THE BUDAPEST CONVENTION ON CYBERCRIME AND CROSS BORDER ACCESS TO ELECTRONIC EVIDENCE

Last update: 13/07/2022

The scope of the 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 Convention are also not covered by this review.

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

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

In addition, the Cybercrime Convention Committee (T-CY) issued 11 Guidance Notes which are not binding and are aimed at facilitating the effective use and implementation of the 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

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

---

1 All EU Member States, except Ireland; see also Annex
3 Convention on Cybercrime, Preamble; Explanatory Report, para. 16.
4 The TC-Y, which includes representatives from all the State Parties to the Convention, assesses the implementation of the Convention and makes recommendations in this respect.
2. THE SCOPE

- Legal regime covered

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

![Fig.2 Areas covered by the Budapest Convention on Cybercrime](image)

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

![Fig.3 Data categorization in the Budapest Convention on Cybercrime](image)

- **Data covered**

- **Subscriber information**

  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.


It is notable that the definition of “subscriber information”, as per Article 18(3) of the Convention, may also include information that under EU law is considered as traffic data. Such data refers to information needed to identify a subscriber of a service which includes certain Internet Protocol (IP) address information, e.g. the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time.
The Budapest Convention On Cybercrime and Cross-border access to Electronic Evidence

Traffic data (Article 1(d))

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.

Content data (Explanatory Report, para. 209)

“Content data” is not defined in the Convention 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 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 depend on the nature and form of the data and the nature of the procedure, as specifically described by each measure provided for in the Convention.⁷

- Types of crimes covered

Aiming to prevent and suppress computer- and computer-related crime and establishing a minimum standard, the Convention provides for the criminalization of a number of types of conduct⁸:

<table>
<thead>
<tr>
<th>Criminal offences committed by means of a computer system</th>
<th>Criminal offences involving evidence in electronic form</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Illegal access (Art.2)</td>
<td>“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 (Art.10)</td>
</tr>
<tr>
<td>- Illegal interception (Art.3)</td>
<td>The Convention does not provide a definition of “electronic evidence”, yet Art. (1)1(a) includes relevant definitions in this respect:</td>
</tr>
<tr>
<td>- Data interference (Art.4)</td>
<td>- “computer system”;</td>
</tr>
<tr>
<td>- System interference (Art.5)</td>
<td>- “computer data”;</td>
</tr>
<tr>
<td>- Misuse of devices (Art.6)</td>
<td>- “traffic data”.</td>
</tr>
<tr>
<td>- Computer-related forgery (Art.7)</td>
<td></td>
</tr>
<tr>
<td>- Computer-related fraud (Art.8)</td>
<td></td>
</tr>
<tr>
<td>- Offences related to child sexual exploitation material (Art.9)</td>
<td></td>
</tr>
<tr>
<td>- Offences related to infringements of copyright and related rights (Art.10)</td>
<td></td>
</tr>
</tbody>
</table>

Fig.4 Types of crimes covered by the Convention

The specific criminal investigations and proceedings covered by the Convention include not only cybercrime, but any criminal offence involving evidence in electronic form. This means that the provisions of the 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. There are two exceptions from this scope of application:

a) The measure of a real-time interception of content data is limited to serious offences, which has to be determined by domestic law.⁹

b) 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 Convention defines service providers as:

---

⁸ As the Convention uses technology-neutral language, the substantive criminal law offences may be applied to both current and future technologies involved.
⁹ Convention, Article 21; Explanatory Report, para. 142.
¹⁰ Convention, Article 20, Explanatory Report, para. 143.
The Budapest Convention On Cybercrime and Cross-border access to Electronic Evidence

B - INTERNATIONAL COOPERATION

As regards the tools for international cooperation, the 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. The Convention includes several international cooperation tools.

- General principles

Section 1 of the International cooperation chapter of the Convention includes provisions setting out general principles concerning:

- 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
- Confidence 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

Some provisions are unique to the Convention, including:

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

---

31 Convention, Article 23.
With regard to expedited preservation and disclosure of data, Article 29 provides that when criminal justice authorities of a country need to preserve data that is stored by means of a computer system located in another Party of the Convention, they are able to request that the competent authorities of the other Party order the expedient preservation of such data. However, there is a requirement to declare that a formal request for assistance in 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 data.

Article 30 refers to previous preservation orders pursuant to Article 29 and only allows 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 currently requested country Party). With regard to trans-border access to data, Article 32 provides the possibility for criminal justice authorities to obtain evidence stored on a computer that is physically located in the territory of another Party. This procedure does not require any formal request for international cooperation, however it is limited to publicly available information (Article 32(a)) and to data obtained with the legal and voluntary consent of the person legally authorized to provide access to that data (Article 32(b)).

With regard to trans-border access to data, Article 32 provides the possibility for criminal justice authorities to obtain evidence stored on a computer that is physically located in the territory of another Party. This procedure does not require any formal request for international cooperation, however it is limited to publicly available information (Article 32(a)) and to data obtained with the legal and voluntary consent of the person legally authorized to provide access to that data (Article 32(b)).

4. CONDITIONS AND SAFEGUARDS

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

- **Purpose limitation**

The procedural measures set out in the Convention are only applicable to specific criminal investigations or proceedings relating to criminal offences established in accordance with Section 1 of the Convention, other criminal offences committed by means of a computer system and the collection of evidence in electronic form pertaining to any criminal offence.

- **Protection of human rights**

Article 15 of the Convention requires Parties to ensure that the powers and procedures established under the 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.

---

12 Explanatory Report, para. 298.
13 Protocol, Article 9(1)(b).
14 Protocol, Article 10(9).
15 Convention, Article 14(1)-(2).
16 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 thereto), other applicable human rights instruments, such as e.g. the 1969...
The Budapest Convention on Cybercrime and Cross-border access to Electronic Evidence

5. The Way Forward

The Budapest Convention on Cybercrime 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 Annex).

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

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

The T-CY facilitates this regular exercise of consultation, as all the Parties to the Convention are members thereof, contributing to the evolution of the Convention. The work of the T-CY in regard to the evolution of the Convention, has recently materialised by the Second Additional Protocol.

Besides the work on the Second Additional Protocol, the T-CY has recently made a number of recommendations concerning trans-border access to data, which has the potential to be considered in a separate protocol to the Convention on Cybercrime. In this regard, the T-CY Transborder Group is operating since 2011 and is tasked to develop an instrument (an amendment to the Convention, a Protocol or Recommendation) to further regulate the transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet and related issues.

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

---

23. T-CY Ad-hoc Subgroup on Transborder Access and Jurisdiction, Transborder access to data and jurisdiction: Options for further action by T-CY, 3 December 2014, pp. 12-14; T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, final report of the T-CY Cloud Evidence Group, 16 September 2016, paras 143-144.
The Budapest Convention On Cybercrime and Cross-border access to Electronic Evidence

experiences and best practices, or negotiation of a binding instrument)\textsuperscript{25}. Furthermore, in light of emerging or critical uses for criminal purposes of the Internet or other technologies (such as ransomware), in May 2022 the T-CY was invited to prepare draft Guidance Notes on “ransomware” and on “the scope of procedural powers and of international cooperation provisions of the Convention”\textsuperscript{26}.

\footnotesize

\textsuperscript{26} https://www.coe.int/en/web/cybercrime/t-cy-plenaries
## ANNEX

### STATES PARTIES TO THE BUDAPEST CONVENTION ON CYBERCRIME AS OF JULY 2022\(^2\)

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