. 2 and Art. 26 para. 5 BÜPF).

This Swiss formulation of the preservation request in accordance with Art. 29 CCC is relatively far removed from the spirit of the Convention, which intended a quick, uncomplicated measure with the least possible restrictions for all parties involved. The process outlined above involves at least three authorities and the company addressed, i.e. numerous interfaces, which leads to delays and inevitably increases the susceptibility to errors. A disclosure order, combined with the physical or digital delivery and storage of - possibly very substantial - volumes of data, also means a **considerable amount of work** for service providers and the authorities responsible for data storage. There is an international debate as to whether countries that have not introduced preservation orders within the meaning of the Convention and instead make do with disclosure orders (such as Switzerland) fulfill the requirements of the Convention at all. Although the majority of respondents seem to agree with this, there are still points of criticism, namely with regard to higher legal hurdles (not in Switzerland), longer proceedings and the possible increased risk that the persons concerned will find out about the measure, which can frustrate the purpose of the investigation. 34

The execution of foreign preservation requests in Switzerland is not yet part of formal mutual legal assistance proceedings and is also not a precautionary measure under the IMAC (or other principles of mutual legal assistance law). It is upstream of any mutual assistance proceedings. In fact, not every preservation request is likely to be followed by a formal request for mutual assistance. The Preservation Request is based on the Cybercrime Convention itself (which is directly applicable in Switzerland's monistic system, provided it is sufficiently specific). The implementation of the Preservation Request here is not sufficiently specific, which is why - as mentioned above - recourse must be made to the legal institutions of national criminal procedure law, i.e. the 35

Code of Criminal Procedure (e.g. Art. 265 CrimPC, Edition) as well as the BÜPF and its ordinances (e.g. Art. 38 VÜPF, IR_8_IP (NAT): Holders of IP addresses). This is always with the aim of living up to the spirit of the Cybercrime Convention (rapid, uncomplicated, effective prevention of the loss of evidence) as much as possible. This also means that disclosure orders issued to execute a preservation request must be accompanied by a **prohibition on** disclosure to the disclosure addressee so as not to jeopardize the success of the investigation (Art. 29 para. 6 CCC; Art. 73 para. 2 CrimPC in conjunction with Art. 292 SCC; cf. Art. 292 SCC; cf. analogously also Art. 11b para. 2 lit. c IMAC and Art. 80b para. 2 lit. a IMAC). The consequence of this is that the persons concerned cannot yet appeal against the execution itself at the time of execution due to a lack of knowledge. As soon as (if) formal legal assistance proceedings are opened, the data owners (the affected customers of the service) must be informed of their right to seal (Art. 9 IMAC in conjunction with Art. 248 para. 2 CrimPC). However, if no request for mutual legal assistance is received within 60 days in accordance with Art. 29 para. 7 CCC and any reminder/extension of the deadline, the data must be irrevocably deleted due to the lack of a legal basis for longer storage.

36 According to the current legal situation, the service provider itself has its own right to seal the data as the holder of custody of the data (see Art. 248 para. 1 CrimPC). However, sealing by the service **provider** could lead to pointless expense, namely if a time-consuming unsealing procedure has to be carried out and the requesting state subsequently waives the legal assistance procedure. In addition, the service provider's own confidentiality interests are often not affected by the disclosure. However, this would be a prerequisite for a valid sealing request, as sealing cannot be requested on behalf of a third party (such as the account holder). On the other hand, if data is collected from service providers who, due to the nature of their service, can regularly be expected to have data protected by secrecy, the question arises as to whether the public prosecutor's office, which executes the preservation request (issues the disclosure order), would not already have to seal the data ex officio at the time of disclosure. In both cases, however, the public prosecutor's office would have to submit a request for unsealing within 20 days in order to execute the preservation request (Art. 248 para. 3 CrimPC), at a time when the data owner should not yet be aware of the preservation request and should therefore not be included in the unsealing procedure (quite apart from the fact that he will regularly not have a domicile for service in Switzerland).

In order not to jeopardize the success of the investigation and to avoid unnecessary idle time, the only consistent approach in the context of the Cybercrime Convention would therefore be for sealing/unsealing to be applied only in the context of formal mutual legal assistance proceedings. In any case, sealing can only be possible once the data collection as such has been completed. For example, data collection that is based on a single preservation request but requires several consecutive steps in Germany, e.g. several requests for information to the PTSS (1st determination of addressing element based on IP address, 2nd determination of subscriber based on addressing element). 37

The question arises as to whether it would be permissible under Swiss law to oblige service providers to merely retain certain data, even outside the scope of application of the BÜPF, instead of handing it over. This would alleviate many of the previously discussed problems with the edition and would therefore be a good thing. However, a real **increase in efficiency** could be achieved above all if the enforcement of foreign preservation requests were centralized at federal level (fedpol), for which there is currently no basis in the Criminal Procedure Code (cf. Art. 22 et seq. CrimPC *e contrario*). However, a comparable legal basis can already be found today in Art. 18 para. 2 IMAC, according to which the Federal Office of Justice can itself order precautionary protective measures if there is imminent danger. 38

BIBLIOGRAPHY

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.

MATERIALS

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

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 32 CCC (Convention on Cybercrime)

A commentary by Damian K. Graf

SUGGESTED CITATION

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

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

Art. 32 Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority todisclose the data to the Party through that computer system.

CONTENT

I. General 231
A. Introduction, genesis, purpose, and critique. 231
B. International Law Foundation: Principles of Territoriality and Sovereignty (Art. 31 CCC) and their Breach (Art. 32 CCC) 235
C. Materials and Interpretation 237
D. Legal Nature 238
E. Scope of Application 238
F. Practical Relevance 241
II. Access to publicly available data stored in another contracting state ("open source") (lit. a) 242
A. Publicly accessible data 242
B. Legal Nature: Qualification as Interference with Fundamental Rights? 244
C. Prerequisites for permissible data access under Swiss criminal procedure law. 246
III. Access to other data stored in another contracting state (lit. b) 247
A. Lawful and voluntary consent of the person lawfully authorized to disclose the data 247
1. Authorization to disclose 247
2. Consent 249
B. Consequence of legally valid consent 251
C. Prerequisites for permissible data access under Swiss criminal procedure law.. 251
IV. Preservation of evidence beyond Art. 32 CCC according to the access principle. 254
V. Consequences of the Violation of Foreign Sovereignty Law 257
VI. Need for Reform 258
Bibliography 259
Materials 265

I. GENERAL

A. Introduction, genesis, purpose, and critique.

Given the ever-increasing shift of communications to Internet services (such as email, social media, and Internet telephony) and the technological evolution away from local storage to "cloud computing," the investigative focus of law enforcement has also changed. Their work is becoming increasingly complex as a result of this shift of evidence to the digital world. This complexity is due, on the one hand, to the fact that data is volatile in nature, can easily be moved across borders (which can also be done automatically, for example, to improve the utilization of computer systems), and is accessible to encryption. On the other hand, leading providers of Internet services that can hardly be dispensed with (such as Google, Facebook or Meta, WhatsApp, X or Microsoft) usually operate from abroad (especially the USA) and offer their services from there to natural and legal persons in Switzerland, while their user data is stored abroad. As a result, investigating authorities regularly have to turn their attention beyond national borders, even in domestic cases. In EU member states, a cross-border request to obtain electronic data is already made in over 50 percent of all criminal investigations. This poses some challenges for law enforcement authorities, not least of an international law nature, since extraterritorial evidence gathering constitutes prima vista an interference with the sovereignty of the other state (see below, n. 10 ff.). 1

In this cross-border context, authorities must be provided with effective powers of intervention that enable them to secure the evidence necessary for domestic criminal proceedings. Meanwhile, mutual legal assistance as a traditional mechanism of international cooperation is considered inefficient and sluggish, especially when it comes to volatile data or data that can be moved, deleted, or manipulated without particular effort. Investigators usually do not know in which country the data is stored or, depending on the Internet service provider, in which country the data is stored at all, which means that at the time of access they can often neither judge whether they are crossing the "digital state border", nor can they see in which country mutual assistance is to be sought at all - and even if the investigators have identified a country, they need a minimum of information (e.g. a user account or an IP address) to justify 2

a request for mutual assistance in a promising way. a user account or IP address), which can also prove difficult at times.

3 The need for cross-border preservation of evidence was already recognized in the 1990s, and on September 11, 1995 - at a time when today's technical possibilities were only foreseeable in some popular literature - the Council of Europe adopted Recommendation No. R (95) 13 on the problems of criminal procedure law in connection with information technologies. Its para. 17 reads as follows: "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." In implementation of this recommendation, negotiations then began on a convention on cybercrime. The acceleration of international cooperation and the possible granting of cross-border powers in violation of the principle of sovereignty were among the key issues.

4 Article 32 of the Cybercrime Convention ("CCC"), which was ultimately adopted, permits access to data stored in other contracting states in two constellations, without the need for a request for mutual legal assistance addressed to the authorities of the other state: first, if publicly accessible data are involved (lit. a), and second, if the authorized person has given his consent to the access (lit. b). In other words, Art. 32 CCC allows in these cases a direct seizure of data stored abroad without first obtaining the consent of the state concerned and without having to go through the (rocky) legal assistance route before or after collection. The administrative ballast is completely eliminated, since the other state does not have to be informed about the collection of evidence. If the requirements of Art. 32 CCC are not met, namely if the authorized person does not cooperate, or if a collection is technically not possible or cannot be enforced for other reasons, then, in application of Art. 31 CCC, the ordinary legal assistance route must be taken as a subsidiary measure, if necessary combined with a request for immediate preservation of evidence within the meaning of Art. 29 CCC, if a loss of evidence threatens to occur.

5 In the consultation and legislative process for the implementation of the CCC in Switzerland, Art. 32 CCC did not give rise to any comments, despite the

terms used therein that are subject to interpretation and the associated encroachment on sovereignty.

The thrust of Art. 32 CCC has not remained uncriticized elsewhere, on the one hand because of the accompanying abolition of the protection of fundamental rights guaranteed by territorial sovereignty, without the domestic authorities even becoming aware of such encroachments on fundamental rights. Art. 32 CCC allows uncontrolled foreign sovereign acts on the territory of the state, which interferes with the constitutional rights of the affected persons and third parties, and is disproportionate and sensitive, especially with regard to states with a clouded human rights situation. However, the facilitation of the collection of evidence in criminal proceedings associated with Art. 32 CCC is indispensable in the prosecution of crimes with a digital component: Our lives - and thus those of suspects - have become digital and increasingly do not take place in the digital space attributable to Swiss territory. It is true that most electronic devices today still have their own, often generous, local memory which, if the device can be seized in Switzerland, can be seized, searched (Art. 246 CrimPC) and confiscated (Art. 263 CrimPC) on the basis of the general rules of criminal procedure. The trend, however, is moving away from local storage to cloud-based or dislocal solutions, the storage location of which will be somewhere in the world, or at least only a fraction in Switzerland (with the exception of special industries such as banking and consulting). Communication nowadays also regularly takes place via social media and comparable Internet services, with the content sometimes not even being stored locally on the user's own device. By allowing the domestic law enforcement authorities of a contracting state, in particular, to request foreign Internet service providers to hand over data directly, avoiding the mutual legal assistance route (cf. below, n. 48, 55), Art. 32 CCC ensures, at least in part, that the substantive establishment of truth in the case of crimes with a digital component does not become entirely illusory. 6

On the other hand, law enforcement circles in particular consider Art. 32 CCC to be too restrictive: as the "lowest common denominator," Art. 32 CCC represents an ultimately unrevolutionary compromise. Discussions on the admissibility of cross-border evidence gathering beyond Art. 32 CCC failed, however, due to the lack of consensus within the Council of Europe. Even in the discussions that have continued since then, there has largely been no consensus, although the majority of states consider the transfer of evidence beyond na- 7

tional borders to be one of the central challenges of territorial state criminal prosecution. Even with the II. Nevertheless, it is to be permitted to request service providers abroad directly and without detour via mutual legal assistance to hand over registration information on domain names as well as inventory data (Art. 6 and 7 ZP II-CCC). Switzerland has not yet signed or ratified ZP II-CCC, which, according to sources in the Federal Office of Justice, is not expected to happen in the near future - on the one hand, because the new regulation would again affect the principle of sovereignty, and on the other hand, because discussions on this topic are being held at the level of the United Nations, which would have to wait. In fact, discussions on a United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes ("UN Treaty on Cybercrime") are at an advanced stage. However, the current draft, which is supported by the majority, does not provide for the cross-border collection of evidence, which is why it does not seem appropriate to wait until ZP II-CCC has been signed and ratified.

8 One step further than Art. 32 CCC is the recently adopted EU Regulation (EU) 2023/1543 on European surrender orders and European preservation orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings of 12.7. 2023 ("e-Evidence Regulation"), according to which judicial authorities of a Member State may request electronic evidence directly from a service provider in another Member State (Art. 1 para. 1 e-Evidence Regulation) and the service providers are legally obliged to redact the data within 10 days or the set time limit (Art. 10 e-Evidence Regulation). Art. 32 CCC, on the other hand, relies on the voluntary nature of foreign service providers - if they do not comply with the request or do not comply completely, the mutual assistance route must be taken, even in the case of arbitrary, opaque or unfounded refusal to cooperate. Art. 18 para. 1 lit. b CCC at least provides that the Internet service provider that offers its services "in the territory of the contracting party" must hand over inventory data in connection with these services upon request. However, the Federal Supreme Court does not permit an order to disclose data to a foreign provider on the basis of Art. 18 para. 1 CCC, or at most considers such an order to be lawful if it is addressed to its Swiss branch, provided that the latter either possesses or controls the data.

The criticism of the limitations of Art. 32 CCC, which was voiced primarily in law enforcement circles, has become somewhat quieter in Switzerland. This is because the fact that the international community has so far failed to find a consensual solution has not prevented the Federal Supreme Court (probably for reasons of practicability, albeit in disregard of the principle of sovereignty) from also permitting transnational collection of evidence from data without the consent of the authorized persons, with implicit recourse to the so-called access principle (see below, n. 63 ff.). 9

B. International Law Foundation: Principles of Territoriality and Sovereignty (Art. 31 CCC) and their Breach (Art. 32 CCC)

The principle of territoriality represents a barrier to state action that is removed from sovereignty under international law. It not only serves to limit the applicability of domestic criminal law to foreign situations - although there are exceptions to this - but also limits state action to its own territory. The performance of official acts on foreign territory is not completely prohibited. However, unless such conduct is expressly permitted by international (mutual legal assistance) agreements, bilateral treaties or at least ad hoc authorizations, it constitutes an inadmissible encroachment on state sovereignty and may be punished accordingly under foreign law. Unauthorized official acts on foreign territory are also sanctioned under Swiss law (Art. 299 SCC; see also Art. 271 SCC). Evidence gathered in violation of the principle of territoriality may also not be used in domestic criminal proceedings (see below, n. 69 ff.). 10

In particular, "arbitrary acts of coercion and intervention on foreign territory" violate state sovereignty and are therefore contrary to international law. Thus, unless the legal assistance of the foreign state is used for this purpose, arrests of persons abroad by Swiss officials are inadmissible, as is the conduct of interrogations, the taking of visual examinations or the direct execution of judgments. The same applies, according to the Federal Supreme Court, to the sending of summonses to accused persons domiciled abroad, which may not be accompanied by threats of coercion, i.e. they are to be designed as mere invitations. It thus seems clear that the prosecution authorities may not physically collect evidence abroad or carry out procedural acts there without going through the legal assistance channel or without such acts being explicitly permitted in an agreement. Unauthorized house searches or the seizure and 11

search of electronic devices or documents on foreign territory are thus undoubtedly prohibited.

12 Evidence-gathering situations in which the criminal authorities are not physically present on foreign territory but carry out investigative actions in Switzerland that affect the foreign territorial sovereignty are no different. This includes, for example, the observation of persons on the German side of the Rhine by Swiss police officers from Schaffhausen, as well as the video interrogation of a defendant abroad by a Swiss court. Such conduct also violates international law, since its effects are equivalent to an act of sovereignty directly on foreign territory.

13 Access to computer systems abroad from a location in Switzerland and thus the seizure of data stored abroad also qualify as such extraterritorial acts of sovereignty. The community of states also claims sovereignty with regard to data processing systems stationed on its own territory and the data stored there. National search powers cannot legitimize such encroachments on foreign sovereign rights. This has once been recognized in principle by the Federal Supreme Court (cf. however below, n. 63 ff.) and is also reflected in particular in the (intensive) discussions on the content or further development of the CCC.

14 As soon as the sovereignty of a foreign state is to be encroached upon in such a sense, the state must consequently consent, either by providing mutual legal assistance upon individual request or by granting international partners the authority to act accordingly by treaty or on an ad hoc basis. Examples of the partial surrender of Swiss sovereignty can be found in agreements with neighboring countries on police "hot pursuit" or, to a limited extent, in the context of the Cybercrime Convention. This is because the creation of Art. 32 CCC dispensed with the need for a request for mutual legal assistance in two constellations: On the one hand, access to publicly accessible stored computer data is permissible, regardless of where the data is geographically located (lit. a). On the other hand - and very broadly compared to other mutual legal assistance accords - according to Art. 32 lit. b CCC, a Party may "access or receive stored computer data located in the territory of another Party by means of a computer system in its territory if it obtains the lawful and voluntary consent of the person lawfully authorized to disclose the data to it by means of that computer system." This legitimizes not only a direct request to foreign providers to hand over information, but also the authorities' own access

through existing user accounts (see below, n. 55). In other words, the CCC sets out in binding terms for the contracting states under which circumstances authorities can directly access data located abroad (i.e. under the conditions of Art. 32 CCC) and when they are obliged to make a formal request for mutual assistance (in all other cases; Art. 31 CCC). This shows that access to foreign data, regardless of the fact that members of law enforcement agencies are not physically present on foreign territory during such evidence-gathering measures, is considered an intrusion on sovereignty in principle. Indeed, in the course of drafting the CCC, it just emerged "that no consensus could be reached for more far-reaching rules under which conditions unilateral access by one State to data located in another State Party may occur without authorization by that State Party."

C. Materials and Interpretation

The terms used by Art. 32 CCC and the constellations covered by them were only partially explained in more detail in the Explanatory Report to the CCC - mutatis mutandis the Council of Europe's "message" on the CCC - which risks being interpreted differently by the authorities of the Contracting States. However, this seems to have been a deliberate decision. After all, a working group on transborder access to data ("T-CY Transborder Group") of the Committee of the Parties ("Cybercrime Convention Committee, "T-CY") issued a Guidance Note on December 3, 2014 on transborder access to data under Art. 32 CCC, which can be used as an interpretative aid. However, the prerequisites of Art. 32 CCC - such as the question of who is entitled to grant consent under Art. 32 lit. b CCC - are ultimately to be determined according to domestic law (cf. below, n. 41 f.); in this respect, a domestic definition and thus possible differing views between the contracting states are unavoidable. 15

According to the Federal Council, the provision should be interpreted narrowly "in order to counteract the danger of abuse by circumventing mutual assistance or in violation of the privacy of third parties." However, if one takes into account the effect intended by Art. 32 CCC - the acceleration of proceedings or the simplified collection of evidence - this leaves room for interpretations that are practical and fit for purpose. 16

D. Legal Nature

17 Art. 32 CCC is a "self-executing" norm of international law that is directly applicable upon ratification. The contracting parties thereby grant the other contracting states the right to directly access data in their territory bypassing the mutual legal assistance channel. In other words, the provision standardizes a "waiver of the domestic procedure in the requested state." The prosecuting authorities of the Contracting States may directly rely on Art. 32 CCC, both in domestic criminal proceedings in order to legitimize corresponding evidence gathering abroad (while still having to comply with domestic procedural rules, see below, n. 56) - Art. 32 CCC does not constitute an original coercive measure in this respect - and, in relation to the Contracting State concerned, they may rely on the absence of unlawful interference with foreign sovereignty. In relation to the IMAC, the provisions of the CCC take precedence over those of the IMAC in any case (Art. 1 para. 1 IMAC).

E. Scope of Application

18 Art. 32 CCC permits the seizure of computer data stored in another contracting state.

19 According to Art. 1 lit. b CCC, computer data are all representations "of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of initiating the execution of a function by a computer system." Article 32 of the CCC thus covers access to inventory, traffic or peripheral data as well as content data that is either stored or in the transmission stage at the time of access. Due to its legal qualification as electronic data, crypto assets, for example, can also be seized in application of Art. 32 lit. b CCC, provided that the authorized persons grant their authorization.

20 Art. 32 CCC explicitly focuses on the location of the specifically envisaged data (Art. 32 lit. b CCC: "[...] stored computer data located in the territory of another Party"; cf. also Art. 31 CCC: "[...] stored by means of a computer system located in the territory of the requested Party"). In the case of data stored in several locations, the location of the data set that is to be specifically seized is decisive. Consequently, access in application of this provision is only permissible if the CCC is applicable at the place where the data is stored. Since none of the 68 contracting states has made a reservation to Art. 32 CCC, the

examination can be limited to whether the state at the storage location to be affected is a party to the Cybercrime Convention, i.e. whether it has signed and ratified it.

Art. 32 CCC is not applicable to purely domestic circumstances: If the data are stored locally on a terminal or server located in Switzerland and secured here, Swiss national law is applicable in this regard (in particular Art. 246, Art. 263 and Art. 265 CrimPC, for marginal data see Art. 273 CrimPC). This is also the case if foreign data records are in the cache of the device seized here at the time of access. However, if the device is used as a "key" or "gateway" to gain access to services that have stored their data abroad (e.g. cloud, webmail, etc.) without these being stored locally on the device, this is a transnational data seizure in this respect and Art. 32 CCC must be observed (cf. however below, n. 63 ff.). Swiss national law is also applicable if foreign providers have Swiss subsidiaries or partners that store the data in Switzerland. In this case, access can take place at the latter. However, data centers are not usually included in this category, since the data stored with them is often encrypted and can hardly be read out without the cooperation of or forced collection from the persons authorized to receive the data. The foreign persons must then be requested to hand over the data or keys either in application of Art. 32 lit. b CCC or subsidiarily by way of mutual legal assistance. Art. 32 lit. b CCC is also applicable if domestic subsidiaries or partners of foreign providers are ordered by the public prosecutor to hand over data they have stored abroad. Correctly, a domestic person may not be ordered under threat of coercion to obtain evidence available to the prosecuting authorities abroad, even if this should involve data with respect to which he or she is entitled to access. The Federal Supreme Court held that an order to disclose data pursuant to Art. 265 CrimPC to a Swiss branch of an Internet service provider was admissible if it had access to the data in question and was authorized to do so ("pouvoir de disposition, en fait et en droit, sur ces données"). This is not inconsistent with what has just been said, since the disclosure order does not yet constitute a coercive measure and can be understood and assessed in this context as a request under Art. 32 CCC for voluntary disclosure. 21

With regard to third countries that have not signed up to the Convention, it must be assumed that state sovereignty prohibits any online access to (non-public, cf. below, n. 35) data and therefore the only option is to use the mutual legal assistance route. 22

23 It is obvious to base this on the storage location, because the states can also invoke the principle of sovereignty with regard to the IT infrastructure located on their territory. However, it is problematic that at the time of access, it is not uncommon for neither the law enforcement agency nor the data controller or even the data custodian to know where the data is stored at any given moment. For example, Internet service providers sometimes store their customers' data not in their country of domicile, but elsewhere. The storage location may also change over time due to technical restructuring or relocation to other (cheaper) locations. In any case, the storage location often cannot be determined conclusively at the time the data is accessed. This raises the question of how to deal with the standard case in which the law enforcement authority cannot determine at the time of the intended seizure whether the data is stored in a CCC contracting state, a third country or even in its own country. The materials to Art. 32 CCC do not address this conclusively; the T-CY Guidance Note only, but nonetheless, provides that in situations where the location of storage is unknown or uncertain, States Parties should evaluate for themselves the legitimacy of access in light of domestic law, relevant international law principles, or considerations of international relations ("[...] Parties may need to evaluate for themselves the legitimacy of a search or other type of access in light of domestic law, relevant international law principles, or considerations of international relations"). In the case of unknown location, the following suggests itself: If for the applicability of Art. 32 CCC the certain knowledge would be required that the storage location is in a Contracting State, Art. 32 lit. b CCC would lose its meaning and the seizure of cloud data would be reduced to absurdity. "The mere possibility of a location in a third country can also not trigger a mutual legal assistance obligation, especially since it is not even clear which country should be addressed for this." Detailed clarifications of the storage location are often impossible before access or take too much time - admittedly: if there is no urgency and the storage location can be determined technically without special effort, efforts should be made. In view of the CCC's idea of acceleration, however, it would not be advisable to generally wait until certain knowledge is available, especially if there is a risk of loss of evidence. If it turns out in retrospect that the storage location was actually in a third country, a subsequent authorization for data access will have to be obtained through mutual legal assistance (see below, n. 71).

In relation to the large social media providers, the situation is somewhat more complicated. They have their headquarters in the USA, but their European headquarters are often in Ireland and, according to their own information (which is not necessarily correct in view of the U.S. Cloud Act), they only have access to the data of European and Swiss customers from Ireland (which the providers justify with the European General Data Protection Regulation of 27 April 2016 ["DSGVO"]), although the data is regularly stored in other countries (e.g. Sweden). However, Ireland has not ratified the CCC to date. Accordingly, the question arises whether requests under Art. 32 lit. b CCC for European data for the attention of the Irish branch are permissible at all and whether the collected data are usable. Alternatively, should Sweden be addressed as a possible storage location, even though the data may be accessed there, but it is likely to be encrypted and thus unusable? Or should the American parent company be affected, which should obtain the data from its European subsidiary? In practice, the explosiveness of this question is mitigated by the fact that requests for information can be made via "law enforcement portals" provided by Internet service providers - it is up to them to decide from which group company the providers then make the requested data available to the authorities or how they have organized themselves internally, and this does not need to be examined further, especially since the law enforcement authorities have no way of verifying where the edited data has actually been stored and exactly which group company has had access to it anyway. 24

In view of all these difficulties, the storage location makes little sense as a decisive criterion. De lege ferenda, therefore, the criterion of the place of storage should be dispensed with for Art. 32 CCC and instead be linked to the registered office or place of residence of the person who has lawful access to the data. Alternatively (in line with the EU e-Evidence Regulation and Art. 18 para. 1 lit. b CCC), it may be sufficient that the respective company offers its services in the relevant state. 25

F. Practical Relevance

Art. 32 CCC has emerged as an indispensable means of prosecuting crime with a digital component. Swiss law enforcement authorities regularly rely on Art. 32 CCC, be it through the collection of open source information ("OSINF") in application of Art. 32 lit. a CCC, be it through access to data upon voluntary disclosure of login data by the Swiss data subject pursuant to Art. 32 26

lit. b CCC or in particular by direct requests ("information requests") to foreign Internet service providers for the disclosure of inventory, marginal or content data (whereby in practice usually only inventory and marginal data are supplied and for content data the legal assistance route must be taken, if necessary in combination with a "preservation request" under Art. 29 CCC). The numbers of direct requests for information are remarkable: in the first half of 2022, Google alone received over 422,000 direct requests, including 1,357 from Swiss law enforcement agencies, 90% of which were approved. However, providers are not accountable for denying a request; they can set the conditions for surrender on their own, keep changing them, and moreover, the conditions vary considerably depending on the provider. This is acceptable under the current regime, since Art. 32 CCC is based on voluntariness.

II. ACCESS TO PUBLICLY AVAILABLE DATA STORED IN ANOTHER CONTRACTING STATE ("OPEN SOURCE") (LIT. A)

A. Publicly accessible data

27 The collection and analysis of "open source information" is referred to in the intelligence sector as "OSINT" ("Open Source Intelligence"). The use of publicly available data has also emerged in law enforcement as a useful and non-invasive investigative method. This is supported by the tech industry, which has developed tools that eliminate the need to manually gather data and instead automate it: For example, by providing software that can pull all publicly available information from Facebook and display it in relationship trees and on the timeline, or technical tools to track the flow of money from cryptocurrencies (whose blockchain is publicly accessible). The use of artificial intelligence is also no longer a pipe dream.

28 Data are public if they are freely accessible via a data processing system and are not withdrawn from general access by special security precautions. It is sufficient if they are made accessible to an undefined circle of users, even if a login is required, "but this is in principle granted to every user if an appropriate login form has been completed." A system may also be merely partially public. By contrast, data that "can only be accessed by means of an interface of a terminal device located in the - not publicly accessible - search object" are not "open source."

Examples of publicly accessible data are - in the sense of a non-exhaustive list - freely accessible mass media (print media [even if protected by a paywall], broadcasting), all information that can be found on the Internet (clearnet as well as darknet), web-based applications (such as Google Earth), information on the publicly viewable blockchain (e.g. Bitcoin), data that can be publicly accessed on the website at the domain address of a company or an administration, freely accessible webcams, a mailing list that is open to all interested parties, data that is freely available on a sharing platform, the retrieval of technical data from a web server, the determination of domain information via "WhoIs" databases, debtor, land register, commercial register and residents' control information freely accessible abroad or against payment or available records from criminal, administrative and civil proceedings, observing public chats, open Internet forums and publicly switched social networks (the use of public data, photos and relationships on Facebook, information from X, Instagram, LinkedIn, etc.).). Even a post in a closed group (online forum, Facebook or similar) can be qualified as public in the case of groups with a high number of members or with de facto unrestricted access, unless the group of persons is specifically delimited and the persons are personally connected to each other. Accordingly, "closed user groups in which case-by-case verification of users' identities is performed by administrators of the site and an investigator would only gain access, for example, by feigning a legend, can no longer be qualified as public." 29

Depending on the circumstances, not only content data (personal or other data), but also inventory data (e.g., registration information from "WhoIs" databases) or (rarely) even marginal data may be public and consequently collected in application of Art. 32 lit. a CCC. 30

For the qualification as publicly accessible data, it is irrelevant whether the data were published without authorization or with the consent of the data subject. If the publication was made unlawfully (e.g., by violating legal confidentiality obligations), the data can be used in domestic criminal proceedings if they could have been lawfully obtained by the law enforcement authorities and a balancing of interests speaks in favor of their use. Consequently, it must be clarified for the first criterion whether the data could hypothetically also have been seized if they had not been public - i.e. whether they could have been obtained within the meaning of Art. 32 lit. b CCC or via mutual legal assistance. 31

B. Legal Nature: Qualification as Interference with Fundamental Rights?

32 It is questionable to what extent the collection and analysis of publicly accessible data should be qualified as an interference with fundamental rights and, as a consequence, as a coercive measure within the meaning of Art. 196 CrimPC. The answer to this question is central, firstly in order to determine the extent to which public data located in a third country can also be accessed, and secondly because if the answer is yes, there must be a sufficiently concrete legal basis (Art. 197 para. 1 lit. a CrimPC). The latter, however, has already been implemented by Art. 95 CrimPC (acquisition of personal data).

33 According to Art. 196 CrimPC, coercive measures are defined as procedural acts by the criminal authorities that serve, among other things, to secure evidence insofar as they interfere with the fundamental rights of the persons concerned. Art. 196 CrimPC thus (in contradiction to the wording ["coercive" measure]) does not necessarily presuppose coercion, but rather relies decisively on whether the measure is to be considered an encroachment on the fundamental rights of the persons concerned. In the foreground, in addition to the right to personal freedom and the guarantee of property, is the protection of privacy under Article 13 FC and Article 8 ECHR, or more specifically the right to informational self-determination enshrined therein. Interventions in this constitutional right include telephone surveillance, the collection of telecommunications data, the collection and analysis of DNA and fingerprints, observation (including systematic surveillance by private detectives), video recordings by the police, the use of an IMSI catcher and password-protected online searches or seizure of chat messages.

34 With regard to automated traffic surveillance, the Federal Supreme Court once held that the protection of privacy is not limited to private premises, but also extends to the private-public sphere; Article 13 FC also covers matters of life with personal content that occur in the public sphere. According to the German Federal Constitutional Court, access to "communication content and information available on the Internet that is directed at everyone or at least at a group of persons that is not further delimited" cannot yet be correctly characterized as an encroachment on the right to informational self-determination. Content that is reserved for a specific group of users on blogs, forums or in social media and is thus directed at an environment characterized by per-

sonal relationships or special trust can be attributed to the private sphere within the meaning of Article 13 para. 1 FC and its access can be considered an encroachment on fundamental rights. Data that can be accessed by any Internet user without any preconditions or that can be viewed by all users registered on a platform (irrespective of a close relationship to the person disclosing the information) can no longer be classified as "private", regardless of the content. There is correctly no longer any interest worth protecting in information that is already publicly known (with the exception of the "right to be forgotten" under data protection law).

If access to generally accessible data is not a coercive measure, this also means that Art. 32 lit. a CCC is not constitutive but purely declaratory in nature: If access to public sources does not violate state sovereignty due to the lack of an actual exercise of coercion, no intergovernmental agreement is required. Accordingly, publicly available data from third countries that have not ratified the CCC can also be accessed without any problems. The latter is sometimes also justified by the fact that transnational access to "open source data" is customary international law; such acts of investigation are considered to be so uncontested. 35

Even if this were not followed in such absoluteness, in any case the tapping of voluntarily disclosed data - such as communication content in social media - could not be characterized as an encroachment on fundamental rights. This is because by consciously deciding to share personal information, the individuals concerned are relinquishing their informational self-determination with respect to that specific data, or in other words, by releasing it into the public domain, they have just exercised their informational self-determination. The same applies to the public data trail left by their own inputs, such as transactions made with Bitcoin that are traceable on the public blockchain. Next, data that cannot be directly attributed to a specific person is not worthy of protection under any fundamental rights title. This includes, for example, the use of "Google Earth" or technical data disclosed by a web server. Consequently, the tapping and analysis of personal information that has not been disclosed voluntarily is the most that can be considered a coercive measure; in this case, it could legitimately be argued that the individuals concerned have no control over what information is available about them on the Internet. However, even then it would have to be taken into account that OSINT is a comparatively less invasive and thus proportionate intervention, since it is 36

limited to information that can be accessed by anyone without special access restrictions.

C. Prerequisites for permissible data access under Swiss criminal procedure law

37 The tapping of "open source" data is permissible for any criminal offense (felony, misdemeanor or infraction) to the extent that the collection of evidence available in electronic form is useful for its prosecution (cf. Art. 25 para. 1 and Art. 14 para. 2 lit. c CCC). To the extent permitted by cantonal police law, public information may also be accessed in the context of preventive police activity.

38 Due to the lack of interference with fundamental rights, "open source" investigations are not to be classified as coercive measures within the meaning of Art. 196 et seq. CrimPC (cf. above, n. 32 et seq.). As a result, neither the formal and substantive provisions on searches (Art. 246 et seq. CrimPC) nor on seizures (Art. 263 CrimPC) are applicable. "OSINF" or "OSINT" is rather deemed to be a permissible collection of evidence based on Art. 95 CrimPC within the meaning of Art. 139 para. 1 CrimPC.

39 Logging on by members of law enforcement authorities under a false identity in social media or in a chat in order to gain access to the content published there is not to be classified as an undercover search (Art. 298a CrimPC) or undercover investigation (Art. 285a CrimPC), as no direct contact with the target person is established here. The situation would be different if the investigator were to actively send the target a friend request or the like in order to also take note of the target's (private) contributions, or if he were to gain access to a chat or forum that is not generally accessible by creating a legend.

40 The evidentiary value of publicly available data must be examined in detail within the framework of the free assessment of evidence (Art. 10 para. 2 CrimPC). Various considerations play a role here, first and foremost the origin of the evidence, its authenticity and reliability, the relationship of its author to the parties to the proceedings, and above all whether the source is anonymous or known, especially since doubts are great in the case of unknown origin and data are relatively easy to manipulate. It is also important that the data are forensically secured in accordance with the current state of the art, since

metadata can be used to draw conclusions about the probative value; simply taking screenshots will hardly suffice for this purpose.

III. ACCESS TO OTHER DATA STORED IN ANOTHER CONTRACTING STATE (LIT. B)

A. Lawful and voluntary consent of the person lawfully authorized to disclose the data

1. Authorization to disclose

Art. 32 CCC only regulates the permissibility of data access under international law; "the domestic rules against which the transfer of data is to be measured, i.e., according to which it is to be decided whether consent to the transfer has been lawfully given by a person authorized to do so, are not affected by the Convention." The Council of Europe has refrained from further defining the concept of transfer authorization in the CCC. The Explanatory Report states that who can give consent "may vary depending on the circumstances, the nature of the person and the applicable law concerned." 41

The question of who is "lawfully authorized to disclose the data [...]" is determined by the domestic law of the requesting state, i.e., the one in which the investigation takes place. This also appears to make sense because it is often not possible, or not possible without great effort, to precisely locate the data prior to access. Moreover, it would be impracticable and incompatible with the CCC's idea of acceleration to require Swiss authorities to check the authorization situation for each contracting state separately before they would be allowed to back up data. 42

What is necessary is the authorization to pass on data. Necessary, but also sufficient, is the consent of a person who is lawfully authorized to disclose it to law enforcement authorities. The authorization may be of a legal or mandatory nature. 43

Contrary to the message, it is not an additional requirement that consent must be given by "a person within the country"; Art. 32 lit. b CCC knows no such restrictive criterion, which, moreover, would run counter to the spirit and purpose of the Convention. 44

45 The Explanatory Report and the Dispatch cite as eligible for consent, by way of example, persons who have their e-mails stored with a service provider in another state or otherwise have their data stored abroad. In the literature, the customer renting the storage space is referred to as the authorized person in the case of data stored on cloud servers, the bank in the case of data on financial transactions, the employer in the case of the business e-mail account, and the persons declared internally responsible for this in the case of legal entities, or the board of directors (AG) or the management (GmbH) in the absence of such internal regulations; administrators or other persons authorized to access data are likely to lack this authorization on a regular basis.

46 One aspect not conclusively discussed in the Explanatory Report concerns the question of whether consent must always be given by the data subjects (data controllers) or whether the authorization of other entities that process the personal data (first and foremost the Internet service provider as data controller) is sufficient. An extension to Internet service providers is viewed critically, because they would merely exercise data custody and would therefore not be in a position to be able to give legally valid consent.

47 The question of the right to pass on data must be considered in the broader context that, under the current legal situation, there is no property-like right to data in Switzerland: The property right under Article 641 CC extends only to the "thing," which the doctrine understands to mean "a corporeal object, distinct from others, which is amenable to actual and legal control." Since data are immaterial goods, no ownership within the meaning of Art. 641 CC can be established in them (but certainly not in data processing systems or data carriers). Copyright law also extends only to intellectual creations with an individual character in data form and is applicable only in exceptional cases. Nevertheless, a right of access to data is recognized in data protection law, at least with regard to personal data, with respect to which a right of access is standardized in Art. 25 of the Federal Data Protection Act of 25.9.2020 ("FADP", SR 235.1). Art. 28 FADP also grants data subjects the right to data surrender and transfer of personal data (data portability) if certain conditions are met, provided that they have disclosed such data to the data controllers. Furthermore, personal data "may only be obtained for a specific purpose that is apparent to the data subject; it may only be processed in a manner that is compatible with that purpose" (Art. 6 para. 3 FADP). In this context, the surrender of personal data to law enforcement authorities constitutes a form of data

processing (cf. Art. 5 lit. d FADP). This means: The authorized person can consent to the disclosure by the data processor.

Switzerland, in line with other contracting states, therefore allows the consent of Internet service providers to suffice as a consequence of their relationship under private law with the data subject if the service providers have stipulated a right of onward transmission to foreign law enforcement authorities in their general terms of use or data usage guidelines. The majority of Internet service providers stipulate in their user agreements that data can be disclosed not only in the presence of a valid court order, but also upon simple request by law enforcement authorities, or that the providers cooperate with law enforcement authorities. Disclosure in these cases is in compliance with the law. 48

2. Consent

The fact that a foreign provider company concerned would in principle be entitled to declare its consent to direct data disclosure in the sense described is not yet sufficient (according to the clear wording of Art. 32 lit. b CCC) for cross-border access: Rather, it must be further examined whether the requesting law enforcement agency has obtained a legally effective "lawful and voluntary consent." 49

As seen, the person capable of giving consent is the legal entity or natural person capable of judgment who may dispose of the data on the basis of legal or obligatory authorization and grant third parties access to it (cf. also above, n. 43 ff.). If there are several persons authorized to disclose data, the consent of one person is sufficient. If, for example, the account holder has given her authorization, no additional consent is required from the foreign provider company. Conversely, it is sufficient if the foreign provider, based on a corresponding authorization by the customer in the General Terms and Conditions of Use, releases the data (for consent by Internet service providers, see above, n. 46 ff.). 50

In accordance with general principles of criminal procedure, consent can either be expressly declared (for which there is no formal requirement) or implied. The latter is the case, in particular, if the person requested by the criminal prosecution authorities - for example, a service provider or the owner of the account in question - surrenders the data upon request. 51

52 At the same time, this means that corresponding "information requests" may be made abroad without this qualifying as an inadmissible act in a foreign state. In practice, direct requests to foreign providers have become an international standard, which can either be entered via law enforcement portals operated by the providers themselves or, in the case of other (smaller) providers, can also be delivered through the police (via Interpol). Various international treaties also permit direct service of official documents abroad, at least in principle, most notably Art. 52 para. 1 of the Schengen Convention of 19 June 1990 ("CISA"). However, the latter provides that each state may or must make a declaration as to which documents may be sent to persons in its territory. Consequently, it must be checked separately for each contracting state whether direct service is permitted and, if so, to what extent. Insofar as it is pointed out to the addressees that any cooperation is voluntary and that no direct negative consequences are attached to a refusal to cooperate, it is, however, not apparent to what extent this can be seen as a violation of foreign territorial sovereignty and thus a case of application of Art. 52 para. 1 of the Schengen Convention - it is a matter of mere invitations without any threat of coercion and without any negative consequences attached to a possible refusal to cooperate. It would therefore make little sense if the exception in Art. 32 lit. b CCC were intended to increase the efficiency of the cumbersome formal mutual assistance procedure, but at the same time this were to be torpedoed by the requirement to clarify the willingness of the persons concerned to cooperate voluntarily via this same formal mutual assistance procedure. In this respect, Art. 32 lit. b CCC takes precedence over Art. 52 CISA.

53 Consent must be voluntary; the data subject must not be deceived or coerced into handing over data. There is often an indirect pressure situation, because in the event of refusal, the public prosecutor's office may demand the seizure and transfer of the data in question by way of mutual legal assistance. However, this is not sufficient to impair the formation of wills. The same applies, for example, in the case of a detention situation, where the accused person could subjectively feel compelled by the circumstances to cooperate and provide the data stored abroad in order to be released from detention as quickly as possible. However, even a pressure situation of this general nature does not prevent the person from giving consent in accordance with the law. What is prohibited, however, is the concrete threat of possible further disadvantages. Accordingly, a person domiciled in Switzerland cannot be forced to produce

data stored abroad to which he has access. However, he or she can be requested to do so by means of an editing order (Art. 265 CrimPC).

Finally, consent can be revoked at any time, although revocation is only ex nunc. Revocation after data backup has taken place is therefore irrelevant. 54

B. Consequence of legally valid consent

If the person authorized to dispose voluntarily discloses his login data to foreign derived Internet services or consents to the online search, it is open to the law enforcement authorities in application of Art. 32 lit. b CCC to directly access and secure the information by using the login data. Also, any private individual is free to make copies of his or her own data stored with a foreign provider (such as e-mails or chat messages) available to the law enforcement authorities. It is also permissible for the law enforcement authority to directly request an Internet service provider domiciled abroad to hand over data (see above, n. 48, 51 f.). 55

C. Prerequisites for permissible data access under Swiss criminal procedure law

Access to non-public data in Switzerland is not possible without preconditions. If it is content data, the data must be seized (for example, by an edition order [Art. 265 CrimPC] or on the occasion of a house search [Art. 244 CrimPC]), searched (Art. 246 CrimPC), and subsequently seized if relevant to the evidence (Art. 263 CrimPC). For traffic data, a retroactive marginal data collection (Art. 273 CrimPC) must be ordered and approved by the compulsory measures court (Art. 274 CrimPC). Now, Art. 32 lit. b CCC does not constitute an independent evidence preservation or evidence collection measure that would override the domestic requirements. The provision only regulates that if a legally valid consent exists, a mutual assistance procedure can be waived. Data access, even if transnational, therefore constitutes a domestic coercive measure that must satisfy domestic legalities. The seizure of data abroad must therefore - in addition to the consent described above - fulfill the same conditions as if the data had been stored in Switzerland. An "information request" to an Internet service provider must therefore be qualified as an order for disclosure within the meaning of Art. 265 CrimPC. 56

57 First of all, it follows that in principle the opening of a criminal investigation within the meaning of Art. 309 para. 1 CrimPC and thus sufficient suspicion of a crime are a prerequisite, whereby criminal proceedings that have not yet been formally opened are automatically deemed to have been opened with the data interception (Art. 309 para. 1 lit. b CrimPC). In independent police investigation proceedings, Art. 32 lit. b CCC may not be relied upon. Intelligence services may not invoke it either.

58 The CCC serves to collect evidence of a criminal act that is available in electronic form (cf. Art. 25 para. 1 and Art. 14 para. 2 lit. c CCC). In principle, reasonable suspicion can thus extend to any criminal act, provided there is at least criminological suspicion that it was committed with a technical aid. The severity of the offense is irrelevant: transnational data access is in principle open to felonies, misdemeanors and infractions (in minor cases, however, the proportionality of data access may be open to discussion).

59 For content data to be seized, it must be suspected that it contains information that is subject to seizure (Art. 246 CrimPC). According to Art. 263 para. 1 lit. a CrimPC, objects belonging to an accused person or a third party may be seized specifically if they are needed as evidence. For the seizure and search of records, a potential relevance as evidence is sufficient, which is given if the data "may be of importance for the clarification of the alleged criminal offence" or does not appear "obviously unsuitable". Case law does not place high demands on this. Finally, the seizure and search must be proportionate (Art. 197 para. 1 lit. c and d CrimPC) and thus suitable, necessary and appropriate. Proportionality may be questionable, especially in the prosecution of misdemeanors. From a formal point of view, the seizure and search by the public prosecutor must as a rule be ordered in a written warrant (Art. 241 para. 1 CrimPC). For the collection of inventory data, on the other hand, the only requirement is that there is a suspicion that an offense has been committed via the Internet (Art. 22 para. 1 of the Federal Act on the Interception of Postal and Telecommunications Traffic of 18 March 2016 ["BÜPF"; SR 780.1]).

60 If the IP history/log data or other marginal data are collected abroad, the question arises as to whether the public prosecutor's office may make these records available on its own authority or whether, in application of Art. 273 para. 2 CrimPC, permission must be obtained from the compulsory measures court. The Federal Supreme Court once held that Art. 273 CrimPC only permits retroactive marginal data collection of telecommunications traffic

"against telecommunications service providers or Internet access providers domiciled in Switzerland and subject to Swiss law." It thus ruled out its applicability to international situations, with the consequence that no authorization by the compulsory measures court should be required for the collection; in other words, Art. 32 lit. b CCC allows "a facilitated international exchange of marginal data." In another decision, however, the Federal Supreme Court rejected an application for approval by the public prosecutor's office on the grounds that the requirements of Art. 32 lit. b CCC had not been met in this case, adding that direct cross-border access would have had to be approved by the compulsory measures court under Art. 273 CrimPC. Even more, it explicitly stated in a further ruling that permission from the compulsory measures court must also be obtained for IP histories queried from foreign providers, and because this had not been done in the specific case, the findings derived from the queries were absolutely unusable. The fact that the Federal Supreme Court dealt with Art. 273 CrimPC here may seem understandable at first glance if one considers the legal nature of Art. 32 lit. b CCC, which only declares transnational access permissible under international law, but does not affect domestic regulations, especially with regard to the competence to collect data. However, it must be taken into account that the provisions on retroactive marginal data collection are not activated solely by the type of data to be collected (traffic or marginal data), but the data must be obtained from a telecommunications provider or be protected by telecommunications secrecy (Art. 321ter SCC and Art. 43 of the Telecommunications Act of 30.4.1997 ["TCA"; SR 784.10]). However, telecommunications secrecy applies (insofar as it is of interest here) only to providers who offer Internet access or telecommunications transmission. Internet service providers or providers of derived communications services that do not offer Internet access but only services provided via the Internet ("over-the-top services") are not considered telecommunications providers. For this reason, neither the seizure of edge data from such companies in Germany nor abroad is subject to a licensing requirement. Rather, an editing order issued to the Internet service provider is sufficient for this purpose (Art. 265 CrimPC). Consequently, if IP histories and other marginal data are collected from non-telecommunications providers abroad on the basis of Art. 32 lit. b CCC, no approval must be obtained from the compulsory measures court.

Finally, the question arises as to the extent to which the other requirements for mutual assistance, namely grounds for refusal and the need for double 61

criminality, also apply to Art. 32 lit. b CCC. Art. 25 para. 4 CCC provides, under the 3rd title ("General Principles of Mutual Legal Assistance"), that unless the CCC expressly provides otherwise, "mutual legal assistance shall be subject to the conditions provided for in the law of the requested Party or in the applicable mutual legal assistance treaties, including the grounds on which the requested Party may refuse to cooperate." However, Art. 32 lit. b CCC allows direct access prior to mutual assistance; a "request" to the other contracting state, as it is based on Art. 25 para. 4 CCC, is not required here. Consequently, the voluntarily granted access does not require double criminality, nor are further conditions to be met that would otherwise apply in mutual legal assistance proceedings. This softening is justified, on the one hand, by the voluntary nature of the consenting persons and, on the other hand, in view of the legal nature of Art. 32 lit. b CCC, which extends the territorial arm of the law enforcement authorities, while it continues to be a domestic evidence preservation measure. If the attempt to seize the records on the basis of Art. 32 lit. b CCC fails, then the ordinary mutual assistance route must be taken, for which the corresponding limitations apply again.

62 The person concerned cannot defend himself against the direct seizure as such or the provider inquiry; nevertheless, the legal remedy of sealing (Art. 248 CrimPC) is open to him against the search, insofar as he can credibly demonstrate a prohibition of seizure (Art. 264 CrimPC). The effect of sealing is that the prosecution authorities may not search the records for the time being until the compulsory measures court has ruled on the admissibility of the data collection and search.

IV. PRESERVATION OF EVIDENCE BEYOND ART. 32 CCC ACCORDING TO THE ACCESS PRINCIPLE.

63 In friction with the principle of territoriality, which is based on the place of storage of the evidence and thus, in the case of data, on the physical place of storage, the Federal Supreme Court allows access even in the absence of consent, regardless of where the data is stored at the time of access; the decisive factor is that the data can be accessed from Switzerland: "Anyone who uses a derived Internet service offered by a foreign company via Internet access in Switzerland is not acting abroad. Even the mere fact that the electronic data of the relevant derived internet service are managed on servers (or cloud storage media) abroad does not make an online search conducted from Switzer-

land in compliance with the law appear to be an inadmissible investigative act on foreign territory (within the meaning of the practice set out) [...]."

The subject of the assessment was the access to the Facebook account of a person accused of qualified narcotics trafficking, whose access data had been made available by the prosecution authorities. The public prosecutor's office then had the Facebook account sifted through using the identified login data and seized chat messages relevant to the evidence. The storage location of this data was not in Switzerland at the time - and still is not. In the cited ruling, the Federal Supreme Court held that accounts of defendants or third parties on foreign Internet services may be accessed directly if the general requirements of a search under the Swiss CrimPC are met and the investigators act "from computers, servers and IT infrastructures located in Switzerland", i.e. remain physically in Switzerland. 64

Practice has gratefully accepted this case law. It is applicable not only to Facebook, but to a wide range of domestic and foreign services such as host providers, communication services, cloud services, data outsourcing providers, chat forums, document exchange platforms, shopping portals, and email service providers. Crypto assets held in a hot wallet can also be seized (i.e., usually transferred to a law enforcement wallet) in application of this case law. Federal court case law is also gaining momentum. The general trend for electronic devices is to move away from individual storage to cloud backup. Cell phones in particular are now often used by users for various services only as "keys", with the data in question no longer stored on the physical device. If a cell phone or tablet is seized during a house search or police stop and it turns out that the data is not stored on the device but in the cloud, or if apps from communication services or web e-mail providers are found on the device, all of this data can be seized based on federal court case law. This procedure is facilitated in practice by the fact that users often save their login data for Internet services in the password manager or in an Internet browser for reasons of convenience or use the same password for different services. Also, during house searches at companies, it is increasingly found that they no longer host or store their data themselves at their headquarters or place of management, but have outsourced data processing and storage to external service providers. In such situations, the cited Federal Court decision also helps, as it allows data backup in such cases as well. 65

66 Implicitly, the Federal Supreme Court invoked the so-called "access principle" in the cited decision. According to this, in the case of computer data, it is not the location of the data carrier on which the information is stored that is relied upon, but rather who has access to the data relevant to the proceedings from where. The control over the data lies with the person who has the access authorization and not with the person who is in physical possession of the data carrier. Some authors cite this as a reason why the search and seizure of data stored abroad by Swiss authorities in Switzerland should not be seen as a violation of sovereignty. In other words, the admissibility of online access should depend solely on the legality of the domestic investigative act.

67 However, if foreign sources that are not publicly accessible, in particular those that are password-protected or protected by other barriers, are accessed, this has a high impact on the foreign ("digital") territory. For this reason, access by investigative authorities to data abroad is sometimes seen as an encroachment on the sovereignty of the state in question; such evidence can only be obtained via international mutual legal assistance or directly if this is explicitly provided for in international agreements. In fact, the access principle does not change the effects of state online access on foreign sovereignty, where the actual success of the measure occurs. It is true that the lack of physical action by officials on foreign territory should not yet exceed the limits drawn by Art. 299 SCC. However, in terms of the intensity of their intervention, they in no way take a back seat to equivalent physical investigative activities (the search of the storage medium abroad by Swiss officials), which would clearly be inadmissible. In addition, the online retrieval triggers data processing operations abroad; the access leaves traceable traces in the target state. In the worst case, depending on national legislation, the investigating officer may be liable to prosecution there for unauthorized intrusion into a data processing system, unauthorized data acquisition or disregard for foreign sovereign rights. Moreover, digital evidence gathering from Switzerland is carried out secretly for the foreign state, which - in view of the intelligence scandals of the recent past - makes it even more dangerous from the latter's point of view. Remarkably, according to a UN study, the national law of various states nevertheless permits a kind of direct access to data stored abroad, while the proportion of states that permit such direct access by foreign law enforcement agencies is noticeably smaller, according to the same study. Consequently, the international law sensorium seems to be greater when one's own sovereignty is affected than when one is dependent on obtaining evidence abroad. In any

case, the Cybercrime Convention already allows direct access to foreign data in a limited way in Art. 32 CCC; obtaining evidence beyond this - at least in the relationship between the convention states - is to be seen e contrario as an encroachment on state sovereignty. It is not for nothing that the Council of Europe has expressly provided for the subsidiary Art. 31 CCC entitled "Mutual assistance in accessing stored data". A proposal put forward by EU member states in the context of the negotiations, according to which transnational online searches should be permissible in urgent cases, was therefore not included - for lack of consensus, it was decided not to regulate such situations. Efforts that have been resumed since then have also been largely fruitless; the 2nd Additional Protocol to the CCC is not a great success in this respect either. Direct transnational access to data without the consent of an authorized person is thus still not covered by an international consensus, violates the sovereignty of the state concerned, and is thus contrary to international law as long as no further development of the current bilateral or multilateral agreements has taken place.

This result is unsatisfactory. First, especially when there is a risk that the data may be lost without immediate action. It is therefore conceivable to allow the temporary transnational preservation of data in exceptional circumstances where there is a risk of collusion or loss of evidence, if even a "preservation request" within the meaning of Art. 29 CCC would be made too late. In this case, the preserved data would have to be kept separately and would not be allowed to be searched until the Contracting State concerned has been asked for subsequent permission. Second, the foregoing critique is premised on the understanding that law enforcement authorities have positive knowledge at the time of access that the data are not stored in their own country. However, it is often not clear from the outset where the data is stored, whether locally on the device or in the cloud after all. In these cases, too, it must be permissible to preserve evidence, if necessary with a subsequent request for legal assistance in the event that the data is subsequently found to be stored abroad (cf. above, n. 23). 68

V. CONSEQUENCES OF THE VIOLATION OF FOREIGN SOVEREIGNTY LAW

If the powers of the CCC are exceeded, if mutual assistance in criminal matters is circumvented by direct access to foreign data carriers, and if the princi- 69

ple of territoriality or sovereignty is thus violated, the question of the unusability of evidence obtained in this way arises. In principle, the circumvention of the mutual legal assistance channel can be objected to in domestic criminal proceedings.

70 Cantonal courts have so far advocated a relative prohibition of exploitation within the meaning of Art. 141 para. 2 CrimPC, whereby the evidence in question may be exploited insofar as it is necessary to clarify a serious criminal offense. It is questionable, however, whether the principle of territoriality under international law and the requirement to use the legal assistance channel are in fact merely valid provisions or whether, in view of their importance, an absolute prohibition of exploitation must be assumed (e.g. in the form of a violation of public policy). The Federal Supreme Court has decided in this direction when it considered a secret surveillance measure (GPS tracker and listening devices in a vehicle that was also used for trips abroad) to be absolutely unusable with regard to the trips abroad. However, it seems possible and sensible to adopt the view held in Germany, according to which the question of usability depends on whether the investigator was aware at the time of the data collection that the access would not be in accordance with international law. If it was not aware of this, it must be possible to have a subsequent formal mutual legal assistance procedure (in the sense of an approval procedure) carried out for the evidence (which was objectively obtained in an unlawful manner) in order to avert the inusability of the evidence.

71 The latter is particularly applicable to those cases in which it is not clear from the outset where the data are stored: If a domestic storage location cannot be ruled out, access to preserve evidence must be permitted; positive knowledge of the storage location is not a prerequisite. "The mere possibility of a location abroad cannot trigger an obligation to provide mutual legal assistance, especially since in these cases it cannot be determined which country will actually be affected." If it subsequently turns out (e.g., also in response to corresponding complaints by the defense) that the tapped data were not stored domestically and also not in a contracting state, subsequent authorization will have to be obtained in the state in question by way of mutual legal assistance.

VI. NEED FOR REFORM

72 The Council of Europe recognized early on the need to soften territorial principles due to technological developments and enacted a progressive provision

in Art. 32 CCC compared to traditional mutual legal assistance conventions. Further-reaching ideas were just as visionary as they were not (yet) capable of gaining majority support due to the strongly anchored idea of sovereignty. However, if the community of states wants effective criminal prosecution that can also perform its tasks in the 21st century, it seems necessary and sensible to completely give up sovereignty with regard to networked data. Today, it is no longer just a question of cross-border crime, which has always been difficult for national law enforcement agencies to grasp; as a result of the shift of evidence across national borders, it will soon no longer be possible to investigate purely domestic cases, let alone in an appropriate cost-benefit ratio.

Admittedly, it seems to be more promising to bake smaller rolls for the time being: First, Switzerland should sign and ratify the 2nd Additional Protocol to the CCC as soon as possible, even if it is not the big one. Secondly, much would already be done if, in the context of Art. 32 lit. b CCC, one would keep pace with legal reality and no longer only link the storage location, but rather (also) to the domicile of the person entitled to access or to the fact that a company offers its services in the state in question (cf. above, n. 25). Third, Switzerland should seek to associate itself with the EU's e-Evidence system (although this will be politically difficult to implement). Fourth, the recurring discussions on unilateral access to data abroad should be resumed and brought to a conclusion. At the very least, a domestic access location should be considered sufficient in the future so that data access no longer has to be classified as violating the sovereignty of the state at the storage location. In particular, protective measures and guarantees (e.g. an obligation to inform the state concerned about the access, the need for subsequent authorization, requirements regarding the rule of law and the protection of fundamental rights, etc.) could be included to increase the acceptance of such a solution. 73

BIBLIOGRAPHY

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

Aepli 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.

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-grenzuberschreitenden-zugangs-zu-elektronischen-beweismitteln/, besucht am 17.10.2023.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MATERIALS

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 Än-

derung 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-Transbprder-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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 33 CCC (Convention on Cybercrime)

A commentary by Nicolas Bottinelli / Julien Wenger

SUGGESTED CITATION

Nicolas Bottinelli/Julien Wenger, Commentary of art. 33 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Bottinelli/Wenger, art. 33 CCC N. XXX.

Art. 33 Mutual assistance regarding the real-time collection of traffic data

[1] The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

[2] Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

CONTENT

I. Introduction 271
II. Notions 272
III. Implementation in Swiss law 274
A. Art. 18b IMAC 274
1. Background 274
2. Definitions 275
3. Procedure 275
4. Some material delimitations 278
B. Distinctions 279
Bibliography 280
Materials 281

I. INTRODUCTION

Part of Chapter III of the Convention on Cybercrime, entitled "International Cooperation", art. 33 CCC is the first of the Convention's two provisions dealing with the obligations of States Parties to cooperate in the collection and transmission of communications data. This provision concerns traffic data, as opposed to art. 34 CCC, which deals with data relating to the content of the communication. 1

The ratio legis of this provision is that, very often, investigators cannot be sure of being able to trace the source of a communication by relying on records of previous transmissions, as crucial traffic data may have been automatically deleted by a service provider from the transmission path before it could be retained; it was therefore deemed necessary for investigators in each Party to be able to obtain real-time traffic data concerning communications transmitted by a computer system located on the territory of other Parties. 2

Swiss practice confirms this need, in view of the proliferation of messaging and e-mail platforms offering anonymization services not only through the use of end-to-end encryption, sometimes coupled with zero-access encryption, but also by the fact that connection logs are not kept, so that neither retroactive monitoring of traffic data nor search of stored data is likely to identify the user of the service. Real-time interception of data enables the source of the communication to be traced - if necessary via the mechanism provided for in art. 30 CCC. 3

Art. 33 para. 2 CCC obliges States Parties to provide mutual assistance "at least in respect of criminal offences for which real-time collection of traffic data would be available in a similar domestic case". It is therefore the national substantive criminal law (catalog of offences in particular) that defines the minimum framework for each Party's commitments. This solution has the merit of avoiding the pitfall of drawing up a list of offences for which mutual assistance should be granted in this constellation, which, given the diversity of cultures and legal systems, would undoubtedly have led to an outcry from many States. On the contrary, it aims to encourage the Parties to grant the widest possible mutual assistance, even in situations where the offences being prosecuted could not justify such a surveillance measure in national criminal proceedings, a solution which Switzerland has not decided to adopt. 4

5 At the level of national procedural law, the CCC obliges States Parties to adopt such legislative measures as may be necessary to empower its competent authorities, on the one hand, to collect or record on its territory, in real time, traffic data associated with specific communications transmitted on its territory by means of a computer system, and, on the other hand, to compel service providers to collect or record such data themselves, or to assist the authorities in doing so (art. 20 CCC).

II. NOTIONS

6 By "traffic data", the Convention means "any data relating to a communication passing through a computer system, produced by the latter as part of the communication chain, indicating the origin, destination, route, time, date, size and duration of the communication or the type of underlying service" (art. 1 let. d CCC). These data are produced by computers belonging to the communication chain to route the content of a communication from its origin to its destination. They are therefore auxiliary to the communication itself. Origin" refers to a telephone number, IP address or similar means of identifying a communication device to which a service provider supplies services. Destination" means a comparable indication of a communication device to which communications are transmitted. Type of underlying service" refers to the type of service used within the network: file transfer, e-mail or instant messaging. In short, traffic data provides information on the sender and receiver, as well as on the time, extent, duration, type and route of a communication.

7 The very definition of "traffic data" was not expressly taken up by the Swiss legislator when implementing the Convention (in particular in art. 18b IMAC; see III.A. below). At the time, the Federal Council considered that the definition was sufficiently described by doctrine and practice, namely: "Traffic data includes in particular the addressing resources of the origin of the access, the date and time of the start and end of the connection, the data used for the identification procedure (login) and the type of connection". Since September 1, 2016, Swiss law has defined "secondary telecommunications data" (art. 273 CPP referring to art. 8 let. b LSCPT) as "data indicating with whom, when, for how long and from where the person under surveillance has been or is in communication, as well as the technical characteristics of the communication in question". If this notion of secondary data is also applicable to telecommunications in general - and not just to computer traffic - it covers the notion of

traffic data. This concept is opposed to that of content data (see commentary on art. 34 CCC).

Art. 33 CCC covers the real-time collection of traffic data. The aim is to intercept this data, now and in the future, as and when communications arrive or depart. This concept is opposed to the collection of pre-existing data, recorded or stored on a data storage medium (server, cloud, etc.), even when the data relates to the traffic of communications that have already taken place. This direct temporality implies that the person under surveillance has no control over this data. In other words, there is typically no possibility of deleting the data before it is intercepted. In principle, the "interception" of this data is carried out by a third-party provider (internet and/or telephone provider, derivative telecoms provider, such as companies managing communication applications). In our view, Art. 33 CCC does not cover, in particular, the interception of data directly from the person under surveillance by means of Trojan horse software (Govware). On the other hand, interception of traffic by means of a special technical surveillance device, such as an IMSI catcher, does not appear to be ruled out (see III.A.3 below). 8

Intercepted data must be "associated with specified communications". The use of the plural is explained by the fact that it may be necessary to collect traffic data relating to several communications in order to establish the identity of the person originating the communication and/or the person for whom it is intended. The notion of "specified" means that the CCC does not require States Parties to set up general or systematic monitoring and collection of large quantities of traffic data. This provision cannot therefore justify an indeterminate search for evidence ("fishing expedition"). In the opinion of the authors, logs of connections to an e-mail box (logs and associated IPs) are also "associated with a specific communication" under the terms of this provision. Indeed, even though connection to an e-mail box does not necessarily lead to the sending or receiving of a communication, it is a necessary precondition for it. This seems to be the approach adopted by Swiss law; indeed, as we have seen, in the CCC Message, the Federal Council relied on a definition of the doctrine which includes addressing resources, including the dates and times of connection and disconnection. Moreover, art. 18b IMAC does not include this notion of "specified communications", which in particular paves the way for the real-time collection and anticipated transmission of connection logs (cf. infra III.A.4.). 9

10 Furthermore, specified communications must take place on the territory of a Party. This aspect could be potentially problematic, given that the use of cloud-type technology no longer makes it possible to associate a storage location with a particular State. In practice, the criterion of the place of storage of data has lost its importance in favor of that of the location of the person (natural or legal) who has effective control over the data. In the authors' view, art. 33 CCC also applies in this new context.

11 This provision requires the Parties to provide mutual assistance in the real-time collection of such data. While, on first reading, the notion of "collection" includes that of "transmission" - since this collection takes place at the request and for the needs of a foreign authority - we shall see that the Swiss legislator has distinguished between these two notions in implementing art. 33 CCC (cf. III. below).

12 Finally, the Convention does not apply as such to traditional telecommunications (analog telephony), since data must be transmitted by means of a computer system. The advent of digital telephony, and more generally the convergence of telecommunications technologies, is nevertheless blurring the distinctions between telecommunications and teleinformatics, and the specificities of their infrastructures. Thus the Convention - in particular art. 20 and 33 CCC - applies to specified communications transmitted by means of a computer system, the communication being able to be transmitted via a telecommunications network before being received by another computer system.

III. IMPLEMENTATION IN SWISS LAW

A. Art. 18b IMAC

1. Background

13 Art. 18b IMAC was introduced in the wake of Switzerland's ratification of the CCC. The CCC Message recalls that real-time surveillance measures must, by their very nature, remain unknown to the persons under surveillance; this postulate is difficult to reconcile with the basic principle of the IMAC, according to which no information pertaining to a person's secret sphere may be transmitted abroad without that person having first been given the opportunity to object. Art. 18b IMAC thus meets the requirements of art. 33 CCC.

2. Definitions

Under Art. 18b para. 1 IMAC, the federal or cantonal authority responsible for processing a request for mutual assistance may order the transmission abroad of data relating to computer traffic before the conclusion of the mutual assistance procedure if the provisional measures show that the source of the communication which is the subject of the request for mutual assistance is abroad (para. 1 let. a) or if these data are collected by the executing authority under an authorized real-time surveillance order (art. 269 to 281 CCP; para. 2 let. b). While letter a is the implementing legislation for art. 30 CCC, letter b implements Switzerland's international commitments under art. 33 CCC. However, this provision does not yet guarantee the granting of mutual assistance, since para. 2 prohibits the use of such data as evidence before the decision on the granting and scope of mutual assistance (art. 80d IMAC) has acquired the force of res judicata. The decision based on art. 18b IMAC allowing rapid access to the data by the requesting authority is an incidental decision, which then paves the way for the classic mutual assistance procedure required under Swiss law. In this respect, the legislator has taken care to distinguish the collection of data and its rapid access by the requesting authority from the mutual assistance itself, reconciling the Swiss legal order with international commitments. 14

3. Procedure

Art. 18b para. 1 let. b IMAC refers to arts. 269 to 281 of the Swiss Code of Criminal Procedure, and thus to art. 273 of the Swiss Code of Criminal Procedure with regard to the surveillance of secondary telecommunications data. In particular, the latter stipulates that only serious suspicion of the commission of a crime (art. 10 para. 2 and 3 PC) allows the public prosecutor to obtain secondary telecommunications data. Thus, the Swiss legislator did not wish to open the scope of application of art. 33 CCC to offences which would not allow the application of these measures under Swiss law, as proposed in art. 33 para. 2 CCC. 15

Art. 18b para. 1 let. b IMAC represents a departure from the classic system of mutual assistance, under which the right to be heard of the person affected by a mutual assistance measure must be guaranteed and a closing order duly notified and entered into force prior to any transmission of evidence abroad (art. 80d IMAC). Before this provision came into force, Switzerland could not pro- 16

vide such secret surveillance data abroad without first informing the person concerned (provided he or she was domiciled in Switzerland or had elected domicile there; cf. art. 80m IMAC), which often rendered the measure useless for foreign proceedings, or even jeopardized them.

17 From now on, once it has taken a decision (art. 80a IMAC), the executing authority will order the surveillance measure through the Service Surveillance de la correspondance par poste et télécommunication (Service SCPT; art. 273 CPP in conjunction with art. 60 ff OSCPT).

18 It must then obtain authorization for the measure from the Coercive Measures Court within 24 hours of the order (art. 274 al. 1 CPP). It should be noted that, with regard to the condition, set out in art. 273 CPP, of the existence of a "serious suspicion", the Federal Court rightly recalled that, according to the rules on mutual legal assistance and established case law, art. 14 CEEJ, 28 IMAC and 10 OIMAC require the requesting authority to explain what its suspicions consist of, but not to prove them or even make them likely. Subject to the prohibition on exploratory requests, the requesting authority's suspicions need not therefore be particularly serious or precise. Indeed, while domestic law must be applied when it is more favorable to cooperation than treaty law, it cannot lay down material conditions for mutual assistance that are not provided for in treaty law.

19 The Compulsory Measures Court decides within five days (art. 274 para. 2 CPP). If surveillance is refused, the documents and recordings collected must be destroyed immediately (art. 277 al. 1 CPP). If authorization is granted, it should be noted that art. 279 of the Swiss Code of Criminal Procedure (CCP), which provides for communication to the accused or to the third party subject to surveillance, and establishes a right of appeal for the latter and for the monitored telecommunications service (art. 279 para. 3 CCP), does not apply, despite the reference in art. 18b para. 2 let. a to arts. 269 to 281 CCP. In fact, the conventions and laws applicable to international mutual assistance in criminal matters derogate from the usual system of the CPC, which only applies if it is more favourable to cooperation than the applicable conventions and laws (principle of favourability). In particular, this means that party status, the right to notification and legal remedies are governed by the specific provisions on mutual assistance. However, according to art. 80m para. 1 IMAC, the obligation to notify decisions on mutual assistance is limited to persons residing or having elected domicile in Switzerland. Any indications to the contrary

by the TMC, whether by reference to the law or by imposing conditions within the meaning of art. 274 para. 2 CPP, would therefore be invalid, as the TMC has no jurisdiction over this aspect of the proceedings. It will be up to the executing authority, in the context of the mutual assistance procedure - i.e. after the anticipated transmission provided for in art. 18b IMAC - to ensure compliance with these conventions and applicable laws, and to make the notifications provided for in art. 80m IMAC.

Upon receipt of the surveillance data, the executing authority may issue an incidental decision based on art. 18b IMAC, ordering early transmission of the data to the requesting authority. The decision, as well as the surveillance order and authorization, are communicated to the FOJ (art. 18b para. 3 IMAC). If the surveillance is intended to last over time, and data are regularly collected, the decision may cover all future data resulting from the authorized surveillance, so as to enable the executing authority (or the police, as the case may be) to transmit the data as and when they are received. In the absence of any notification to the person concerned at this stage, and in view of the limits imposed by art. 18b para. 2 IMAC, such a procedure does not prejudice the rights of the parties to the mutual assistance procedure, and must be allowed. 20

It should nevertheless be borne in mind, whenever data is transmitted in advance to the requesting authority, that it may not be used as evidence until the decision on the granting and scope of mutual assistance has become res judicata (art. 18b para. 2 IMAC). In this way, legal protection is guaranteed a posteriori. It is also essential to keep a record - at least in the form of a list - of the data transmitted in advance, so as to enable the executing authority, at the end of the mutual assistance procedure, to know precisely which data will be the subject of the final closing decision. 21

In practice, when the person affected by the surveillance measure is unknown, is not domiciled in Switzerland or has not elected domicile there, or even uses a false identity, the executing authority can quickly validate the use of the data as evidence by means of a closure decision. As this decision is notified only to the FOJ (art. 80h let. a IMAC), secrecy regarding the existence of the measures is preserved. 22

If the person affected by the surveillance measure is domiciled or has elected domicile in Switzerland, his or her right to be heard must be guaranteed (art. 80m para. 1 IMAC in conjunction with art. 80b IMAC), which implies that he 23

or she must be informed of the measure and given the opportunity to express his or her views in writing before the closing decision is issued. Under art. 18b IMAC, it is possible to postpone informing the affected person and granting him or her the right to be heard for as long as is necessary for the procedure abroad. In practice, the executing authority will regularly have to ascertain from the requesting authority whether it is necessary, for the proceedings abroad, to keep secret the surveillance measure ordered in Switzerland.

24 The decision to terminate the procedure may be appealed to the Federal Criminal Court (art. 80e IMAC). The incidental decision to transmit traffic data in advance, in accordance with art. 18b IMAC, may be challenged together with the decision to close the case (art. 80e para. 1 IMAC). An immediate appeal against the incidental decision seems possible, if the executing authority has not taken the necessary precautions to ensure that the requirements of art. 18b para. 2 IMAC are respected. An appeal to the Federal Court remains possible under the restrictive conditions of art. 84 FSCA (particularly important case). Some scholars maintain that if the appeal is upheld, the information transmitted must be removed from the foreign file. This is certainly the case if the foreign authority has undertaken to do so, although this obligation does not appear in art. 18b IMAC.

25 The very broad wording of art. 18b para. 1 let. b IMAC also seems to allow for the anticipated transmission of data relating to computer traffic when this has been intercepted by means of IMSI catcher (art. 269bis CPP), govware (art. 269ter CPP) or even other technical surveillance devices (art. 280 CPP), even though art. 33 CCC would not impose such an obligation.

4. Some material delimitations

26 Unlike art. 33 CCC, art. 18b IMAC is not limited to "specified communications". Thus, the logs of an e-mail box can be obtained by means of real-time monitoring and transmitted in advance to the requesting authority, even in the absence of a communication (e.g. no e-mail sent during that connection session, or no e-mail received).

27 The Federal Court has held that art. 18b IMAC provides a legal basis for the advance transfer of traffic data resulting from real-time surveillance, to the exclusion of content data, in the absence of a legal or contractual basis.

In the same ruling, the Federal Court opened up the possibility of advance transmission of data within the meaning of art. 18b IMAC to data relating to telephone traffic. Thus, secondary data resulting from active monitoring of a telephone connection (e.g. numbers called or calling, duration of telephone conversation or antenna activated) are data which should be able to be transmitted in advance to a foreign authority on the basis of art. 18b IMAC. In our view, this interpretation by the Federal Court is logical in view of the widespread digitization of telecommunication systems and, consequently, the increasingly obsolete and artificial nature of the distinction between traditional telecommunication systems on the one hand, and computer systems on the other. 28

Art. 18b IMAC has a further advantage: if the collection of traffic data transmitted in advance reveals that a new surveillance measure on another account, another line, etc., in Switzerland or abroad, is justified, the requesting authority can immediately request the execution of such a measure. 29

B. Distinctions

The advance transmission of information relating to computer traffic provided for in art. 18b IMAC must be distinguished from the spontaneous transmission of evidence and information (art. 67a IMAC), which is also an exception to the principle that a final decision is required before any transmission abroad can take place. Unlike the system under art. 67a IMAC, art. 18b IMAC is necessarily involved in the execution of a foreign request for mutual assistance to obtain such evidence. Article 18b IMAC makes no provision for "spontaneous" advance transmission of traffic data. What's more, art. 67a IMAC prohibits the transmission of evidence as soon as it falls within the sphere of secrecy (art. 67 para. 4 IMAC). In such cases, only information may be provided to a foreign authority (art. 67a para. 5 IMAC). 30

The advance transmission of information relating to computer traffic under art. 18b IMAC must also be distinguished from dynamic mutual assistance (art. 80dbis IMAC), which exceptionally allows the advance transmission of information or evidence (a) when foreign investigations into organized crime or terrorism would be excessively difficult without this mutual assistance measure, in particular because of the risk of collusion, or because the confidentiality of the proceedings must be preserved, or (b) in order to prevent a serious and imminent danger, in particular the commission of a terrorist act. The 31

introduction in 2021 of this new provision - accompanied by new rules on the joint investigation team - was seen as an important first step towards more flexible rules and faster, more responsive mutual assistance, based on international trust. In terms of material scope, art. 18b IMAC is unlimited, while art. 80dbis IMAC is limited to organized crime and terrorism, except in cases of grave and imminent danger. Conversely, art. 80dbis IMAC provides that any type of evidence or information may be transmitted in advance by this means, whereas the scope of art. 18b IMAC is limited to data relating to computer traffic, although the Federal Court has paved the way for an analogous application of art. 18b IMAC to telephone surveillance. Finally, art. 18b IMAC does not provide - explicitly at least - for any prior commitment on the part of the requesting authority, the executing authority having to inform the latter that the data transmitted in advance may not be used as evidence before the decision on the granting and scope of mutual assistance has acquired the force of res judicata (art. 18b para. 2 IMAC). On this point, art. 80dbis IMAC is more formalistic (cf. art. 80dbis al. 4 IMAC).

32 Finally, early transmission within the meaning of art. 18b IMAC does not appear to be of particular interest in the context of a Joint Investigation Team (JIT; art. 80dter to 80dduodecies IMAC); indeed, the restricted material scope of art. 80dbis IMAC does not, in the authors' opinion, apply to joint investigation teams, despite the unfortunate reference in art. 80docties IMAC to the conditions of art. 80dbis IMAC.

The authors have written this contribution in their personal capacity. The assessments and opinions presented are their own and are not binding on the Swiss Federal Prosecution Service.

BIBLIOGRAPHY

Böhi Simon, commentaire de l'art. 18b EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1ère 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, 1ère 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, 3e 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, 5e édition, Berne 2019.

MATERIALS

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).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 34 CCC (Convention on Cybercrime)

A commentary by Nicolas Bottinelli / Julien Wenger

SUGGESTED CITATION

Nicolas Bottinelli/Julien Wenger, Commentary of art. 34 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Short citation: OK-Bottinelli/Wenger, art. 34 CCC N. XXX.

Art. 34 Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

CONTENT

I. Introduction 285
II. Notions 285
III. Implementation in Swiss law 287
A. Interception of content data under Swiss law 287
B. Distinctions and special cases 290
1. Advance transmission of content data? 290
2. Distinction between a deposit order (art. 265 CPP) and a surveillance measure (art. 269 et seq. CPP), particularly with regard to e-mail boxes 292
3. Use of a false identity 293
Bibliography 293
Materials 293

I. INTRODUCTION

Part of Chapter III of the Convention on Cybercrime, entitled "International Cooperation", art. 34 CCC deals with international cooperation in relation to content data, as opposed to traffic data, which is covered by art. 33 CCC. 1

The CCC recognizes the importance of being able to intercept content data for the purposes of national criminal proceedings (art. 21 CCC): the collection of telecommunications content data has always been a useful investigative tool for determining whether a communication is illegal, and for providing evidence of past or future offences. Computer communications can constitute or prove the same type of offence, while offering greater possibilities thanks to the transmission of large quantities of data (text, images and sound). It is not possible to determine in real time the harmful and illegal nature of these communications without intercepting the content of the message. If they were unable to establish and prevent the commission of offences at the time they took place, law enforcement authorities would be reduced to investigating past offences, where the harm has already been done. It follows that real-time interception of data relating to the content of computer communications is at least, if not more, important than real-time interception of telecommunications. 2

However, art. 34 CCC places no obligation on States Parties to be able to cooperate in the cross-border collection of such data; at most, the Council of Europe's Explanatory Report refers to the good practices contained in the 1985 Recommendation on the application of the ECCJ to telecommunications surveillance. The Second Additional Protocol to the CCC, of May 12, 2022, does not deal with this measure, nor does the preparatory work for the 3rd Additional Protocol to the ECCJ. 3

II. NOTIONS

Art. 34 CCC provides that the Parties shall afford each other mutual assistance "to the extent permitted by their applicable domestic treaties and laws". Unlike art. 33 CCC, which applies to data relating to computer traffic, art. 34 CCC does not impose any strict obligation on States parties to provide mutual assistance in the interception of data relating to the content of computer communications. The decision to rely on domestic regimes and legislation is 4

justified by the highly intrusive nature of interception, and by the fact that mutual assistance in this area was still in its infancy.

5 The notion of "content data" is not defined in the Convention. It refers to the information content of the communication, i.e. the meaning of the communication or the message or information transmitted by the communication (other than traffic data). In concrete terms, "content data" refers to the communication itself, its very object, i.e. in particular the text of an e-mail (including the Swiss design of the "subject" section), an instant message, any attachments or the audio and/or video file or stream transmitted. This concept is opposed to that of "traffic data", which essentially covers the elements of the communication chain (origin, destination, route, time, date, size and duration of the communication or type of underlying service; art. 1 let. d CCC). This distinction is fundamental to surveillance measures, and has direct consequences for the granting of international mutual assistance. For example, under certain conditions, Switzerland allows the rapid and anticipated transmission of data relating to computer traffic on the basis of art. 18b IMAC, which is excluded in the case of data relating to content (see III.B.1. below).

6 Art. 34 CCC covers "interception in real time", a concept which is opposed to the search of data recorded or stored on a computer medium (server, cloud or other). This direct temporality implies that the person under surveillance has no control over the data. In other words, the data cannot be deleted before it is intercepted. In principle, the "interception" of this data is carried out by a third-party provider (internet and/or telephony providers, providers of derived communication services [hereinafter: FSCD], such as companies managing communication applications). In our view, art. 34 CCC does not cover, in particular, the interception of content data directly from the investigation suspect by means of Trojan Horse software (Govware); however, nothing precludes art. 34 CCC being used as a basis for the interception of communications via an IMSI Catcher.

7 The provision stipulates that mutual assistance is granted for the real-time "collection or recording" of data. In our view, although the distinction between these two terms seems uncertain, collection covers the initial act of gathering the data, while recording concerns its storage with a view to transmission to the requesting authority, or its use in the criminal investigation. These two concepts thus constitute two successive stages necessary for the execution of surveillance, but their distinction has little practical significance.

Furthermore, while at first glance the notions of "collection" and "recording" include that of "transmission" - since this collection takes place at the request and for the needs of a foreign authority - we shall see that the Swiss legislator has distinguished these notions. Indeed, data collected in execution of a request for foreign judicial assistance is not exempt from the usual mutual assistance procedure prior to any transmission of the evidence abroad (cf. in particular infra III.A. ad art. 18a IMAC).

Intercepted data must be linked to "specific communications". This term means that the Convention neither requires nor authorizes the general or systematic surveillance and collection of large quantities of content-related data (mass surveillance). Nor does it authorize "fishing expeditions" in the hope of uncovering criminal activity - a very different situation from investigations into specific cases of unlawful conduct. Obviously, this term does not mean that it is necessary to determine which specific future communication between several computer systems will need to be monitored, since it is only rarely possible to anticipate future communications. What is important to remember, however, is that the object of the surveillance (e-mail address, user ID for an e-mail application, etc.) must be precisely determined. 8

Finally, the Convention does not apply as such to traditional telecommunications (analog telephony), since data must be transmitted via a computer system. The advent of the digital telephone, and more generally the convergence of telecommunications technologies, is nevertheless blurring the distinctions between telecommunications and telecomputing, and the specific features of their infrastructures. As a result, the Convention - in particular art. 21 and 34 CCC - applies to specified communications transmitted by means of a computer system, the communication being able to be transmitted via a telecommunications network before being received by another computer system. 9

III. IMPLEMENTATION IN SWISS LAW

A. Interception of content data under Swiss law

While art. 33 CCC was responsible for the introduction of art. 18b IMAC, which allows data relating to computer traffic to be transmitted to the requesting authority in advance (i.e. prior to the entry into force of a closure decision), art. 34 CCC did not - directly at least - lead to any changes in Swiss legislation concerning the interception of content data. The usual rules of 10

Swiss criminal procedure (art. 269 et seq. CPP) apply, subject to certain reservations, by reference to art. 18a IMAC.

11 Art. 18a IMAC is the key provision governing the surveillance of postal and telecommunications correspondence in the context of mutual legal assistance. In essence, it states that, at the express request of a requesting authority, the Public Prosecutor's Office - and in certain cases even the Federal Office of Justice - may order such surveillance (para. 2), and that the order must be submitted to the competent Court of Compulsory Measures for approval (para. 3). For the rest, art. 18a IMAC refers to arts. 269 to 279 of the Swiss Penal Code and to the Federal Act of October 6, 2000 on the Surveillance of Correspondence by Post and Telecommunication (LSCPT). This reference to art. 269 et seq. of the Swiss Penal Code - in particular to the catalog of offences set out in art. 269 of the Swiss Penal Code - corresponds to the "range of serious offences" that the Parties must define in their domestic law in order to allow the interception of content data (art. 21 and 34 CCC). The general reference to the provisions of the LSCPT also means that art. 18a IMAC applies to both ordinary communications (traditional analog telephony) and communications linked to a computer system (cf. in particular art. 2 let. c LSCPT).

12 In practice, after entering into the matter (art. 80a IMAC), the executing authority will order the surveillance measure through the Service Surveillance de la correspondance par poste et télécommunication (hereinafter: Service SCPT; art. 269 CPP in conjunction with art. 55 ff OSCPT). It will thus be possible to order real-time monitoring of the content and secondary data of network access services (art. 55 OSCPT), real-time monitoring of the content and secondary data of telephony and multimedia services (art. 57 OSCPT) or real-time monitoring of the content and secondary data of e-mail services (art. 59 OSCPT).

13 The executing authority must then have the measure authorized by the Compulsory Measures Court within 24 hours of the order (art. 274 para. 1 CPP). It should be noted that, with regard to the condition of the existence of a "serious suspicion" set out in art. 269 al. 1 let. a CPP, the Federal Court rightly pointed out that, according to the rules on mutual legal assistance and established case law, art. 14 CEEJ, 28 IMAC and 10 OIMAC require the requesting authority to explain what its suspicions consist of, but not to prove them or even make them likely. Subject to the prohibition on exploratory requests, the requesting authority's suspicions need not therefore be particularly serious or

precise. Indeed, while domestic law must be applied when it is more favourable to cooperation than treaty law, it cannot lay down material conditions for mutual assistance that are not provided for in treaty law.

The Compulsory Measures Court rules within five days (art. 274 para. 2 CPP). 14
If surveillance is refused, the documents and recordings collected must be destroyed immediately (art. 277 al. 1 CPP). If authorization is granted, it should be noted that art. 279 of the Code of Criminal Procedure (CCP), which provides for communication to the accused or the third party subject to surveillance, and establishes a right of appeal for the latter, as well as for the monitored telecommunications service (art. 279 para. 3 CCP), does not apply, despite the reference in art. 18a para. 4 IMAC to arts. 269 to 279 CCP. In fact, the conventions and laws applicable to international mutual assistance in criminal matters derogate from the usual system of the Swiss Criminal Code, which only applies if it is more favorable to cooperation than the applicable conventions and laws (principle of favorability). In particular, this means that party status, the right to notification and legal remedies are governed by the specific provisions on mutual assistance. However, according to art. 80m para. 1 IMAC, the obligation to notify decisions on mutual assistance is limited to persons residing or having elected domicile in Switzerland. Any indications to the contrary by the TMC, whether by reference to the law or by imposing conditions within the meaning of art. 274 para. 2 CPP, would therefore be invalid, as the TMC has no jurisdiction over this aspect of the proceedings. As part of the mutual assistance procedure, it will be up to the executing authority to ensure compliance with these conventions and applicable laws, and to make the notifications provided for in art. 80m IMAC.

Upon receipt of the surveillance data, the executing authority must guarantee 15
the right to be heard of the person affected by the surveillance measure (art. 80b IMAC). As we shall see, in the case of content-related data, any advance transmission, i.e. prior to the entry into force of a termination decision, is in principle excluded (see III.B.1. below). Since the coercive measure in question is essentially secret, its disclosure to the person concerned may have serious consequences for the proceedings abroad. A distinction must be made between two situations:

1. If the person concerned is not domiciled in Switzerland or has not elected domicile there, he or she need not be notified of the authority's decision (art. 80m para. 1 IMAC). The decision to close the case will therefore only be noti-

fied to the FOJ (art. 80h let. a IMAC), which means that the result of the surveillance can be passed on to the requesting authority without the person concerned actually having been informed. Of course, if the person concerned applies to the enforcement authority, having taken up residence in Switzerland before the closure decision comes into force, his or her right to take part in the proceedings and to have access to the file must be guaranteed (art. 80b para. 1 in conjunction with art. 80m para. 2 IMAC).

2. If the person concerned by the measure is domiciled in Switzerland or has elected domicile there, the executing authority must guarantee him the right to take part in the proceedings and to consult the file (art. 80b para. 1 IMAC; subject to the specific case of the use of a false identity, cf. infra III.B.3) before any transmission of the means of proof abroad. However, the requesting authority is under no obligation to grant this right to the person concerned as soon as the surveillance measure has been completed. The measure may remain secret for as long as is necessary for the foreign proceedings. The executing authority will have to ascertain from the requesting authority when the existence of the surveillance measure can be disclosed to enable the mutual assistance procedure to continue.

16 At the end of the procedure, the executing authority will issue a closing decision, which may be appealed to the Federal Criminal Court (art. 80e IMAC). A subsequent appeal to the Federal Supreme Court remains possible under the restrictive conditions of art. 84 FSCA (particularly important case).

B. Distinctions and special cases

1. Advance transmission of content data?

17 Under certain conditions, art. 18b IMAC allows the early transmission - i.e. before a decision to close the case has been taken - of data relating to computer traffic collected under an authorized real-time surveillance order. Art. 18b IMAC implements the obligations arising from art. 33 CCC. In the case of content-related data, however, the Federal Court has confirmed that art. 18b IMAC does not apply, and that any early transmission, i.e. prior to the entry into force of a closure decision, is therefore excluded on the basis of this provision. This deprives Switzerland of an important tool in the fight against international crime, particularly organized crime and terrorism. It is also ques-

tionable whether, with this interpretation by the Federal Court, Art. 18a IMAC still has any real practical scope and utility.

In 2021, however, the legislator has introduced new provisions which partly compensate for this shortcoming, and which represent an important step towards more flexible rules and faster, reactive mutual assistance based on international trust. Art. 80dbis IMAC (dynamic mutual assistance) allows, by way of exception, the advance transmission of information or evidence (a) when foreign investigations into organized crime or terrorism would be excessively difficult without this mutual assistance measure, in particular because of the risk of collusion, or because the confidentiality of the proceedings must be preserved, or (b) in order to prevent a serious and imminent danger, in particular the commission of a terrorist act. The aim of this provision is to enable effective prevention in urgent and well-founded cases (e.g. hostage-taking or terrorist attack), by avoiding too late a reaction to planned criminal acts, confidentiality being of great importance in this context. From a material point of view, unlike art. 18b IMAC, which restricts advance transmission to data relating to computer traffic, or even to secondary data relating to conventional telecommunications, art. 80dbis IMAC provides that any type of evidence or information may be transmitted in advance by this means. From a formal point of view, art. 80dbis para. 4 IMAC requires the executing authority to obtain certain additional undertakings from the requesting authority prior to any advance transmission, in particular to use the information or means of evidence only for investigative purposes and under no circumstances to request, motivate or pronounce a final decision (let. a) and to remove from the file of foreign proceedings, if mutual assistance is refused, the information or means of evidence submitted in advance (let. c). If all these conditions are met, there is nothing to prevent the advance transmission of content data under the conditions of art. 80dbis IMAC. 18

On the other hand, early transmission of content-related data can take place within the framework of a Joint Investigation Team (JIT; art. 80dter to 80duodecies IMAC). In this case, it can intervene even if the conditions laid down in art. 80dbis para. 1 let. a and b or para. 2 IMAC are not met. 19

2. Distinction between a deposit order (art. 265 CPP) and a surveillance measure (art. 269 et seq. CPP), particularly with regard to e-mail boxes

20 The secrecy of telecommunications is a constitutional guarantee enshrined in art. 13 para. 1 Cst. This right is an essential aspect of the right to privacy. The monitoring of correspondence and of postal and telecommunications relationships constitutes a serious infringement of this fundamental right. It is therefore essential to distinguish between what is covered by this guarantee and what is not. Two criteria have traditionally been applied to distinguish between cases where information can be obtained directly by a production order and those where an LSCPT request is required:

- the first criterion is the relationship with the telecommunication correspondence;
- the second criterion is whether the data requested falls within the scope of the fundamental right to secrecy of telecommunications protected by art. 13 para. 1 Cst.

21 If both criteria are met, the LSCPT must be applied.

22 In practice, the majority of cases will concern access to the contents of electronic mailboxes (e-mail). In order to distinguish between data covered by the secrecy of telecommunications and data that can be obtained directly by the criminal authorities (filing order under art. 265 of the Criminal Procedure Code), the Federal Court has established the criterion of the time of the e-mail recipient's last access (connection, log) to his or her electronic mailbox. The Federal Court ruled that the communication procedure must be considered as having ended at the moment when the recipient becomes the sole master of the data, i.e. when he accesses his e-mail inbox, irrespective of whether he has actually opened and read the e-mails received. In practice, this means that the public prosecutor will be able to obtain the content of e-mails prior to the last log-in directly from the service provider (art. 265 CPP), whereas he will have to go through the SCPT Service and the Court of Constraint Measures to obtain the content of e-mails subsequent to the last log-in (art. 269 ff CPP). In other words, art. 31 CCC (mutual assistance regarding access to stored data) and not art. 34 CCC applies to the collection and transmission of e-mails prior to the last log.

3. Use of a false identity

In our opinion, anyone who, in order to commit an offence, uses an account 23
on a platform (messaging application, e-mail inbox, etc.) that guarantees a high degree of confidentiality (end-to-end encryption, sometimes coupled with zero-access encryption, little or no data required for registration, etc.) should not be recognized as a party to the mutual assistance procedure, thereby making it more difficult for the criminal authorities to identify him. Indeed, in the absence of any initial identification, there are few means of verifying that the person claiming this status is actually the user of this resource.

The authors have written this contribution in a personal capacity. The assessments and opinions presented are their own and do not commit the Office of the Attorney General of Switzerland.

BIBLIOGRAPHY

Aepli Michael, commentaire de l'art. 18a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1ère 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, 5e édition, Berne 2019.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2e édition., Zurich et al. 2015.

MATERIALS

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).