www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 30 November 2022 T-CY(2022)16

Cybercrime Convention Committee (T-CY)

Assessing implementation of the Budapest Convention on Cybercrime

Questionnaire on

search and seizure of stored computer data (Article 19)

Adopted by the 27th Plenary of the T-CY
(29-30 November 2022)

T-CY representatives are invited to submit replies in electronic form and in English or French to the T-CY Secretariat at **T-CY.secretariat@coe.int by 1 March 2023**

Background

The Cybercrime Convention Committee (T-CY), at its 26th Plenary Session (10-11 May 2022) decided to assess in its 4th round of assessments pursuant to Article 46 of the Convention and the T-CY Rules of Procedure the implementation by Parties of Article 19 of the Convention on the search and seizure of stored computer data.

Purpose of the Assessment

The purpose of the assessment is to share experience and good practices on the ways Parties have implemented Article 19 (Search and seizure of stored computer data) of the Convention on Cybercrime.

Assessing implementation of Article 19 is of interest for a number of reasons, including:

- Article 19 is an important procedural power under the Convention. Sharing of information and experience on legislative and other measures as well as practices in implementing Article 19 would facilitate further reforms in current and future Parties where necessary.
- The domestic procedure in Article 19.2 – which requires each Party to adopt measures necessary to ensure that when its authorities search or access a computer system in its territory, they are able to expeditiously extend the search or similar accessing to another computer system in its territory under certain conditions – can be linked to the question of extension of searches to other Parties' territories that remains of interest to the T-CY.

Implementation of the assessment

Timelines for this assessment are foreseen as follows:

— December 2022: The T-CY Secretariat will circulate the questionnaire as adopted by the T-CY to T-CY representatives.

— December 2022 – February 2023: T-CY representatives are invited to prepare/compile consolidated replies to this questionnaire in cooperation with the respective authorities of their State.

— By 1 March 2023: T-CY representatives are invited to submit replies in electronic form and in English or French to the T-CY Secretariat at **T-CY.secretariat@coe.int**

— June 2023: The T-CY Bureau will present the compilation of replies received and initial comments to the 28th T-CY Plenary.

— November/December 2023: The T-CY Bureau will present a draft assessment report to the 29th T-CY Plenary. Parties will be invited to present their relevant legal provisions, procedures and practices and to respond to comments made by Bureau members.

— June/July 2024: Final reading of the assessment report in view of adoption by the 30th T-CY Plenary.

_____

1 Information on the legal basis for the search and seizure of stored computer data

Q 1.1.1 Please provide an overview of the legal basis for the search and seizure of stored computer data in your country.

Q 1.1.2 Do the powers for the search and seizure of stored computer data apply only to offences against or by means of computers or also other offences under your domestic law where evidence is on a computer system?[1]

Q 1.1.3 What do you consider to comprise "stored computer data"?[2]

Q 1.1.4 Are there requirements with respect to notification of the exercise of powers under Article 19? If so, please provide a summary (including legislation, court decisions and practices).

Q 1.1.5 Please provide a copy of the relevant statutes of your law (preferably in English or French).

2 Procedures and requirements

2.1 Requirements for search or similar accessing

Article 19.1 provides that:

> 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
>
> a a computer system or part of it and computer data stored therein; and
> b a computer-data storage medium in which computer data may be stored
>
> in its territory.

Q 2.1.1 Please summarise the legislative and other measures your country has undertaken to ensure that authorities can search or similarly access computer systems, data and data-storage mediums in your territory as described in Article 19.1. In answering, please summarise the requirements to be met and the procedural steps typically taken to obtain the authorisation for such a search.

Q 2.1.2 Do particular rules apply in an emergency or other urgent circumstances? If so, please describe those rules and the applicable understanding of what constitutes an emergency.

[1] See Article 14.2.

[2] See the discussion in paragraphs 188 and 190 of the Explanatory Report.

Q 2.1.3 Does your legislation empower your competent authorities to search or similarly access a computer system and data therein using lawfully acquired access credentials? In answering the question please summarise the requirements to be met and the steps typically taken to execute the power.

Q 2.1.4 Does your legislation empower your competent authorities to search or similarly access a computer system and data therein using covert remote access? In answering, please summarise the requirements to be met and the steps typically taken to execute the power.

Q 2.1.5 Which are the competent authorities that authorise and that carry out a search as described in Article 19.1? What type of technical or other expertise is required and utilized?

Q 2.1.6 Have your authorities adopted internal standard operating procedures or similar guidelines for the search as described in Article 19.1? If possible, please provide an overview and any publicly available links.

Q 2.1.7 Please provide examples of relevant court decisions related to evidence obtained by the searches as described in Article 19.1.

2.2 Extending a search to another system

Article 19.2 provides that:

> 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

Q 2.2.1 Please summarise what legislative or other measures have you undertaken to ensure that your authorities are able to extend the search as described in Article 19.2.

Q 2.2.2 Please summarise the procedure (including authorisations required and investigative techniques applied) for extending a search or similar accessing to another system in practice.

Q 2.2.3 Please summarise how your legal framework applies the "grounds to believe" element of Article 19.2, including how competent authorities typically establish that they have "grounds to believe" that the data sought is stored in another computer system or part of it in its territory.

Q 2.2.4 Please summarise how your legal framework applies the "in its territory" element of Article 19.2, including whether or not your framework imposes an affirmative requirement that the connected system be in your territory.[3]

Q 2.2.5 How do you proceed in cases when it cannot be determined where the data sought is stored ("loss of (knowledge of) location situations")?

Q 2.2.6 Please provide typical examples (use cases) for extending a search.

Q 2.2.7 Please provide examples of relevant court decisions related to the extension of a search to a connected computer system.

2.3 Seizure or similarly securing computer data accessed

Article 19.3 provides that:

> 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
>
> a seize or similarly secure a computer system or part of it or a computer-data storage medium;
> b make and retain a copy of those computer data;
> c maintain the integrity of the relevant stored computer data;
> d render inaccessible or remove those computer data in the accessed computer system.

Q 2.3.1 Please summarise what legislative or other measures your country has undertaken to ensure that your authorities are able to seize or similarly secure computer data as described in Article 19.3. In answering, please summarise the requirements to be met and the procedural steps typically taken to obtain the authorisation for such a seizure.

[3] See the discussion in paragraphs 192 and 193 of the Explanatory Report.

Q 2.3.2 Do you apply the same measures when extending a search (according to Article 19.2) and in situations when it cannot be determined where the data sought is stored?

Q 2.3.3 Which are the competent authorities that authorise and that carry out a seizure as described in Article 19.3? What type of technical or other expertise is required and utilized?

Q 2.3.4 Please provide typical examples (use cases) and relevant court decisions.

2.4 Ordering a person to enable the search and seizure of stored computer data

Article 19.4, provides that:

> 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent 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 is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

Q 2.4.1 Please summarise what legislative or other measures your country has undertaken to ensure that your authorities are able to order a person to provide necessary information as described in Article 19.4. Please summarise the rules applicable to this provision.

Q 2.4.2 Please provide typical examples (use cases) and relevant court decisions.

3 Conditions and safeguards

Article 19.5 provides that:

> 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Q 3.1.1 Please summarise the conditions and safeguards that are applicable when applying the different measures for the search, extension of the search, and seizure of stored computer data described above.

Appendix 1: Extracts of the Convention on Cybercrime

Operative text

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent 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 is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Explanatory report

Search and seizure of stored computer data (Article 19)

184. This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data *per se* will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data.

185. In the traditional search environment concerning documents or records, a search involves gathering evidence that has been recorded or registered in the past in tangible form, such as ink on paper. The investigators search or inspect such recorded data, and seize or physically take away the tangible record. The gathering of data takes place during the period of the search and in respect of data that exists at that time. The precondition for obtaining legal authority to undertake a search is the existence of grounds to believe, as prescribed by domestic law and human rights safeguards, that such data exists in a particular location and will afford evidence of a specific criminal offence.

186. With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain. For example, the gathering of the data occurs during the period of the search and in respect of data that exists at that time. The preconditions for obtaining legal authority to undertake a search remain the same. The degree of belief required for obtaining legal authorisation to search is not any different whether the data is in tangible form or in electronic form. Likewise, the belief and the search are in respect of data that already exists and that will afford evidence of a specific offence.

187. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such copies. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.

188. Paragraph 1 requires Parties to empower law enforcement authorities to access and search computer data, which is contained either within a computer system or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or diskette). As the definition of "computer system" in article 1 refers to "any device or a group of inter-connected or related devices", paragraph 1 concerns the search of a computer system and

its related components that can be considered together as forming one distinct computer system (e.g., a PC together with a printer and related storage devices, or a local area network). Sometimes data that is physically stored in another system or storage device can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. This situation, involving linkages with other computer systems by means of telecommunication networks within the same territory (e.g., wide area network or Internet), is addressed at paragraph 2.

189. Although search and seizure of a "computer-data storage medium in which computer data may be stored" (paragraph 1 (b)) may be undertaken by use of traditional search powers, often the execution of a computer search requires both the search of the computer system and any related computer-data storage medium (e.g., diskettes) in the immediate vicinity of the computer system. Due to this relationship, a comprehensive legal authority is provided in paragraph 1 to encompass both situations.

190. Article 19 applies to stored computer data. In this respect, the question arises whether an unopened e-mail message waiting in the mailbox of an ISP until the addressee will download it to his or her computer system, has to be considered as stored computer data or as data in transfer. Under the law of some Parties, that e-mail message is part of a communication and therefore its content can only be obtained by applying the power of interception, whereas other legal systems consider such message as stored data to which article 19 applies. Therefore, Parties should review their laws with respect to this issue to determine what is appropriate within their domestic legal systems.

191. Reference is made to the term 'search or similarly access'. The use of the traditional word 'search' conveys the idea of the exercise of coercive power by the State, and indicates that the power referred to in this article is analogous to traditional search. 'Search' means to seek, read, inspect or review data. It includes the notions of searching for data and searching of (examining) data. On the other hand, the word 'access' has a neutral meaning, but it reflects more accurately computer terminology. Both terms are used in order to marry the traditional concepts with modern terminology.

192. The reference to 'in its territory' is a reminder that this provision, as all the articles in this Section, concern only measures that are required to be taken at the national level.

193. Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'.

194. The Convention does not prescribe how an extension of a search is to be permitted or undertaken. This is left to domestic law. Some examples of possible conditions are: empowering the judicial or other authority which authorised the computer search of a specific computer system, to authorise the extension of the search or similar access to a connected system if he or she has grounds to believe (to the degree required by national law and human rights safeguards) that the connected computer system may contain the specific data that is being sought; 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 is stored in the other computer system; or exercising search or similar access powers at both locations in a co-ordinated and expeditious manner. In all cases the data to be searched must be lawfully accessible from or available to the initial computer system.

195. This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation.

196. Paragraph 3 addresses the issues of empowering competent authorities to seize or similarly secure computer data that has been searched or similarly accessed under paragraphs 1 or 2. This includes the power of seizure of computer hardware and computer-data storage media. In certain cases, for instance when data is stored in unique operating systems such that it cannot be copied, it is unavoidable that the data carrier as a whole has to be seized. This may also be necessary when the data carrier has to be examined in order to retrieve from it older data which was overwritten but which has, nevertheless, left traces on the data carrier.

197. In this Convention, 'seize' means to take away the physical medium upon which data or information is recorded, or to make and retain a copy of such data or information. 'Seize' includes the use or seizure of programmes needed to access the data being seized. As well as using the traditional term 'seize', the term 'similarly secure' is included to reflect other means by which intangible data is removed, rendered inaccessible or its control is otherwise taken over in the computer environment. Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data.

198. The rendering inaccessible of data can include encrypting the data or otherwise technologically denying anyone access to that data. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography. The term 'removal' is intended to express the idea that while the data is removed or rendered inaccessible, it is not destroyed, but continues to exist. The suspect is temporarily deprived of the data, but it can be returned following the outcome of the criminal investigation or proceedings.

199. Thus, seize or similarly secure data has two functions: 1) to gather evidence, such as by copying the data, or 2) to confiscate data, such as by copying the data and subsequently rendering the original version of the data inaccessible or by removing it. The seizure does not imply a final deletion of the seized data.

200. Paragraph 4 introduces a coercive measure to facilitate the search and seizure of computer data. It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision, therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.

201. This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.

202. The information that can be ordered to be provided is that which is necessary to enable the undertaking of the search and seizure, or the similarly accessing or securing. The provision of this information, however, is restricted to that which is "reasonable". In some circumstances, reasonable provision may include disclosing a password or other security measure to the

investigating authorities. However, in other circumstances, this may not be reasonable; for example, where the disclosure of the password or other security measure would unreasonably threaten the privacy of other users or other data that is not authorised to be searched. In such case, the provision of the "necessary information" could be the disclosure, in a form that is intelligible and readable, of the actual data that is being sought by the competent authorities.

203. Under paragraph 5 of this article, the measures are subject to conditions and safeguards provided for under domestic law on the basis of Article 15 of this Convention. Such conditions may include provisions relating to the engagement and financial compensation of witnesses and experts.

204. The drafters discussed further in the frame of paragraph 5 if interested parties should be notified of the undertaking of a search procedure In the on-line world it may be less apparent that data has been searched and seized (copied) than that a seizure in the off-line world took place, where seized objects will be physically missing. The laws of some Parties do not provide for an obligation to notify in the case of a traditional search. For the Convention to require notification in respect of a computer search would create a discrepancy in the laws of these Parties. On the other hand, some Parties may consider notification as an essential feature of the measure, in order to maintain the distinction between computer search of stored data (which is generally not intended to be a surreptitious measure) and interception of flowing data (which is a surreptitious measure, see Articles 20 and 21). The issue of notification, therefore, is left to be determined by domestic law. If Parties consider a system of mandatory notification of persons concerned, it should be borne in mind that such notification may prejudice the investigation. If such a risk exists, postponement of the notification should be considered.