Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence

1. BACKGROUND

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention), which was opened for signature in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime and electronic evidence. After 20 years, it still remains the most significant one in the area. Currently, 69 countries are Parties to the Budapest Convention, including 26 EU Member States [1].

In 2003, the Budapest Convention was extended by an Additional Protocol covering offences of racist or xenophobic nature.

Following significant developments in the field of information and communication technology which took place since the adoption of the Budapest Convention, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Second Protocol) was adopted by the Committee of Ministers of the Council of Europe in November 2021 and was opened for signature by the Parties to the Budapest Convention in May 2022 [2].

A review of the Second Protocol is available in the dedicated SIRIUS Quarterly Review here.

The Budapest Convention aims at:

- Criminalising the conduct pertaining to cyber-related crime;
- Supporting the investigation and prosecution of these crimes as well as of other offences committed by means of a computer system or evidence in relation to which is in electronic form by providing necessary procedural tools; and
- Setting up a fast and efficient system for international cooperation [3].

The scope of the Budapest Convention goes considerably beyond the scope of this review, especially when it comes to procedural measures and international cooperation tools. Further, the provisions of the additional protocols to the Budapest Convention are also not covered by this review.

The Budapest Convention is accompanied by an Explanatory Report which is intended to guide and assist Parties in its application.

Furthermore, the Budapest Convention is backed up by a number of capacity building projects, which are managed by the Cybercrime Programme Office of the Council of Europe (C-PROC).

The Cybercrime Convention Committee (T-CY) [4] issued **13 Guidance Notes** which, although not binding, are aimed at facilitating the effective use and implementation of the Budapest Convention:

1. Notion of "computer system"
2. Botnets
3. Transborder access to data (Article 32)
4. Identity theft and phishing in relation to fraud
5. DDOS attacks
6. Critical information infrastructure attacks
7. New forms of malware
8. Spam
9. Aspects of election interference by means of computer systems
10. Production orders for subscriber information (Article 18)
11. Aspects of terrorism
12. Aspects of ransomware
13. The scope of procedural powers and of international co-operation provisions

All these elements establish a mechanism which remains highly relevant even after 20 years.

[1] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. All EU Member States, except for Ireland.
[2] https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention.
[3] Budapest Convention, Preamble; Explanatory Report, para. 16.
[4] The TC-Y, which includes representatives from all the State Parties to the Budapest Convention, assesses the implementation of the Budapest Convention and makes recommendations in this respect.

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

Figure 1 – The mechanism of the Budapest Convention[5]

2. SCOPE

- **Legal regime covered**

Providing a global legal framework on cybercrime and gathering electronic evidence, the Budapest Convention covers:

Crimes	Procedural measures	International cooperation tools
- Illegal access - Illegal interception - Data interference - System interference - Misuse of devices - Computer-related forgery - Computer-related fraud - Child Sexual Exploitation Material - IPR-offences	- Expedited preservation - Production orders - Search and seizure - Real-time collection of traffic data - Interception of content data - Conditions and safeguards applicable to all aforementioned powers	- Extradition - Mutual legal assistance (MLA) in absence of treaty - Spontaneous information - Expedited preservation - Partial disclosure of traffic data - MLA for accessing stored computer data - Transborder access to stored computer data - MLA for real-time collection of traffic data - MLA for interception of content data - 24/7 Network

Figure 2 – Areas covered by the Budapest Convention

- **Data covered**

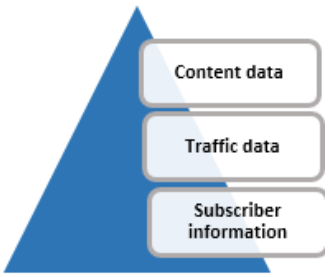

Figure 3 – Data categorization in the Budapest Convention

Subscriber information[6] (Article 18(3) of the Budapest Convention)

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 and by which can be established:

- The type of communication service used, the technical provisions taken thereto and the period of time during which the person subscribed to the service;
- The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider; or
- Any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Traffic data (Article 1(d) of the Budapest Convention)

Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

[5] T-CY, The Budapest Convention on Cybercrime: benefits and impact in practice, 13 July 2020, p. 4.

[6] It is notable that the definition of "subscriber information", as per Article 18(3) of the Budapest Convention, may also include information that under the domestic law of some EU Member States is considered as traffic data.

Content data (Explanatory Report, para. 209)

"Content data" is not defined in the Budapest Convention itself but refers to the content of the communication; i.e. the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).

The division of data into **three categories** (subscriber data, traffic data and content data), which may exists in **two forms** (stored or in the process of communication) set out in the Budapest Convention is often considered as a common starting point and a reference for the general classification and definition of data categories.

⚠ The applicability of procedures to a particular type or form of electronic data depends on the nature and form of the data and the nature of the procedure, as specifically described by each measure provided for in the Budapest Convention[7].

- **Substantive criminal law provisions covered**

Aiming to prevent and suppress computer- and computer-related crime and establishing a minimum standard of relevant offences, the Budapest Convention provides for the criminalization of a number of types of conduct set out in Articles 2 to 10 of the Budapest Convention[8].

- **Scope of the procedural powers and international cooperation provisions covered**

The procedural powers and international cooperation provisions covered by the Budapest Convention include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that the provisions of the Budapest Convention apply either where a crime is committed by use of a computer system, or where a crime not committed by use of a computer system (for example a murder) involves electronic evidence.

This is also confirmed in Guidance Note #13, which states that: "The T-CY agrees that the procedural law provisions and the principles and measures for international co-operation of the [Budapest Convention] are applicable not only to offences related to computer systems and data but also to the collection of electronic evidence of any criminal offence."

There are two exceptions from this scope of application:

- The measure of a real-time **interception of content data** is **limited to serious offences**, which has to be determined by domestic law[9].
- On the basis of a reservation, Parties may **limit** the measure of **real-time collection of traffic data** to the same range of offences to which they apply the powers and procedures of real-time interception of content data[10].

- **Entities covered**

Article 1 of the Budapest Convention defines **service providers** as:

- Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and
- Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

3. DEFINING THE TOOLBOX

A - PROCEDURAL MEASURES

Section 2 of the Budapest Convention includes a number of procedural measures for obtaining access to data for the purpose of specific criminal investigations or proceedings, such as expedited

[7] Explanatory Report, para. 136.

[8] As the Budapest Convention uses technology-neutral language, the substantive criminal law offences may be applied to both current and future technologies involved.

[9] Budapest Convention, Article 21; Explanatory Report, para. 142.

[10] Budapest Convention, Article 20; Explanatory Report, para. 143.

preservation of stored computer data (Article 16), expedited preservation and partial disclosure of traffic data (Article 17), production orders for subscriber information (Article 18), search and seizure of stored computer data (Article 19), real-time collection of computer data (Article 20) and interception of content data (Article 21).

Considering the global reach of services of service providers, regardless of their location, **Article 18 of the Budapest Convention** provides the legal framework for the implementation into the national law of the Parties to the Budapest Convention of two types of **domestic measures that, according to some Parties, may have cross-border (extraterritorial[11]) effects**:

- Domestic production orders for any type of data when a person (including a service provider) is in the territory of a Party, even if the data sought is stored in another jurisdiction (Article 18(1)(a)); and
- Domestic production orders for subscriber information where a service provider is not necessarily present in the territory of a Party but is offering a service in the territory of such Party (Article 18(1)(b)).

Although not binding, Guidance Note #10, adopted by the T-CY, provides Parties to the Budapest Convention with a common way of interpretation of Article 18.

More information about the toolbox available under Article 18 of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review here.

B - INTERNATIONAL COOPERATION

As regards the tools for international cooperation, the Budapest Convention makes it clear that international cooperation is based on the principle of cooperation "to the widest extent possible" for the purposes 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[12]. The Budapest Convention then sets out the following.

- **General principles**

Section 1 of the international cooperation chapter of the Budapest Convention includes provisions on:

- General principles relating to international co-operation (Article 23);
- Extradition (Article 24);
- Mutual assistance (Article 25);
- Spontaneous information (Article 26);
- Procedures pertaining to mutual assistance requests in the absence of applicable international agreements (Article 27); and
- Confidentiality and limitation on use (Article 28).

The purpose of these provisions is to facilitate cooperation among States that **do not have any specific international cooperation treaties** between them. For example, the provisions under Article 25 (General principles relating to mutual assistance), Article 27 (Procedures pertaining to mutual assistance requests in the absence of applicable international agreements) and Article 28 (Confidentiality and limitation on use) are intended only to fill in the gaps in case no other binding international instruments apply.

- **Specific provisions**

Section 2 of the international cooperation chapter sets out a number of provisions which are unique to the Budapest Convention, including:

- Expedited preservation of stored computer data (Article 29);
- Expedited disclosure of preserved traffic data (Article 30);
- Mutual assistance regarding accessing of stored computer data (Article 31);
- Trans-border access to stored computer data with consent or where publicly available (Article 32);

[11] It is noted that the term "extraterritorial" is not used in the text of the Budapest Convention itself, its Explanatory Report or Guidance Note #10. However, for the purposes of the present document, the term is to be understood to refer to a domestic order with potential cross-border effects.

[12] Budapest Convention, Article 23.

- Mutual assistance in the real-time collection of traffic data (Article 33); and
- Mutual assistance in the real-time collection of content data (Article 34).

With regard to the **expedited preservation and disclosure of data**, **Article 29 of the Budapest Convention** provides that, when criminal justice authorities from one Party need to **preserve data that is stored by means of a computer system located in another Party** of the Budapest Convention, they are able to request that the competent authorities of the other Party order the expeditious preservation of such data. However, there is a requirement to declare that a formal request for mutual assistance for the search or similar access to data will follow. Upon receipt of a request under Article 29, the requested authorities must take all appropriate measures to expeditiously preserve the data.

Article 30 of the Budapest Convention refers to previous preservation orders pursuant to Article 29 and only allows for the **disclosure of a very narrow set of traffic data**, namely the data required to allow the requesting authorities to understand that the sought information is stored by a service provider located in another country (not in the requested Party).

With regard to **trans-border access to data**, **Article 32 of the Budapest Convention** provides a possibility for competent authorities from one Party to **unilaterally access computer data stored in another Party**, when the data is either **publicly available** (Article 32(a)) or with the consent of the person who has the lawful authority to disclose the data (Article 32(b)).

Although not binding, Guidance Note #3, adopted by the T-CY, provides Parties to the Budapest Convention with a common way of interpretation of Article 32.

More information about the toolbox available under Article 32 of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review here.

- **24/7 network of points of contact**

Article 35 of the Budapest Convention further provides a tool for **expedited international cooperation on cybercrime and electronic evidence** between the Parties to the Budapest Convention[13]. It requires Parties to establish **points of contact available 24 hours a day, 7 days a week**, which shall **facilitate**, or, if permitted by its domestic law and practice, **directly carry out** a number of specific measures, namely:

- The provision of technical advice (Article 35(1)(a));
- The preservation of data pursuant to Article 29 (Expedited preservation of stored computer data) and Article 30 (Expedited disclosure of preserved traffic data) of the Budapest Convention (Article 35(1)(b)); and
- The collection of evidence, the provision of legal information and locating of suspects (Article 35(1)(c)).

The Second Protocol will bring new responsibilities for the 24/7 network in order to enhance international cooperation between States, as well as cooperation with the private sector[14].

Specifically, Article 9 of the Second Protocol provides a basis for cooperation between authorities for the **disclosure of stored computer data in emergency situations**. It permits each Party to utilize their 24/7 points of contact established under the Budapest Convention to both send and receive immediate requests to a point of contact in another Party "seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data" in an emergency situation, **without the need to send an MLA request**[15].

Furthermore, pursuant to Article 10 of the Second Protocol, Parties may seek **expedited MLA in case of an emergency**. Parties may also make a declaration that emergency MLA requests under Article 10 of the Second Protocol may be sent, among other channels, **from the 24/7 point of**

[13] https://www.coe.int/en/web/cybercrime/24/7-network-new-#{%22105166685%22:[0,1,2,3]}.

[14] Ibid.

[15] Second Protocol, Article 9(1)(b).

contact in the requesting country to the 24/7 point of contact in the receiving country[16].

A review of Article 35 of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review here.

4. CONDITIONS AND SAFEGUARDS

Articles 14 and 15 of the Budapest Convention set out conditions and safeguards applicable to all powers and procedures covered by the Budapest Convention.

- **Purpose limitation**

In accordance with Article 14(1), the powers and procedures set out in the Budapest Convention are to be established for the purpose of "specific" criminal investigations or proceedings, in particular cases, concerning specific individuals. This also excludes their use for, e.g., crime prevention or intelligence gathering purposes.

- **Protection of human rights**

Article 15(1) of the Budapest Convention requires Parties to ensure that the powers and procedures established under the Budapest Convention are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or minimum safeguards arising pursuant to a Party's obligations under applicable international human rights instruments[17].

- **Principle of proportionality**

Article 15(1) of the Budapest Convention further requires Parties to apply the principle of proportionality. This will be done in accordance with each Party's relevant domestic law principles. For European countries, these principles will be derived from the European Convention on Human Rights (ECHR) and related jurisprudences, meaning that the measures must be proportional to the nature and circumstances of the offence. Other Parties may apply related domestic law principles, such as limitations on overly broad production orders and reasonableness requirements for searches and seizures. Another example of the application of the proportionality principle is an explicit limitation to use interception measures only for serious offences[18].

- **Other conditions and safeguards**

Pursuant to Article 15(2) of the Budapest Convention, applicable conditions and safeguards include, as appropriate, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. Other safeguards that should be addressed under domestic law include the right against self-incrimination, legal privileges, and specificity of individuals or places which are the object of the application of the measure[19].

- **Public interest, sound administration of justice and rights of third parties**

Pursuant to Article 15(3) of the Budapest Convention, when applying the measures provided by the Budapest Convention, Parties shall first consider the sound administration of justice and other public interests (for example public safety, public health, the interests of victims, respect for private life). To the extent that it is consistent with these interests, consideration shall also be given to the impact of those measures on the rights, responsibilities and legitimate interests of third parties, which may include minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure or protection of proprietary interests[20].

[16] Second Protocol, Article 10(9).
[17] These instruments include the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and its additional protocols (in respect of European states that are parties them), other applicable human rights instruments, such as e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights (in respect of states in other regions of the world which are parties to them) and the 1966 International Covenant on Civil and Political Rights (Explanatory Report, para. 145).
[18] Explanatory Report, para. 146.
[19] Explanatory Report, para. 147.
[20] Explanatory Report, para. 148.

5. THE WAY FORWARD

The Budapest Convention continues to be a point of reference for the world when drafting legislation on cybercrime and electronic evidence, with its clear benefits and membership which is continuing to increase (see also the Annex).

Under Article 46 of the Budapest Convention, the Parties have an obligation to consult periodically with a view to facilitating:

- The effective use and implementation of the Budapest Convention;
- The exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form; and
- The possible supplementation or amendment of the Budapest Convention.

The T-CY facilitates this regular exercise of consultation, as all the Parties to the Budapest Convention are members thereof, contributing to the evolution of the Budapest Convention. The work of the T-CY in regard to the evolution of the Budapest Convention has recently materialised through the adoption and opening for signature of the Second Protocol (see section Background).

In addition, in November 2021, the T-CY also established a Working group on **undercover investigation and extension of searches**, tasked to prepare a report on, among others, extension of searches, containing draft options and recommendations for further action by the T-CY (for example, guidance notes, documenting experiences and best practices, or negotiation of a binding instrument)[21].

[21] T-CY, Working group on undercover investigations and extension of searches: Terms of Reference, 15 November 2021, p. 1.

ANNEX
STATES WHICH HAVE RATIFIED THE BUDAPEST CONVENTION AS OF JANUARY 2024[22]

Albania	Finland	North Macedonia
Andorra	France	Norway
Argentina	Georgia	Panama
Armenia	Germany	Paraguay
Australia	Ghana	Peru
Austria	Greece	Philippines
Azerbaijan	Hungary	Poland
Belgium	Iceland	Portugal
Bosnia and Herzegovina	Israel	Romania
Brazil	Italy	San Marino
Bulgaria	Japan	Senegal
Cabo Verde	Latvia	Serbia
Cameroon	Liechtenstein	Slovak Republic
Canada	Lithuania	Slovenia
Chile	Luxembourg	Spain
Colombia	Malta	Sri Lanka
Costa Rica	Mauritius	Sweden
Croatia	Republic of Moldova	Switzerland
Cyprus	Monaco	Tonga
Czech Republic	Montenegro	Türkiye
Denmark	Morocco	Ukraine
Dominican Republic	Netherlands	United Kingdom
Estonia	Nigeria	United States of America

[22] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.