Procedural Provisions in the Convention on Cybercrime

FILIP RADONIEWICZ

Abstract The objective of this study is to analyse the solutions provided in the Council of Europe Convention on Cybercrime (ETS No. 185) of 23 November 2001 with regard to criminal procedures concerning the obtaining and preservation of evidence in the form of computer data, i.e. preservation of data (Articles 16 and 17), and four measures aimed at data collection (production orders – Article 18, search and seizure of stored computer data -– Article 19, real-time collection of traffic data – Article 20, and interception of content data – Article 21). The investigation of this subject-matter is preceded by an introductory part in which the key notions defined in the Convention on Cybercrime – namely computer data, computer system, service provider and traffic data – are discussed.

Keywords: • cybercrime • online search • on-line operational activities • hacking • interception of content data

CORRESPONDENCE ADDRESS: Filip Radoniewicz, Ph.D., War Studies University, Department of Cyber Security Law and New Technologies, Institute of Law, Centre for Cybersecurity Studies, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, e-mail: filip.radoniewicz@radoniewicz.eu, ORCID: 0000-0002-7917-4059.

https://doi.org/10.4335/2022.1.12 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

The Convention on Cybercrime (the Council of Europe Convention on Cybercrime (ETS No. 185) of 23 November 2001) is the first international treaty that deals with combating crimes committed with the use of the Internet and computer networks.

Representatives of most Member States of the Council of Europe (including Poland) and, in the capacity of observers, delegates from the USA, Japan and Canada, representatives of EU institutions and independent experts took part in the works on the Convention, which took over four years to be completed. The objective of the Convention on Cybercrime was to create a legal framework for prosecuting crimes. Numerous innovative solutions were proposed in the Convention (innovative at the time – we should bear in mind that it was being drafted at the end of the last century). The list of offences was extended in relation to previous international documents (*Computer-Related Crime. Analysis of legal policy in the OECD Area*, OECD, ICCP Series No. 10, Paris 1986; *Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*, Council of Europe, Publishing and Documentation Service, Strasbourg 1990). They include, i.a., illegal access, illegal interception, data interference, system interference, offences related to hacking tools – misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights). It also includes provisions concerning the penal liability related to individual stages of an offence (attempt), the forms of accessory liability (aiding and abetting), and corporate liability (this term is understood also as the liability of non-corporate organisational units). The Convention also sets out a number of procedural solutions, such as the preservation of data, search and seizure of stored computer data, etc. These were included in Section 2 of the Convention (Procedural law). They should, first and foremost, be applied to proceedings concerning "conventional" offences (i.e. offences established in accordance with Articles 2 through 11 of the Convention). In addition, they should be applied in relation to all other offences committed by means of a computer system, and the collection of evidence in electronic form in the course of criminal proceedings concerning other offences (Radoniewicz, 2016: 162-165).

2 Explanation of key terms

Before the provisions stipulated in Section 2 of the Convention are discussed, it is necessary to explicate the most important terms, i.e. "computer system", "computer data", "service provider" and "traffic data".

In the light of Article 1(a) of the Convention, a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

According to the Explanatory Report (*Explanatory Report to Convention on Cybercrime*

– a commentary to the Convention prepared by its authors, Points 23 and 24), a "computer system" is a device consisting of hardware and software. "Hardware" may include input, output and storage facilities. A 'computer program' is a set of instructions that can be executed by the computer system to achieve the intended result. A "computer system" usually consists of different devices. A "central processing unit" is the indispensible component. Other elements are "optional" and include "peripherals" (devices that perform certain specific functions in interaction with the processing unit, such as a video screen, printer, DVD reader/writer or other storage devices, etc.). In the light of the Convention on Cybercrime, computer systems include mobile phones, decoders and, most of all, a device which is commonly understood as a stand-alone "personal computer" (PC), i.e. a single host. Furthermore, two or more independent interconnected computer systems (i.e. able to communicate computer data) comprise a "network". The connections through which data is transmitted may be earthbound (e.g., wire or cable) and/or wireless (e.g., radio). A network may have a different geographical reach – from small "local area networks" (LANs) – composed of several computers, to networks spanning a large area ("wide area networks" – WANs). Computer systems may be connected to the network as endpoints (single hosts, decoders, phones, etc.) or as a means to assist in the data transfer process, such as routers or servers. The prerequisite for considering a given structure a network is the exchange of data over the network.

"Computer data" means any representation of facts, 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.

As per Article 1(c) of the Convention, the term "service provider" is understood as 1) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and 2) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

In general, the term "service provider" encompasses two categories of entities: "content providers", i.e. entities providing access to their own services (content) (e.g. web portal operators), and entities intermediating in the access to services – "intermediary service providers", broken down into "access providers" and "service providers", namely entities which transmit, store and provide access to information on the Internet. In some cases the same entity performs both functions, e.g. a web portal operator may at the same time post its own content (thus being a content provider) and render services to other entities, e.g. a hosting service (storage of data provided by third parties – clients). This usually consists in providing access to own servers (or, for instance, virtual digital platforms). It might include, for example, the maintenance of a client's website on a server, in which event, the service provider concerned assumes the role of an intermediary service provider. This distinction is significant from the legal point of view, due to the exclusion of liability in the event of rendering certain services by entities belonging to the last group (i.e. intermediary service provider offering the aforementioned hosting, mere conduit and caching (temporary and automated data storage in order to accelerate further access to it

– e.g. downloading the most popular websites among network users to the servers of a local area network to facilitate fast access to them).

Based on the definition provided in Article 1(c), it can be inferred that, for the purpose of the Convention on Cybercrime, the term 'service providers' refers only to the group of intermediary service providers. According to the definition, they encompass public or private entities which provide the users of its services the ability to communicate by means of a computer system, or other entities that process or store computer data on behalf of such communication service or users of such service (which means that they have mere conduit, hosting or caching in their service portfolio).

Under Article 1(d) of the Convention, "traffic data" is defined as any computer data relating to a communication by means of a computer system, generated by a computer system (e.g. a mobile phone, a computer, but also router or server, as points on the data transfer route) that formed a part in the chain of communication, indicating the communication's origin (a place where data transfer was initiated, expressed as, most of all, an IP address, optionally a phone number, or a similar identification of a communications facility to which a service provider renders services), destination (the identification data of a communications facility to which communications are transmitted is the same as that of the communications facility being a location where data transfer was initiated), route, time, date, size, duration, or type of underlying service (e.g. file transfer, or electronic mail). Traffic data can assume a dynamic form, i.e. data on transmission (data included in packet headers) and static form, such as system logs stored in firewalls, routers or servers (including information about any events taking place in the networks, including the details of participating entities). E-mail addresses and IP addresses are undoubtedly traffic data.

Certain doubts may arise when qualifying URL addresses or search criteria entered in a search engine. On the one hand, it is a set of simple instructions in a binary code, allowing users to obtain information from the web. In this context, they have the features of traffic data. On the other hand, they constitute a form of communication, because they indicate what a given user has in mind by entering a URL address or a phrase in a search engine. Similar issues can be observed as regards HTTP requests that may include such information as user's e-mail address, recently visited websites or search criteria (Clough, 2013: 153-154).

3 Conditions and safeguards

In Article 15 of the Convention, emphasis was placed on the protection of human rights. Pursuant to this provision, the establishment, implementation and application of the powers and procedures provided for in the Convention are subject to conditions and safeguards provided for under the domestic law of each Party, which should ensure the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the

Protection of Human Rights and Fundamental Freedoms (ECHR), the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments. It was also stressed that the adopted measures must incorporate the principle of proportionality, and such conditions and safeguards should, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party is obliged to consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties. Since the Convention is to be applied by states having different legal systems, it is not possible to define the conditions and safeguards applicable for each power and procedure provided for in its provisions. Therefore, certain common standards and minimum safeguards to be observed by Parties to the Convention have been indicated. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments, i.e. primarily the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols (Explanatory Report, Point 145).

4 Procedural provisions

The Convention provides for five new measures – one aimed at the preservation of data (Articles 16 and 17), and four aimed at data collection (production order – Article 18, search and seizure of stored computer data – Article 19, real-time collection of traffic data – Article 20, and interception of content data – Article 21).

The first of the instruments laid down in the Convention involves the granting of powers to competent law enforcement authorities of the Parties to order network administrators, or to similarly obtain, the expeditious preservation of specified computer data, including traffic data that has been stored by means of a computer system, and has probative value. This measure may be applied, in particular, where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

This construct should not be confused with data retention – which is limited to traffic data and includes the data of all entities operating in the network. It involves the retention by providers of publicly available electronic communications services or of a public communications network of the so-called “transfer data” (traffic and location data, and the related data necessary to identify the subscriber or registered user) generated or processed by such service providers, in order to ensure their availability for the purposes of investigation, detection and prosecution of criminal offences. As regards EU law, the obligation to retain data for a period of not less than six months and not more than two years from the date of the communication was imposed under Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks and amending Directive 2002/58/EC (OJ EU 2006 L 105/54). It was rendered invalid as a result of the Judgement of the Court of Justice of 8 April 2014 (Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications et al., ECLI:EU:C:2014:238).

The preservation of data provided for in the Convention refers to specific data regardless of data type.

The preservation order should impose an obligation on the person in possession of (or controlling) computer data to preserve and maintain the integrity of specified stored computer data in that person's possession or control for as long as necessary, but no longer than ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. There should also be a possibility to oblige the custodian or other person required to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law (Article 16(3)).

As regards traffic data to be preserved under Article 16, in Article 17, it is stipulated that Parties are obliged to ensure that the expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication, and ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the authority to identify the service providers and the path through which the communication was transmitted.

Due to the significant controversies between state governments in relation to the issues of cross-border evidence collection, the Convention does not impose any specific solutions in this respect, instead only encouraging states to cooperate on this matter. Accordingly, the cross-border access to evidence will be as deemed appropriate by a given state, in line with the recommendations of the Convention. It is an open issue whether solutions will be harmonised. However, the Convention requires the adoption of certain "minimum procedures" (see Article 23) (Weismann 2011: 273).

The next legal construct provided for in the Convention is the "production order" described in Article 18. It may be addressed both to a person in the territory of the issuing party, and to a service provider offering its services in the territory of the Party. In the former case, it entails an obligation of the person indicated in the order to submit specified computer data in that person's possession or control, which is stored on a computer system or a computer-data storage medium, and as regards the latter case, an obligation to "submit subscriber information" relating to such services in that service provider's possession or control. As per Article 18(3), "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: 1) the type of communication service used, the technical

provisions taken thereto and the period of service; 2) 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; 3) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Article 19(1) provides for a measure that involves empowering competent law enforcement authorities of a Party to search a computer system or part of it and computer data stored therein, and a computer-data storage medium in which computer data may be stored, or "similarly access" a computer system or part of it and computer data stored therein, and a computer-data storage medium in which computer data may be stored in its territory.

Article 19(2) of the Convention provides an "invasive" form of search, i.e. extended search. The provision allows law enforcement authorities to extend the scope of "search operations" (e.g. to search or similarly access computer data, as provided for in Article 19(1a)) to include the resources stored in another computer system or its part, accessible from or available to the initial system, if they have grounds to believe that the data sought is stored in another computer system or part of it. The other computer system or its part must be located in the territory of the state concerned. The convention does not define the procedure for extending the search. This is left to domestic law. The authors of the Convention give several examples of possible solutions: 1) empowering the judicial or other authority which authorised the search of a specific computer system ("initial" computer system) in a specified network (mainly LAN) to authorise the extension of the search or similar access to a connected system ("secondary or further computer system") if there are grounds to believe (to the degree required by national law and human rights safeguards – e.g. high probability verging on certainty) that the connected computer system may contain the specific data that is being sought in proceedings under which a relevant decision has been issued; 2) empowering the investigative authorities to extend an authorised search or similar access of a specific computer system to a connected computer system where there are similar grounds to believe that the specific data being sought, relevant to the proceedings being conducted, is stored in the other computer system; 3) or exercising search or similar access powers at several locations simultaneously (i.e. both in the initial and secondary systems, which means that it is not precisely an extended search, taking into account that the secondary system is not accessed through the initial system in this case) in a coordinated and expeditious manner (so-called "simultaneous search").

In all cases, the data to be searched must be lawfully accessible from or available to the initial computer system (Explanatory Report, Points 193-195).

It is worth stressing that the extended search constitutes a significant interference in the privacy of computer system users, as there is no possibility to control the search operations, and law enforcement authorities gain wide access to data during the search,

whereas at the same time the rights of persons affected by such actions are not properly secured (it is worth remembering that these are often random computer systems – for example, systems connected to the same local area network).

For that reason, search extension was one of the several solutions which were most criticised by non-governmental organisations during the works on the Convention (in addition to criminalising activities concerning the so-called "hacking tools" – Article 6 of the Convention).

Therefore, the parties to the Convention have been obliged to establish conditions and safeguards which should provide for the adequate protection of human rights and liberties (the aforementioned Article 15).

I believe that, in line with the principle of proportionality and subsidiarity, it would be advisable to include a provision stipulating that a search may only be extended where it is not possible to otherwise obtain the data sought, and in the event where there is a high probability that the data is stored in a connected computer system, while the application of the measure should be limited to matters related to the most serious prohibited acts provided for by law.

Paragraph 3 sets out the obligation to empower the competent authorities of a Party to seize or similarly secure computer data accessed as a result of search, including the power to: 1) seize or similarly secure a computer system or part of it or a computer-data storage medium; 2) make and retain a copy of those computer data; 3) maintain the integrity of the relevant stored computer data; 4) render inaccessible or remove those computer data in the accessed computer system.

According to the authors of the Convention, it is necessary to empower its competent law enforcement authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as reasonable, the necessary information to enable the undertaking of the relevant measures (Article 19(4)).

Pursuant to Article 20(1), a measure entailing the real-time collection of traffic data was introduced. The Convention provides for its two variants, including the collection or record of data through the application of technical means independently by a competent authority, or through, or with the assistance of, service providers, as the Parties may compel a service provider to collect or record traffic data through the application of its own technical means or to co-operate and assist the competent authorities in these operations. The two variants are not alternatives – each Party must ensure that both measures can be carried out. According to Point 223 of the Explanatory Report, such solution is necessary in case a service provider does not have the technical ability to assume the collection or recording of traffic data. Furthermore, in the event of some local area networks (LANs), where no service provider may be involved, the only way for

collection or recording to be carried out would be for the law enforcement authorities to do it themselves. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures in question, it may limit itself to other measures, such as only relying on the operations of service providers (Article 20(2)).

The discussed provision at the same time limits the adoption of the measures by a Party to criminal proceedings in specific cases, and to traffic data associated with specified communications "in its territory."

Each Party should adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in the discussed Article (Article 20(3)).

As regards the interception of content data (computer surveillance), it is assumed that this investigative measure must be restricted to a range of serious offences. The initiative to compile a list of such offences is left to the Parties.

The measure may be applied only in the course of criminal proceedings, as it entails the collection of content data, in real-time, of specified communications in its territory transmitted by means of a computer system. Similarly to traffic data, the Convention provides for two possible variants of such measures – the collection and recording of content data by law enforcement authorities, and "the employment" of service providers to perform the activities, so that within their existing technical capability, they collect or record content data through the application of technical means on the territory of that Party, or co-operate and assist the competent authorities in the collection or recording of content data. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1(a) (collection and recording of data by law enforcement bodies), such Party may limit the measures to relying on the operations of service providers only.

Of course, similarly to collecting and recording traffic data, each Party should adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in the discussed Article (Article 21(3)).

Each Party may reserve the right to apply the measures stipulated in Article 20 solely to criminal offences or categories of offences specified in the reservation, provided that the scope of such offences or categories is not more restricted than the scope of offences to which it applies the interception measures referred to in Article 21. Each Party should consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20 (Article 14(3)(a)). Where a Party, due to limitations in its legislation in force is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system is being operated for the benefit of a closed group of users, and does not employ

public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications.

At the same, it has been stressed that each Party should consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20 (Article 14(3)(b)).

To conclude, it is worth mentioning one more important issue – the nature of traffic data and the degree of its protection. As noted above, the data includes information on the events in the network and details of participating entities. Therefore, they have significant probative value. At the same time, the data can say a lot about network users (whom a given person has contacted, which websites he/she visited, what services he/she uses ...). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures, pursuant to Articles 14 and 15 (Explanatory Report, Point 227). It should be noted that the European Court of Human Rights (ECtHR) found that the use of traffic data constituted interference in the right to respect for private life, within the meaning of Article 8 of the ECHR. In the Judgement in the Malone v. the United Kingdom case (ECtHR Judgement of 2 August 1984, Application No. 8691/79), the Court found that the so called "metering" (recording phone calls made from a given device by registering the numbers dialled and the time and duration of each call), which is a standard activity made by telecommunications service suppliers, per se cannot be considered as interference in the right to privacy. However, the release of the information obtained this way without the consent of the subscriber amounts to the interference with a right guaranteed by Article 8 ECHR. In the Court's view, this stems from the fact that the metering records contain information that is an integral element in the communications made by telephone. In a ruling made in the Copland case (ECtHR Judgement of 3 April 2007 in the Copland v. the United Kingdom case, application No. 62617/00), the Court stressed that the data related to e-mail and Internet usage (i.e. traffic data) were subject to protection equivalent to that of telephone conversations.

5 Conclusions

It is a truism to say that international cooperation is of key significance in combating offences committed by means of computer networks. Telecommunications networks span the entire globe. The perpetrators' conduct can simultaneously affect numerous countries located in distant parts of the world. In addition to close cooperation between law enforcement authorities, as one of the formal conditions of such collaboration (due to the principle of dual criminality), it is important to ensure the criminalisation of computer crimes in the greatest possible number of states, reaching a situation where there are no so-called "hacker havens", which are the countries in which their operations are not prosecuted, and to introduce legal measures allowing the conduct of criminal proceedings

in cybercrime matters in the legislations of such states, such measures being "on-line" operational activities discussed in the present study.

Currently, the only international agreement addressing measures against computer crime is the Convention on Cybercrime. This paper discussed the procedural solutions proposed in the Convention. As of time this paper was written, they should have been adopted in several dozen countries that have ratified the Convention. Some of its unquestionable advantages include the open-ended nature of the Convention – it may be acceded by states that are not members of the Council of Europe, and the provisions of optional clauses. They allow the adoption of the Convention on Cybercrime with the exception of certain provisions, thanks to which the state parties implementing the Convention to their domestic laws may reconcile it with their own legal tradition and culture, and the legal regulations in force. Given the above, nearly all Member States of the Council of Europe signed the Convention on Cybercrime by 17 September 2021 (46 countries to be exact, as only Russia has not signed the Convention), and 45 states ratified the document (apart from Russia, which is obvious, Ireland has not ratified the Convention yet). The Convention has also been signed by four non-European states (Canada, Japan, the United States, the Republic of South Africa; and ratified by three of these countries, except the RSA), while further 17 countries (including Australia, Dominican Republic, Israel, Panama) acceded to it. In total, the Convention was ratified by 66 states. As a side note, it should be mentioned that numerous countries that had not signed the Convention decided to use its provisions to draft their own domestic laws. They include Botswana, Egypt, the Philippines, and Pakistan (Brunst, Gecrke, 2009: 53).

References:

Clough, J. (2013) *Principles of Cybercrime* (Cambridge: University Press).
Brunst, P.W. & Gecrke, M. (2009) *Praxishandbuch Internetstrafrecht* (Stuttgart: Kohlhammer).
Radoniewicz, F. (2016) *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym* (Warszawa: Wolters Kluwer).
Weismann, M.F. (2011) International cybercrime: Recent developments in the law, In: Clifford, R.D. (ed.) *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime* (Carolina: Academic Press), pp. 257-294.