Second Additional Protocol to the 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 signatures 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].

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

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

Since then, information and communication technologies have evolved and transformed societies globally. There has also been a significant increase in the exploitation of technology for criminal purposes [2].

Nowadays the majority of electronic evidence needed in criminal investigations is stored in foreign or unknown jurisdictions. Yet, in many situations, authorities that are investigating a crime may be required to use international cooperation procedures, such as Mutual Legal Assistance (MLA), which are not always able to provide assistance rapidly or effectively enough for the needs of the investigation or proceeding [3].

Under such circumstances, voluntary cooperation by service providers for the disclosure of electronic data is a viable alternative, but it also raises concerns regarding the circumstances in which service providers may respond to direct requests from criminal justice authorities in other Parties [4].

Recognising those challenges, in 2012 the Cybercrime Convention Committee (T-CY) created a working group to consider the issues. Eventually a working group transformed into the Cloud Evidence Group which ultimately recommended negotiation of a Second Additional Protocol to the Budapest Convention on enhanced international cooperation [5].

Accordingly, in June 2017, the T-CY approved the Terms of Reference for the preparation of such a protocol. The negotiations for the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Second Protocol) began in September 2017 [6].

After 4 years and more than 90 meetings, on 17 November 2021, the Committee of Ministers of the Council of Europe adopted the Second Protocol [7], which includes a wide range of provisions, including:

- Standard ones (such as on its purpose, scope of application, effects, territorial application);
- Conditions and safeguards as well as a detailed regime on protection of personal data; and
- Measures for enhanced cooperation of investigatory assistance to obtain the disclosure of domain name registration (Article 6) and subscriber information (Articles 7 and 8), traffic data (Article 8) and content data (Articles 9 and 10); as

[1] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. All EU Member States, except for Ireland.
[2] Explanatory Report, para. 5.
[3] Explanatory Report, para. 91.
[4] Second Protocol, Preamble.
[5] https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07.
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0718&from=EN#.
[7] https://www.coe.int/en/web/portal/-/cybercrime-council-of-europe-strengthens-its-legal-arsenal.

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.

well as provisions on video conferencing (Article 11) and joint investigation teams and joint investigations (Article 12)[8].

The Second Protocol was opened for signature by the Parties to the Budapest Convention in May 2022. It is accompanied by an Explanatory Report which is intended to guide and assist Parties in its application.

2. SCOPE

- **Legal regime covered**

Further to the international legal framework provided by the Budapest Convention, the Second Protocol aims to offer additional measures pertaining to more efficient mutual assistance and other forms of cooperation between competent authorities; cooperation in emergencies; and direct cooperation between competent authorities and service providers and other entities in possession or control of relevant information[9].

The scope of the Second Protocol goes considerably beyond the scope of this review, and includes, as noted above, for example, provisions related to video conferencing (Article 11) and joint investigation teams and joint investigations (Article 12).

- **Data covered**

The Second Protocol uses the same data categorization as the Budapest Convention, dividing data into **three categories** (**subscriber data, traffic data and content data**), which may exists in **two forms** (stored or in the process of communication). The majority of the measures included in the Second Protocol refer to stored data.

It is notable that the definition of "subscriber information", as per Article 18(3) of the Budapest Convention[10], may also include information that under the domestic law of some EU Member States is considered as traffic data.

- **Types of crimes covered**

The measures described in the Second Protocol are applicable to **specific criminal investigations or proceedings** relating to:

- Criminal offences established in accordance with Section 1 of the Budapest Convention and other criminal offences committed by means of a computer system;
- The collection of evidence in electronic form of a criminal offence; and
- Between Parties to the First Protocol, criminal offences established pursuant to the First Protocol[11].

Therefore, the specific criminal investigations and proceedings covered include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that the powers and procedures under the Second Protocol 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[12].

This is also confirmed in Guidance Note #13[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

[8] Explanatory Report, para. 63
[9] Explanatory Report, para. 26.
[10] The term "subscriber information" is defined as 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; or (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
[11] Second Protocol, Article 2(1); Budapest Convention, Article 14(2)(a)-(c).
[12] Explanatory Report, para. 33. See also Explanatory Report to the Budapest Convention, paras 141, 243.
[13] Although not binding, Guidance Notes adopted by the T-CY represent the common understanding of the Parties regarding the use of the Budapest Convention and its protocols, see https://www.coe.int/en/web/cybercrime/guidance-notes.

also to the collection of electronic evidence of any criminal offence. This broad scope also applies to the measures of the [Second Protocol]."

- **Entities covered**

Regarding direct cooperation mechanisms between public authorities and service providers as well as other entities in the territory of another Party in possession or control of pertinent information (Articles 6 and 7), the Second Protocol covers:

- **Service providers** as defined in Article 1 of the Budapest Convention, namely: (a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (b) any other entity that processes or stores computer data on behalf of such communication service or users of such service[14], when these service providers are based in the territory of another Party to the Second Protocol.
- **Entities providing domain name registration services**, including: (a) organisations that sell domain names to the public ("registrars"); and (b) regional or national registry operators, which keep authoritative databases ("registries") of all domain names, registered for a top-level domain and which accept registration requests[15], when these entities are based in the territory of another Party to the Second Protocol.

3. DEFINING THE TOOLBOX

The Second Protocol is based on the principle of cooperation "to the widest extent possible". This requires Parties to provide extensive cooperation and minimize any impediments to the smooth and rapid flow of information and evidence[16].

The provisions concerning direct cooperation with private entities (Articles 6 and 7), the provisions pertaining to enhanced international cooperation between authorities for the disclosure of stored data (Articles 8 and 9), and the provision pertaining to mutual assistance in an emergency (Article 10) apply whether or not there is a mutual assistance treaty or arrangement in force between the requesting and requested Parties[17].

The provisions concerning video conferencing (Article 11) and joint investigation teams and joint investigations (Article 12) apply where there is no mutual assistance treaty or arrangement between the Parties, except as provided for in Article 12(7)[18].

A - ENHANCED DIRECT COOPERATION WITH PROVIDERS AND ENTITIES IN OTHER PARTIES TO THE SECOND PROTOCOL

The Second Protocol introduces two measures for direct cooperation between a competent authority in one Party and entities providing domain name registration services / service providers in another Party to the Second Protocol.

- **Requests for domain name registration information**

Article 6 of the Second Protocol provides a basis for direct cooperation between a competent authority in a Party and entities providing domain name registration[19] services in another Party to the Second Protocol for the disclosure of domain name registration information which is in their possession or control.

[14] Second Protocol, Article 3.
[15] Explanatory Report, para. 75.
[16] Second Protocol, Article 5
[17] Second Protocol, Article 5(2)-(3).
[18] Second Protocol, Article 5(5). Article 12(7) of the Second Protocol states that: "In the absence of an agreement described in paragraphs 1 and 2 [of the article], joint investigations may be undertaken under mutually agreed terms on a case-by-case basis. This paragraph applies whether or not there is a mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the Parties concerned."

[19] Article 6 of the Second Protocol applies to domain name registration information, i.e. information aimed at identifying or contacting the registrant of a specific domain name. This refers to information previously publicly available through so-called WHOIS lookup tools, such as the name, physical address, e-mail address and telephone number of a registrant. Some Parties may consider this information a subset of subscriber information as defined in Article 18(3) of the Budapest Convention (Explanatory Report, para. 81).

A review of Article 6 of the Second Protocol is available in the dedicated SIRIUS Quarterly Review here.

It is notable that requests for the disclosure of domain name registration information under Article 6 are **non-binding**[20].

- **Disclosure of subscriber information**

Article 7 provides a basis for a competent authority in a Party to directly order a service provider in another Party to disclose subscriber information that is within its possession or control.

A review of Article 7 of the Second Protocol is available in the dedicated SIRIUS Quarterly Review here.

Pursuant to Article 7(2)(b), Parties can make a declaration that orders under Article 7 issued towards service providers located within their territory must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision.

Pursuant to Article 7(9), Parties to the Second Protocol may:

1. **Reserve the right not to apply Article 7**. If a Party reserves its right not to apply Article 7, it is not required to take measures under Article 7(2) for service providers in its territory to disclose subscriber information in response to orders issued by other Parties. A Party that makes a reservation to Article 7 is also **not permitted to issue orders** under the article **to service providers in the territory of other Parties**[21].

2. **Reserve the right not to apply Article 7 to the disclosure of certain types of access numbers**, if this would be inconsistent with the fundamental principles of their domestic legal system. A Party that makes such a reservation is also **not permitted to issue orders for such numbers to service providers in the territory of other Parties**[22].

B - EXPEDITED PRODUCTION OF TRAFFIC AND SUBSCRIBER DATA

Article 8 of the Second Protocol provides a basis for enhanced cooperation between authorities for the disclosure of computer data. The purpose of the provision is for a requesting Party to have the ability to issue an order to be submitted as part of a request to another Party and for the requested Party to have the ability to give effect to that order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control[23]. This process is designed to function similarly to mutual assistance but in a more streamlined manner, as the information the requesting Party must provide is more limited and the process for obtaining the data more rapid[24].

Pursuant to Article 8(13), Parties may reserve the right not to apply the article to traffic data.

A Party that makes such reservation will not be allowed to issue orders for traffic data to other Parties under Article 8(1)[25].

C - EMERGENCY ACCESS TO ELECTRONIC EVIDENCE

The Second Protocol defines "emergency" as "a situation in which there is a significant and imminent risk to the life or safety of any natural person"[26].

- **Expedited disclosure of stored computer data in an emergency**

Article 9 of the Second Protocol provides a basis for cooperation between authorities for the disclosure of stored computer data[27] in emergency situations.

[20] Explanatory Report, paras 75, 83
[21] Explanatory Report, para. 122.
[22] Explanatory Report, para. 123.
[23] Explanatory Report, para. 124.
[24] Explanatory Report, para. 125.
[25] Explanatory Report, para. 147.

[26] Second Protocol, Article 3(2)(c).
[27] "Stored computer data" includes any stored or existing subscriber information, traffic data, and content data (Explanatory Report para. 155). The scope of the term is broad and includes any specified computer data, i.e. "any representation of facts, information or concepts in a form

In accordance with this provision, in an emergency, Parties may utilize their respective 24/7 network points of contact established under Article 35 of the Budapest Convention to transmit a request to and receive a request from 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 that service provider's possession or control, without the need to make a request for mutual assistance[28].

It is notable that requests for the expedited disclosure of stored computer data in an emergency **are non-binding**, i.e. the provision does not require requested Parties to provide requested data to requesting Parties[29].

- **Emergency mutual assistance**

Article 10 of the Second Protocol allows Parties to seek expedited MLA when an emergency exists[30]. Once satisfied that an emergency exists and the other requirements for mutual assistance have been fulfilled, the requested Party shall respond to the request on a rapidly expedited basis[31].

In accordance with Article 10(9), Parties may make a declaration that requests under Article 10 may also be sent directly to its judicial authorities; through INTERPOL channels; or through the 24/7 network established under Article 35 of the Budapest Convention[32].

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

4. CONDITIONS AND SAFEGUARDS

A - OVERALL SYSTEM OF SAFEGUARDS

- **Purpose limitation**

In addition to what is noted above (see section Scope), measures under the Second Protocol shall be applied to "specific criminal investigations or proceedings"[33], in particular cases, concerning specific individuals. This excludes, for example, their use for, e.g., crime prevention or intelligence gathering purposes, or for the mass production of data[34].

- **Additional safeguards**

A number of articles of the Second Protocol include important safeguards. For example, individual articles specify information to include in requests, orders and accompanying information that may assist in applying domestic safeguards (for example, Articles 6(9), 7(3)-(4), 8(3) 9(3)). Also, the types of data to be disclosed are specified in each article, for example in Article 7, which is limited to the production of subscriber information. In addition, Parties may make reservations and declarations which may limit the type of information to be provided, such as is the case for Articles 7 and 8[35].

B - ARTICLE 13 OF THE SECOND PROTOCOL: CONDITIONS AND SAFEGUARDS

- **Protection of human rights**

Article 13 of the Second Protocol makes a specific reference to Article 15 of the Budapest Convention and requires Parties to ensure that the powers and procedures established under the Second Protocol 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

suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function" (Budapest Convention, Article 1(b); Second Protocol, Article 3(1)).

[28] Second Protocol, Article 9(1)(a).

[29] Explanatory Report, para. 169.

[30] Explanatory Report, para. 171.

[31] Second Protocol, Article 10(4).

[32] 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.

[33] Second Protocol, Article 2(1).

[34] See, e.g., Explanatory Report, para. 97, in relation to production orders under Article 7 of the Second Protocol.

[35] Explanatory Report, para. 219.

under applicable international human rights instruments[36].

- **Principle of proportionality**

Article 15(1) of the Budapest Convention also requires Parties to apply the principle of proportionality. This will be done in accordance with each Party's relevant domestic law principles. In the case of European countries, these principles will be derived from the European Convention on Human Rights (ECHR) and related jurisprudence, meaning that the powers of competent authorities must be **proportional to the nature and circumstances of the offence**[37]. Other Parties may apply related domestic law principles, such as principles of **relevance** (i.e. the evidence sought must be relevant to the investigation or prosecution), **limitations on overly broad orders**[38] or **exclude their application in cases concerning minor crimes**[39].

- **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 must be addressed under domestic law include the right against self-incrimination, legal privileges, and specificity of individuals or entities subject to the measure[40].

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

In accordance with Article 15(3) of the Budapest Convention, when applying the measures provided for by the Second Protocol, 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 the measure on the rights, responsibilities and legitimate interests of third parties, which may include, for example, protection from liability for disclosure[41].

C - ARTICLE 14 OF THE SECOND PROTOCOL: PROTECTION OF PERSONAL DATA

Article 14 of the Second Protocol provides in its paragraphs 2 to 15 a robust system for data protection. This includes safeguards regarding purpose and use of the data; data quality and integrity; sensitive data; retention of data; automated decision-making; security; records and logging; transparency and notice regarding processing, retention periods, data disclosure, access rectification and redress available; right to access and rectification; judicial and non-judicial remedies; and independent oversight[42]. A Party may also suspend the transfer of personal data to another Party based on substantial evidence of systematic or material breach of Article 14[43].

Pursuant to Article 14(1)(a), each Party shall process personal data that it receives under the Second Protocol in accordance with the specific safeguards set out in Article 14(2)-(15), with two exceptions:

1. If, at the time of transfer of data, both the transferring Party and the receiving Party are bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the

[36] 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 to the Budapest Convention, para. 145).

[37] Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 146.

[38] Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 145.

[39] Explanatory Report to the Budapest Convention, paras 146, 174.

[40] Explanatory Report to the Budapest Convention, para. 147.

[41] Explanatory Report to the Budapest Convention, para. 148.

[42] For more information, see Second Protocol, Article 14(2)-(14) and Explanatory Report, paras 227-281.

[43] Second Protocol, Article 14(15).

transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences (Article 14(1)(b)). This would include, for example, Convention 108+ and the EU-US Umbrella Agreement[44].

2. If the transferring Party and the receiving Party, not bound by an international agreement as described above, nevertheless agree that the transfer of data under the Second Protocol may take place on the basis of other agreements or arrangements between them in lieu of Article 14(2)-(15). For EU Member States, in relation to transfers of personal data to third countries, such an alternative agreement would have to comply with the requirements of EU data protection legislation.

[44] Explanatory Report, para. 222.