www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 5 November 2013 T-CY (2013)30

Cybercrime Convention Committee (T-CY)

Ad-hoc Subgroup on Transborder Access and Jurisdiction

Report of the Transborder Group for 2013

Report prepared by the Subgroup

Contents

Contact

Alexander Seger
Secretary of the Cybercrime Convention Committee (T-CY)
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

The Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows" (hereinafter, the "Transborder Group") was established by the Cybercrime Convention Committee (T-CY), at the 6th plenary session (23-24 November 2011).

The terms of reference adopted by the T-CY tasked the Transborder Group to:

> develop an instrument – such as 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, and to present a report containing its findings to the Committee.

The Transborder Group submitted a full report on "Transborder access to data and jurisdiction: what are the options?"[1] to the 8th T-CY Plenary which adopted the report on 6 December 2012.

The report underlined the need for transborder access, but also points at concerns and risks (legal and policy concerns, risks to procedural safeguards, implications for third parties, risks to the protection of personal data, risks to law enforcement operations) that would need to be addressed should possibilities for transborder access be enhanced, and lists a range of practices already applied some of which are going beyond the limited possibilities foreseen in the Convention on Cybercrime.

The report proposed three solutions:

1. More effective use of the Budapest Convention, in particular its provisions on international cooperation.
2. A T-CY Guidance Note on Article 32.
3. An additional Protocol to the Convention on Cybercrime on access to electronic evidence.

The 8th Plenary of T-CY extended the Terms of Reference of the Transborder Group to 31 December 2013 in order: [2]

- To prepare a Guidance Note on Article 32, including a consultation of private sector entities;
- To submit a draft Mandate for the preparation of a Protocol;
- To prepare a first draft text of a possible Protocol for discussion by the 10th Plenary in December 2013.

The present report summarises the work undertaken by the Transborder Group in 2013 and contains proposals on next steps.

[1] See Appendix for a Summary and Findings. For the full report see: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

[2] Members of the Transborder Group in 2012 included: Ioana Albani (Romania), Andrea Candrian (Switzerland), Markko Kunnapu (Estonia), Erik Planken (Netherlands), Betty Shave (USA), Branko Stamenkovic (Serbia) and Pedro Verdelho (Portugal). In 2013, Tsuyoshi Kitagawa (Japan), Cristina Schulman (Romania) and Justin Millar (United Kingdom) also joined.

2 Activities in 2013

2.1 List of activities of the Transborder Group

The Transborder Group in 2013 carried out the following activities:

6-7 February 2013, Strasbourg	Meeting of the Transborder Group
31 May – 2 June 2013, Klingenthal	Meeting of the Transborder Group
3 June 2013, Strasbourg	Public hearing
4-5 June 2013, Strasbourg	T-CY Plenary
1-2 October 2013, Strasbourg	Meeting of the Transborder Group
4 November 2013	Telephone conference

2.2 Elements of a Protocol

The Transborder Group reviewed the situations that a Protocol to the Budapest Convention could possibly cover:[3]

- transborder access with consent but without the limitation to data stored "in another Party";
- transborder access without consent but with lawfully obtained credentials;
- transborder access without consent in good faith or in exigent or other circumstances;
- extending a search from the original computer to connected systems without the limitation "in its territory";
- the power of disposal as connecting legal factor.

The Transborder Group reiterates the statement already made in paragraphs 309 and 310 of the detailed report as adopted in December 2012 (T-CY(2012)3):

> 309 It will be essential to establish safeguards and conditions to protect the rights of individuals and prevent misuse.
>
> 310 The fact that LEA of many States are already engaged in transborder access to data beyond the scope of the Budapest Convention on an uncertain legal basis, with risks to the procedural and privacy rights of individuals, and with concerns regarding national sovereignty would justify the difficult process of negotiating a binding international legal instrument. Or conversely, without such an instrument risks may increase.

2.3 Public hearing (3 June 2013)

On 3 June 2013, at the Council of Europe in Strasbourg, a hearing was organised in which 35 representatives of private sector and civil society organisations and academia as well as 55 members and observer States and organisations of the T-CY participated.[4] A number of written contributions had been received prior to the hearing.[5]

[3] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)14transb_elements_protocol_V2.pdf
[4] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/PublicHearing_LOP.pdf
[5] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY(2013)PublicHearing_Written_contributions.pdf

The hearing showed the complexity of the matter, with some participants rejecting any possibility for transborder access to data altogether, and with others underlining the need for common solutions taking account of technological changes, the evolution of cybercrime and of the need for clearer international rules to frame practices that are widespread already.

The hearing was to help identify solutions to transborder access to data while at the same time addressing concerns, such as the procedural rights of individuals and the protection of personal data. The hearing provided useful insights, for example, regarding limitations to voluntary consent by service providers to disclose data.

However, the hearing also showed that a better understanding is required by the law enforcement community of data protection requirements, and by the data protection community regarding the realities of cyber- and physical crime, the related electronic evidence and lawful measures already undertaken in many States. It is also to be considered that the data protection frameworks affecting a large number of Parties are still evolving at the level of the Council of Europe and the European Union.

2.4 Guidance Note on Article 32

The detailed report on transborder access adopted in December 2012 (T-CY(2012)3), in its appendix, already contained elements of a Guidance Note on Article 32.

The Transborder Group, in February 2013 prepared a draft Guidance Note[6] for discussion in the public hearing and the 9th Plenary of the T-CY in June 2013.

In October 2013, the Transborder Group then prepared a revised version of a draft Guidance Note (see Appendix).

This draft, among other things,

- underlines that Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention;
- notes that service providers would normally not be able to consent validly and voluntarily to the disclosure of users's data under Article 32b;
- states that LEA must not use Article 32b to take measures that would not be permitted under their domestic law;
- suggests that Parties consider notifying relevant authorities of the searched Party; this is proposed as an additional safeguard to protect the rights of individuals and the interests of third parties.

2.5 T-CY decision on a draft Protocol

The T-CY, at its 9th Plenary (4-5 June 2013) decided to commence work on a draft 2nd Additional Protocol and adopted terms of reference covering the period 1 January 2014 to 31 December 2015.[7]

---

[6] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_7E_GN3_transborder_V2public.pdf

[7] See Appendix 3.3 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)22_PlenAbrMeetRep_V9.pdf

3 Conclusions and next steps

With the report on "Transborder access and jurisdiction: what are the options" (T-CY(2012)3) adopted by the T-CY in December 2012, with the activities of the Transborder Group in 2013, including the public hearing and the work on the draft Guidance Note on Article 32, and with the decision of the T-CY on 5 June 2013 to launch the preparation of a draft Protocol in 2014, good progress has been made with respect to a challenge that has been under considered "urgent" for some 25 years. A number of issues have been clarified.

The activities undertaken in 2012/13 have shown that the need for solutions has become more pressing. While criminals exploit the borderless nature of information and communication technologies, criminal justice authorities appear to be less and less able to meet their positive obligations to protect people against crime. This further weakens the rule of law in cyberspace.

The need for solutions thus remains pressing. Nevertheless, the Transborder Group recommends that the T-CY allows for more reflection and dialogue in 2014 with relevant stakeholders, including the private sector and data protection authorities for the following reasons:

- Solutions regarding transborder access to data must be accompanied by safeguards and conditions to protect the rights of individuals and prevent misuse. Reconciling transborder access to data with such safeguards is a complex matter. The public hearing on 3 June 2013 shows that further reflection may be required, including via continuing the dialogue with data protection authorities, civil society and private sector organisations initiated by the Transborder Group in spring 2013.

- The Budapest Convention is a criminal justice treaty covering specified criminal investigations and proceedings regarding cybercrime and electronic evidence within the scope of Article 14. It is not a treaty covering activities of national security agencies. Nevertheless, the current context is complex and could adversely affect the negotiation of a Protocol. This, in turn would entail that many crimes remain unpunished and that governments may not be able to meet their positive obligation to protect individuals against cybercrime.

- The T-CY is currently assessing Article 31 on mutual assistance and related articles on international cooperation. It is not excluded that this may lead to additional proposals to be reflected in a Protocol to the Budapest Convention.

In the light of this, the Transborder Group recommends to the T-CY Plenary to allow for further reflection and dialogue with relevant stakeholders and to take into account the results of the current round of T-CY assessments.

This time could then also be used for further discussion of the draft Guidance Note on Article 32. The actual negotiation of a draft Protocol is to commence only after a report on the above-mentioned activities has been delivered by the Transborder Group and discussed by the T-CY.

4 Appendix

4.1 Extracts from the Report of the Transborder Group (December 2012)[8]

7 Summary and findings

281 The Cybercrime Convention Committee (T-CY) established the "ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows" (hereinafter, the "Transborder Group") at its 6th Plenary in November 2011 with a mandate expiring on 31 December 2012.

282 The Transborder Group was tasked to:

> develop an instrument – such as 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, and to present a report containing its findings to the Committee.

283 The Transborder Group was to examine in particular the use of Article 32b of the Convention, actual practices of transborder investigative measures and the challenges to transborder investigations under international law on jurisdiction and state sovereignty. The present report reflects the findings of the Transborder Group resulting from its work between January and November 2012.

284 The Transborder Group is of the view that two options could be pursued in parallel, namely, the preparation of a T-CY Guidance Note on Article 32 and of an Additional Protocol on access to data. Before proceeding further, the Transborder Group would require confirmation from the T-CY Plenary that these options should indeed be pursued. Subject to such confirmation, it is proposed that the mandate of the Transborder Group be extended to 31 December 2013.

285 The findings of the present report can be summarised as follows:

Need for transborder access

286 The increasing reliance of societies on ICT is accompanied by increasing offences against and by means of computer systems. Cybercrime violates the rights of individuals and, therefore, governments have the positive obligation to protect society against crime, among other things, through effective law enforcement.

287 A primary goal of law enforcement is to secure evidence. In relation to cybercrime but also many other types of crime, this takes the form of electronic evidence. Electronic evidence is volatile and may be stored in multiple jurisdictions. While the primary means to secure electronic evidence stored in another State is mutual legal assistance, unilateral access to data may also be necessary in certain situations.

288 The question of unilateral access by law enforcement authorities of one State to data stored on a computer system in a foreign State without the need for mutual legal assistance has been under discussion since the 1980s. From the mid-1990s, this question was considered a matter of urgency. With the G8 Principles on "transborder access to stored data not requiring legal

[8] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

assistance" adopted by Ministers of Interior and Justice in Moscow, Russian Federation, in 1999, and the inclusion in 2001 of – the very similar – Article 32 in the Budapest Convention on Cybercrime, an agreement was reached on transborder access under very limited circumstances.

289 In recent years, the need for transborder access has become more pressing in view of:

- the number, complexity and impact of transnational cybercrime
- the increasing relevance of electronic evidence in relation any crime
- the volume of data and devices, of the type of services offered, and of offenders and victims in multiple jurisdictions
- the increasing volatility of data and electronic evidence
- the use of cloud computing and web-based services
- the "loss of location", that is, the difficulty of linking data – and thus electronic evidence – to a specific territory or jurisdiction.

Concerns

290 A number of concerns would need to be addressed should possibilities for transborder access be enhanced. These include:

- Legal and policy concerns for States, including dual criminality or refusal to cooperate if this were contrary to public order. Such principles are addressed under mutual legal assistance regimes but not necessarily in situations of unilateral transborder access
- Procedural safeguards protecting the rights of individuals in the State where investigations take place. The rights of individuals would also need to be protected in situations of transborder access
- Implications for third parties, in particular service providers who may be subject to conflicting requests from different States
- Risks to the protection of personal data. Service providers and other private sector entities may violate data protection rules of one State if they disclose data to the authorities of another State[9]
- Risks to law enforcement operations and judicial proceedings that may be compromised through transborder access.

291 Therefore, in order to establish the trust necessary between Parties to agree to enhanced transborder access this would need to be accompanied by safeguards and procedures to protect the rights of individuals and third parties, and the legitimate interests of other States. Conditions need to be put in place to prevent the misuse of such powers.

Current provisions of the Budapest Convention

292 Under the Budapest Convention, the primary means to obtain electronic evidence stored in foreign jurisdiction is through mutual legal assistance, or more precisely, through a combination of provisional measures to secure volatile evidence (Articles 29 and 30 on expedited preservation and Article 35 on 24/7 points of contact) and formal requests to obtain such evidence (in particular under Article 31).[10]

[9] It should be noted that data protection rules are currently being changed by the Council of Europe as well as by the European Union. Further work on transborder access will need to take these developments into account.
[10] It would seem that the potential of these provisions is yet to be fully exploited. The T-CY, in November 2011, decided to assess the implementation of the expedited preservation Articles 16, 17, 29 and 30 in 2012, and to undertake an assessment of the international cooperation provisions (in particular Article 31) in 2013.

293 Article 32 is the most relevant provision with regard to unilateral transborder access to data. Transborder access to publicly available data (Article 32a) may be considered accepted international practice and part of international customary law even beyond the Parties to the Budapest Convention.

294 Article 32b is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances. This provision has been formulated in a manner to allow for different and complex scenarios between the Parties and for data located on systems in the territory of a Party.

295 The Transborder Group is of the opinion that there is no need to amend Article 32 in its present form. However, as this provision is often misunderstood, the T-CY may wish to provide further guidance to Parties with respect to questions such as the meaning of "consent", the laws that apply with respect to "lawful consent" and "lawfully authorised", the person who can provide access or disclose data, or the location of a person disclosing data or providing access.

296 Article 19.2 (search and seizure) is to enable LEA to extend a lawful search or access from the original system to a connected system if there is reason to believe that data is stored on that system in its "territory". While under the Budapest Convention this has been designed as a domestic measure, in the context of cloud computing it is often not obvious whether the connected system is indeed on the territory of the LEA. In practice, it would seem that the measure is often applied, therefore, without the territorial limitation.

297 Article 22 establishes general and rather broad principles of jurisdiction. Territoriality is the primary principle, but the flag and nationality principles are also referred to and, furthermore, the Budapest Convention "does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law" (Article 22.1d). Thus, it would seem that Article 22 would not stand in the way of additional solutions.

298 While the principle of territoriality will remain predominant, in particular with respect to jurisdiction to enforce, the applicability of this principle in "cyberspace" – where data are moving between, are fragmented over, are dynamically composed from, or are mirrored on servers in multiple jurisdictions – is in doubt. It is not possible to apply the principle of territoriality if the location of data is uncertain.

299 Article 32 has been termed an exception to the principle of territoriality as it provides for jurisdiction to enforce on a foreign territory, that is, to access data that is technically stored in the territory of another Party.

300 The drafters of the Budapest Convention did not consider Article 32 the ultimate solution and noted that situations beyond Article 32 were "neither authorised, nor precluded" and that additional solutions may be agreed upon at a later stage.[11]

[11] Budapest Convention Explanatory Report, paragraph 293.

Practices[12]

301 Information available suggests that increasingly, LEA access data stored on computers in other States in order to secure electronic evidence. Such practices may go beyond the limited possibilities foreseen in Article 32b (transborder access with consent) and the Budapest Convention in general:

- Article 32b is not a measure that is used very often by LEA to access themselves data stored in another Party. It may be used more frequently to obtain access to or the disclosure of data owned by service providers or other private sector entities, such as traffic data or subscriber information, but usually not content data of users or customers. It is not always clear whether this is considered a transborder measure in the meaning of Article 32b or considered a domestic request for data if the private sector entity is delivering a service in the State of the investigating LEA.

- Direct LEA access may consist of extending a search from the original system that is lawfully searched to a connected system. In a sense, Article 19.2 is applied without the limitation of "in its territory".

- Often, transborder access is not deliberate; LEA may act in good faith and may not know or know for sure that they are searching data stored on a system abroad or precisely in which jurisdiction the data is stored.

- In some States and depending on the specific situation, once LEA know for sure that they are searching data stored on a foreign territory, they need to discontinue the search, or are only allowed to retain a copy of the data or are required to notify the other State.

- In States allowing for transborder access, only less intrusive investigative techniques are permitted such as access with consent or with lawfully obtained access credentials, or retaining a copy of evidence while more intrusive techniques such as "hacking" an account or system, installation of key loggers for continued surveillance, removing data or disabling a system may not be permitted or only in limited circumstances.

- Increasingly, access to data stored in foreign jurisdictions, is obtained via service providers or other private sector entities either by voluntary consent or judicial orders.

- Private sector entities operating in multiple jurisdictions may be subjected to conflicting requirements; compliance with a lawful request in one State may entail a violation of privacy and other laws in another State.

- Transborder access to data and the use of evidence thus obtained for use in criminal proceedings is normally subject to conditions and safeguards established by the investigating State.

[12] The Transborder Group only analysed access to data for criminal justice purposes. These observations are related to criminal investigations and do not cover situations of direct transborder access by public authorities or access to data via private sector entities stored abroad for intelligence or national security purposes.

302 Overall, practices, procedures as well as conditions and safeguards vary considerably between different States. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdictions or "in the clouds" as well as national sovereignty persist and need to be addressed.

Solutions proposed

More effective use of the Budapest Convention

303 The Budapest Convention is an international treaty that reflects an agreement between the Parties on how to cooperate with each other. It is already in place and the number of Parties is increasing. The Convention in its present form addresses many law enforcement needs in relation to cybercrime and electronic evidence. It enables Governments to meet their positive obligation to protect people and their rights. With regard to international cooperation it combines formal mutual assistance with expedited provisional measures to secure electronic evidence. The potential of this treaty has not yet been fully exploited by all Parties.

304 Parties should make effective use of the Budapest Convention on Cybercrime, in particular its provisions on international cooperation. Parties are invited to participate in the assessments of relevant Articles by the Cybercrime Convention Committee (T-CY) and to follow up on the recommendations made. Additional States are encouraged to accede to the Budapest Convention.

T-CY Guidance Note on Article 32

305 The T-CY should prepare a Guidance Note on Article 32b to facilitate implementation of the Budapest Convention by the Parties, to correct misunderstandings regarding transborder access under this treaty, and to reassure third parties.

306 Article 32b increasingly involves the cooperation of private sector entities. It will be necessary, therefore, to consult private sector entities and data protection experts in the preparation of such a Guidance Note.

Additional Protocol on access to electronic evidence

307 While priority should be given to the effective implementation of the Budapest Convention in its current form and while Guidance Notes by the T-CY should represent a pragmatic way to facilitate implementation, additional measures may need to be envisaged, covering in particular situations where data is moving between or stored in multiple jurisdiction or where the physical location of the data is not known. Such measures could be reflected in an Additional Protocol to the Budapest Convention.

308 An Additional Protocol may address situations between Parties to such an instrument such as:

- transborder access with consent but without the limitation to data stored "in another Party"
- transborder access without consent but with lawfully obtained credentials
- transborder access without consent in good faith or in exigent or other circumstances
- extending a search from the original computer to connected systems without the limitation "in its territory"
- the power of disposal as connecting legal factor.

309 It will be essential to establish safeguards and conditions to protect the rights of individuals and prevent misuse.

310 The fact that LEA of many States are already engaged in transborder access to data beyond the scope of the Budapest Convention on an uncertain legal basis, with risks to the procedural and privacy rights of individuals, and with concerns regarding national sovereignty would justify the difficult process of negotiating a binding international legal instrument. Or conversely, without such an instrument risks may increase.

Next steps

311 The T-CY adopted the present report at its 8th Plenary (5-6 December 2012) and agreed to make it public.

312 It decided to extend the Terms of Reference of the Transborder Group 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. The Group should at that point provide further elements regarding the possible content and scope of such a Protocol.

- Pending the Mandate by the Committee of Ministers, preparation of a first draft text of a possible Protocol for discussion by the 10th Plenary of the T-CY before 31 December 2013.

313 The T-CY decided to invite Japan to provide an expert to join the Transborder Group, and to open up the work of the Group to representatives of other Parties to the Convention who may wish to participate in its meetings. Additional experts may be invited case by case.

4.2 Draft Guidance Note on Article 32

See Document T-CY(2013)7 (version of 5 November 2013)