www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 27 June 2023 T-CY(2023)6

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #13
The scope of procedural powers and of international co-operation provisions of the Budapest Convention

Adopted by T-CY 28 (27-28 June 2023)

Contact

Alexander Seger		
Executive Secretary Cybercrime Convention Committee	Tel	+33-3-9021-4506
Directorate General of Human Rights and Rule of Law	Fax	+33-3-9021-5650
Council of Europe, Strasbourg, France	Email	alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1] Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the scope of domestic procedural powers and of the international co-operation provisions of the Convention on Cybercrime (ETS 185) as well as of its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (CETS 224).

While the text of the Convention on Cybercrime is rather clear that the procedural powers and the provisions on international co-operation are applicable not only to cybercrime (Articles 2 to 11 of the Convention) but also "other offences committed by means of a computer system"; and "the collection of evidence in electronic form of a criminal offence" (see Article 14.2. b and c. and similarly Articles 23 and 25 of ETS 185), and while this is confirmed again in the Second Additional Protocol to the Convention (see Article 2 of CETS 224), this scope is not always fully understood, and the laws of some countries limit the application of procedural powers or provisions for international co-operation to a set of cybercrimes.

The T-CY decided, therefore, that a Guidance Note, underlining how key procedural and international co-operation provisions could be applied not only to offences against and by means of computer systems but to a range of offences, would be of practical and strategic benefit.

2 Relevant provisions of the Convention on Cybercrime (ETS 185)

2.1 Procedural provisions

Under the Convention on Cybercrime "[e]ach Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to" undertake the procedural measures provided in articles 16 to 21 of the Convention:

- Article 16 – Expedited preservation of stored computer data
- Article 17 – Expedited preservation and partial disclosure of traffic data
- Article 18 – Production order
- Article 19 – Search and seizure of stored computer data
- Article 20 – Real-time collection of traffic data
- Article 21 - Interception of content data

These measures are subject to the conditions and safeguards of Article 15.

The scope of these procedural measures is defined in Article 14:

> Article 14 – Scope of procedural provisions
>
> 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

[1] See the mandate of the T-CY (Article 46 Budapest Convention).

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
   a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
   b other criminal offences committed by means of a computer system; and
   c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
   b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, 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:
      i. is being operated for the benefit of a closed group of users, and
      ii 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. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

According to Article 14.2 of the Convention, therefore, the procedural powers are applicable to the collection of evidence in electronic form of any criminal offence. This "ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in this Section" of the Convention (paragraph 141 Explanatory Report to the Convention).

Paragraph 3 of Article 14 provides for exceptions to this broad scope of application and permits Parties to restrict the scope of more intrusive powers (real-time collection of traffic data under Article 20 and the interception of content data under Article 21).[2]

Therefore, competent authorities may order the preservation of data, order the production of data, search or seize stored computer data, or order or carry out the real-time collection of traffic data or the interception of content data[3] in specific criminal investigations related to any offence under domestic law, including for example:[4]

- corruption;
- counterfeiting of medicines or other threats to public health, including offences related to Covid-19;
- different forms of child abuse;
- different forms of family violence and violence against women;

[2] See reservations and declarations by Parties with regard to Article 14.

[3] As indicated in Articles 20 and 21 of the Convention, restrictions may apply to the powers of real-time collection of traffic data and the interception of content data, such as the limitation to a range of serious offences.

[4] See also the references below to relevant international treaties covering some of these offences.

- different forms of economic and financial crimes;
- drug-related offences;
- fraud;
- kidnapping;
- manipulation of sports competitions;
- money laundering and the financing of terrorism;
- murder;
- organised crime-related offences;
- rape and other forms of sexual violence;
- terrorism;
- genocide, crimes against humanity, war crimes and other international crimes;
- trafficking in human beings;
- xenophobia and racism and other criminal forms of hate speech.

2.2 International co-operation provisions

The broad scope of domestic procedural powers is extended to the principles and measures related to international co-operation (Chapter III of the Convention). Articles 23 and 25 make it clear that co-operation is not only possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, but also for the collection of evidence in electronic form of any criminal offence:

> Article 23 – General principles relating to international co-operation
>
> The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, 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.
>
> Article 25 – General principles relating to mutual assistance
>
> 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose 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.

Paragraph 243 of the Explanatory Report to the Convention confirms that:

> "co-operation is to be extended to all criminal offences related to computer systems and data (i.e. the offences covered by Article 14, paragraph 2, *litterae a-b)*, as well as to the collection of evidence in electronic form of a criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable."

Parties may restrict this broad scope with regard to mutual assistance regarding the real-time collection of traffic data (Article 33) and mutual assistance regarding the interception of content data (Article 34). Furthermore, international co-operation may be subject to conditions, such as

dual criminality requirements,[5] or grounds for refusal in line with Articles 25.4, 27.4 and 27.5[6] of the Convention.

The principles and measures for international co-operation on the offences listed in the Convention and other criminal offences committed by means of a computer system, and the collection of electronic evidence of any other criminal offence are provided in articles 23 to 35[7] of the Convention:

- Article 23 – General principles relating to international co-operation;
- Article 25 – General principles relating to mutual assistance;
- Article 26 – Spontaneous information;
- Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements;
- Article 28 – Confidentiality and limitation on use;
- Article 29 – Expedited preservation of stored computer data;
- Article 30 – Expedited disclosure of preserved traffic data;
- Article 31 – Mutual assistance regarding accessing of stored computer data;
- Article 32 – Trans-border access to stored computer data with consent or where publicly available;
- Article 33 – Mutual assistance in the real-time collection of traffic data;
- Article 34 – Mutual assistance regarding the interception of content data;
- Article 35 – 24/7 network.

Parties to the Convention may make use of these measures and principles to co-operate with each other to the widest extent possible for the purpose of investigations or proceedings and the collection of evidence in electronic form of any criminal offence, and request the preservation of data, access to stored computer data, the real-time collection of traffic data or the interception of content data[8], or to access stored computer data transborder with consent or where publicly available, with regard to any criminal offence and under the conditions stipulated in chapter III of the Convention.

[5] See Article 29.4 of the Convention.
As noted in paragraph 259 of the Explanatory Report to the Convention, "…in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance."

[6] Article 27.5 of the Convention refers to grounds for postponement of action on a request.

[7] Note: The obligation to extradite under "Article 24 – Extradition" applies only "for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty."

[8] As indicated in Articles 20 and 21 of the Convention, restrictions may apply to the powers of real-time collection of traffic data and the interception of content data, such as the limitation to a range of serious offences. Regarding the corresponding Articles 33 and 34 on international co-operation, "Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case" (Article 33.2), and for the interception of content data "The Parties shall provide mutual assistance … to the extent permitted under their applicable treaties and domestic laws" (Article 34).

3 Relevant provisions of the Second Additional Protocol (CETS 224)

On 12 May 2022, the Second Additional Protocol to the Convention on Cybercrime (CETS 224) was opened for signature. Once in force, this instrument will provide Parties to it with additional tools for "enhanced co-operation and disclosure of electronic evidence".

The scope of application of this Protocol is again broad and shall be applied not only to criminal offences related to computer systems and data but also to the collection of evidence in electronic form of any criminal offence:

> Article 2 – Scope of application
>
> 1 Except as otherwise specified herein, the measures described in this Protocol shall be applied:
>
> a as between Parties to the Convention that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, and to the collection of evidence in electronic form of a criminal offence; and
>
> b as between Parties to the First Protocol that are Parties to this Protocol, to specific criminal investigations or proceedings concerning criminal offences established pursuant to the First Protocol.

The measures provided for in this Protocol are:

- Article 6 – Request for domain name registration information directly to an entity in another Party providing domain name registration services;
- Article 7 – Disclosure of subscriber information through direct co-operation with a service provider in another Party;
- Article 8 – Giving effect to orders from another Party for expedited production of subscriber information and traffic data;
- Article 9 – Expedited disclosure of stored computer data in an emergency;
- Article 10 – Emergency mutual assistance;
- Article 11 – Video conferencing;
- Article 12 – Joint investigation teams and joint investigations.

These measures are subject to the conditions and safeguards of Articles 13 and 14 of CETS 224.

Therefore, competent authorities of Parties to this Protocol may – subject to reservations and declarations that are permitted according to Article 19 of CETS 224 – request domain name registration information, order the disclosure of subscriber information, give effect to production orders for subscriber information and traffic data, co-operate in emergencies, make use of video conferencing or set up joint investigation teams or engage in joint investigations related to criminal investigations or proceedings concerning criminal offenses related to computers systems and data, and to the collection of evidence in electronic form of any offence.

4 Synergies between the Convention on Cybercrime and other treaties

The domestic procedural powers and the principles and measures of international co-operation may also be used to collect electronic evidence related to offences foreseen in other international agreements to which States are Parties, subject to any relevant conditions as noted above.[9] Such agreements may include those on corruption;[10] counterfeiting of medicines or other threats to public health[11]; child abuse[12]; domestic violence and violence against women[13]; drug-related offences;[14] manipulation of sports competitions[15]; money laundering and the financing of terrorism[16]; organised crime-related offences;[17] terrorism;[18] trafficking in human beings; [19] or genocide, crimes against humanity, war crimes and other international crimes.[20]

For Parties to the first additional Protocol to the Convention on Cybercrime regarding xenophobia and racism via computer systems (ETS 189),[21] Article 8.2 stipulates that the "Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol".

In 2018, the T-CY recommended that Parties to the Lanzarote Convention on the Sexual Exploitation and Sexual Abuse of Children (CETS 201) and to the Istanbul Convention on Violence against Women and Domestic Violence (CETS 210) be encouraged "to introduce the procedural powers of articles 16 to 21 Budapest Convention into domestic law and to consider becoming Parties to the Budapest Convention to facilitate international co-operation on electronic evidence

---

[9] Such as dual criminality requirements, or grounds for refusal in line with Articles 25.4 and 27.4 of the Convention.

[10] For example, the criminal conduct referred to by the Criminal Law Convention on Corruption (ETS No. 173) of the Council of Europe or the United Nations Convention against Corruption.

[11] For example, the criminal conduct referred to by the Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS No. 211)

[12] For example, the criminal conduct referred to by the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201)

[13] For example, the criminal conduct referred to by the Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210)

[14] For example, the criminal conduct referred to by the United Nations Drug Control Conventions

[15] For example, the criminal conduct referred to by the Council of Europe Convention on the Manipulation of Sports Competitions (CETS No. 215)

[16] For example, the criminal conduct referred to by the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)

[17] For example, the criminal conduct referred to by the United Nations Convention against Transnational Organized Crime and its Protocols.

[18] For example, the criminal conduct referred to by the Council of Europe Convention on the Prevention of Terrorism (CETS No. 196) and its Protocols.

[19] For example, the criminal conduct referred to by the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197)

[20] For example, the conduct referred to by the Convention on the Prevention and Punishment of the Crime of Genocide of 1948, the four Geneva Conventions on International Humanitarian Law and their Additional Protocols of 1949, or the Rome Statute of the International Criminal Court.

[21] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)

(articles 23 to 35 Budapest Convention) in relation to online sexual violence against children and violence against women and family violence".[22]

5 T-CY statement

The T-CY agrees that the procedural law provisions and the principles and measures for international co-operation of the Convention on Cybercrime are applicable not only to offences related to computer systems and data but also to the collection of electronic evidence of any criminal offence. This broad scope also applies to the measures of the Second Additional Protocol to the Convention.

This scope furthermore permits synergies between the Budapest Convention and other international agreements.

[22] See T-CY Mapping Study on Cyberviolence
https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914