www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, version 9 April 2013 T-CY (2013)14

Cybercrime Convention Committee (T-CY)

(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data

Proposal prepared by the Ad-hoc Subgroup on Transborder Access

Contact

Alexander Seger
Secretary Cybercrime Convention Committee
Head of Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

In November 2011, the Cybercrime Convention Committee (T-CY) decided to establish the "ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows" (hereinafter, the "Transborder Group") with a view of developing an instrument "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".

The report prepared by the Transborder Group proposes three solutions that should be pursued in parallel:

1. More effective use of the Budapest Convention in its current form, in particular with regard to its international cooperation provisions.
2. The preparation of a Guidance Note on Article 32 (transborder access to data) "to facilitate implementation of the Budapest Convention by the Parties, to correct misunderstandings regarding transborder access under this treaty, and to reassure third parties", in consultation with private sector entities.
3. The preparation of an Additional Protocol to the Budapest Convention on Cybercrime to allow for additional possibilities for transborder access to data.

The T-CY, at its 8th Plenary (December 2012) decided

– To adopt the report of the T-CY Sub-group on Transborder Access and to make it public.

– To extend the mandate of the T-CY Sub-group on Transborder Access and Jurisdiction to 31 December 2013 with the following tasks:

  - Preparation of a Guidance Note on Article 32 Budapest Convention, including a consultation of private sector entities. A draft should be prepared for discussion at the 9th Plenary of the T-CY in mid-2013 and a hearing of private sector entities could be held on that occasion. The Guidance Note should then be submitted for adoption to the 10th Plenary before 31 December 2013.
  - Submission by June 2013 for approval by the T-CY of a draft Mandate of the Committee of Ministers tasking the T-CY to prepare an Additional Protocol, as well as submission of elements regarding the possible contents and scope such a Protocol.
  - Pending the mandate of the Committee of Ministers, preparation of a first draft text of a possible Protocol for discussion by the 10th Plenary of the T-CY (scheduled for December 2013).

The present Note comprises the elements regarding the possible contents and scope such a Protocol for further discussion by the 9th Plenary of the T-CY (4-5 June 2013).

It is also intended to facilitate the public Hearing on transborder access on 3 June 2013.

2 Options regarding transborder access beyond 32b: possible elements of a Protocol

Already at the time when the principle of transborder access with consent was negotiated by the G8 and the Council of Europe, different other options were discussed covering situations of transborder access without consent or situations where the location of data or systems accessed was not known. The latter point gained in relevance more recently with the growing importance of cloud computing along with the "loss of location".

Some proposals are summarized here to provide food for thought and elements to construct solutions in addition to Article 32b. They do not exclude other options.

These options (Protocol) would apply to specific criminal investigations and proceedings within the scope of Article 14.[1]

Proposal 1: Transborder access with consent without the limitation to data stored "in another Party"

Additional provisions may be needed to cover situations where consent is given under conditions similar to those of Article 32b but where it is unclear where the data are located or where data are moving.[2]

Note: With respect to this option, additional safeguards may be required such as post factum notification once the location becomes known.

Proposals have furthermore been made to broaden the scope to allow for access to data located in non-Parties.

---

[1] 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.

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.

[2] As noted earlier in this report, Article 32b in its present form only applies to situations where data is stored in another Party.

Note: This option may raise concerns of international law. Article 34 of the Vienna Convention on the Law of Treaties[3] does not allow a treaty to create obligations or rights for a third State without its consent.

Proposal 2: Transborder access without consent but with lawfully obtained credentials

Under this proposal, an Additional Protocol would contain a new provision

> permitting a Party, without the authorisation of another Party to access or receive, during a criminal investigation or trial, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the credentials by lawful investigative activities. The investigating Party would be obliged to notify the other Party, prior, during or after acquiring the data.

If this option is pursued, the question arises as to whether such access is then limited to data known to be located in another Party (see above).

Proposal 3: Transborder access without consent in good faith or in exigent or other circumstances

Under this proposal, a new provision could be added to the Budapest Convention permitting transborder access in specific situations to prevent imminent danger, physical harm, the escape of a suspect or similar. Situations may also comprise the risk of destruction of relevant evidence. Again, specific criteria and safeguards as well as notification of the other Party would need to be defined.

A new provision may also need to cover "good faith" situations, where during a search, LEA may not know (for sure) that the system searched is located on a foreign territory, or may not know on which territory, or may have obtained evidence from a foreign territory by mistake or accident.

Note: Such an option could go beyond other Parties.

Proposal 4: Extending a search without the limitation "in its territory" in Article 19.3

Article 19.2 Budapest Convention, requires Parties to authorise an extension of a search to connected computer systems, however, with the limitation "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[4], 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.

It may be conceivable to drop this limitation.

---

[3] http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf

[4] Emphasis added.

Note: Dropping this limitation may only be possible as long as the data is in a Party and/or in an unknown location. Specific criteria as well as safeguards would need to be defined, such as notification, if the location is known to be in a non-Party.

Proposal 5: The power of disposal as connecting legal factor[5]

The "loss of location" has been used as a term to denote situations where it is very difficult if not impossible to link data to a specific location. Data are "somewhere in the clouds", they may move between different servers and locations, or be split over different locations or be dynamically composed from subsets of data from different locations, or mirrored and cached and thus be available in different locations at the same time, or a person may be "in roaming" when data is accessed or intercepted. In the context of cloud computing, an individual person seems most often not aware where his or her data are located at a given moment.

If data cannot be clearly linked to a specific location or territory, it is problematic to rely on the principle of territoriality to determine the jurisdiction to enforce a search or seizure of electronic evidence. It has been argued, therefore, that an approach beyond territoriality was required. A connecting legal factor that provides an alternative to territoriality could be the "power of disposal". Even if the location of data cannot be clearly determined, data can be connected to a person having the power to "alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever".

It has been suggested that if the location of the data is not known, but the person having the power of disposal of the data is physically on the territory of, or a national of the searching Party, the LEA of this Party may be able search or otherwise access the data.

However, a number of safeguards would need to be established and specific criteria would need to apply. It has also been proposed to limit such access to scenarios where access credentials have been lawfully obtained by LEA of the searching Party, and thus avoid "hacking" by LEA into computer systems located in other Parties.

---

[5] Spoenle, Jan (2010): "Cloud computing and cybercrime investigations: territoriality vs the power of disposal", discussion paper, Project on Cybercrime, Council of Europe, Strasbourg.
See also Samson, Gareth (2008) about the problem of "location" in cyberspace.