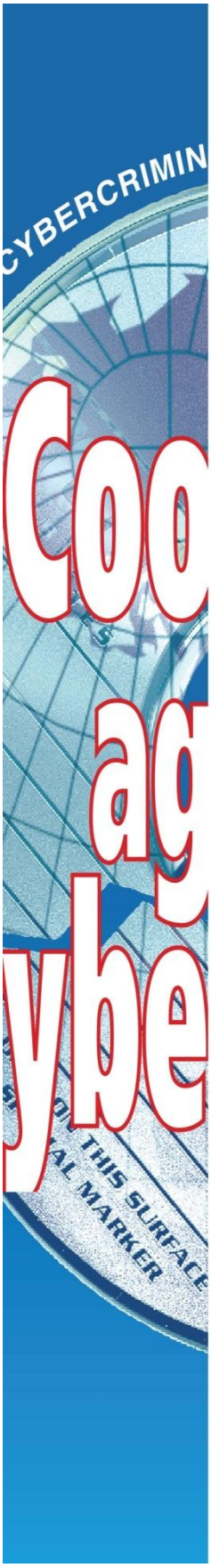


**Cybercrime Convention Committee (T-CY)**

**Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data**

# Transborder access and jurisdiction: What are the options?

Report of the Transborder Group
adopted by the T-CY on 6 December 2012

T-CY (2012)3
Strasbourg, 6 December 2012 (provisional)

**www.coe.int/TCY**

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

## 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

1 The Cybercrime Convention Committee (T-CY), at the 6th plenary session (23-24 November 2011) decided to establish an "ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows"[1] (hereinafter, the "Transborder Group"). This decision was taken on the basis of Article 46.1.a and c of the Budapest Convention on Cybercrime, which stipulates that the Parties[2] shall "consult periodically with a view to facilitating […] the effective use and implementation of the Convention" and "consideration of possible supplementation or amendment of the Convention".[3] 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.

2 It was to examine in particular:

i. the use of Article 32b, of the Convention on Cybercrime;
ii. the use of transborder investigative measures on the Internet;
iii. the challenges to transborder investigations on the Internet posed by applicable international law on jurisdiction and state sovereignty.

3 The Transborder Group was to submit its report to the T-CY at the second plenary session of 2012 (scheduled for 5 and 6 December 2012) with the terms of reference expiring on 31 December 2012.

4 A first meeting of the Transborder Group was held in Strasbourg on 31 January and 1 February 2012, a second meeting on 1-3 June 2012 in Klingenthal near Strasbourg, and a third meeting in Strasbourg on 26-27 September 2012. The Transborder Group consulted a wide range of literature and information made available by the Parties to the Budapest Convention[4], and considered presentations and discussions at the Octopus Conference 2012.[5]

5 The Group focused on transborder access to data for criminal justice purposes, that is, for the investigation of offences against and by means of computer systems and for the gathering of electronic evidence in relation to any crime[6] while meeting rule of law and human rights principles. In this way, the Transborder Group remained within the scope of the Budapest Convention.

---

[1] http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY_2011_10E_PlenAbrMeetRep_V4%20_28Nov2011.pdf
The T-CY decided to appoint as members of the Transborder Group: Ioana Albani (Romania), Andrea Candrian (Switzerland), Markko Kunnapu (Estonia), Vladimir Miloseski ("The former Yugoslav Republic of Macedonia" who withdrew subsequently), Erik Planken (Netherlands), Betty Shave (USA), Branko Stamenkovic (Serbia) and Pedro Verdelho (Portugal).

[2] Through the "Consultations of the Parties", that is, the T-CY.

[3] The Report on the 6th Plenary of the T-CY was shared with the European Committee on Crime Problems (CDPC) in line with Article 46 (2).

[4] See References in the Appendix (Chapter X.X).

[5] See the website of the Octopus Conference 2012, www.coe.int/octopus2012

[6] See article 14 of the Convention.

6 The Transborder Group did not consider the question of transborder access to data for purposes other than for specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention.

7 The report confirms a need to consider enhanced transborder access in the light of technological developments, but also considers human rights and rule of law concerns and issues related to national sovereignty in connection with a possible expansion of transborder access.

8 Much attention is paid to explaining the current provisions of the Budapest Convention, in particular of Article 32. It would seem that further guidance by the T-CY is required to allow for a better understanding of this Article.

9 Current practices regarding direct law enforcement access to data as well as access via Internet service providers and other private sector entities are discussed in detail. They illustrate that law enforcement authorities (LEA) of many States access data stored on computers in other States in order to secure electronic evidence. Such practices frequently go beyond the limited possibilities foreseen in Article 32b (transborder access with consent) and the Budapest Convention in general.

10 With regard to possible solutions, the Transborder Group is of the view that more effective use should be made of the current provisions of the Budapest Convention, that a T-CY Guidance Note on Article 32 should be prepared, but also that the negotiation of an Additional Protocol on access to electronic evidence should be considered.

11 The present report was adopted by the 8th Plenary of the T-CY on 6 December 2012.

12 The mandate of the Transborder Group was extended to 31 December 2013 in order to pursue the two options.

# 2 Justification: The need to address the question of transborder access

## 2.1 Background

13 The question of unilateral transborder access by LEA of one territory to data stored on computer systems in a foreign territory without the need for mutual legal assistance is a very complex one as it touches upon agreed upon principles of international law (in particularly the territoriality principle and thus the question of national sovereignty) and procedural law safeguards protecting the rights of individuals.

14 The need for transborder access to electronic evidence has been discussed since the 1980s. The problem of "direct penetration" – in the form of "pure direct penetration" by LEA or compelling a person to produce data stored abroad – was raised in Recommendation R(89)9 on Computer-related Crime and the final report of the European Committee on Crime Problems (CDPC) of 1990.[7] At that time, the CDPC did not make specific proposals as it considered that the time was not ripe and the issue not too pressing yet.

15 Five years later, in 1995, the Committee of Ministers of the Council of Europe in Recommendation R(95)13[8] noted an urgent need to negotiate an international agreement on this question:

> VII. International co-operation
> 17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

16 In 2000, the preamble of draft versions of the Budapest Convention made specific reference to Recommendations R(89)9 and R(95)13 and specifically to the need to "regulate trans-border search and seizure".[9]

17 In parallel to the negotiations of the Budapest Convention from 1997 onwards, the G8 discussed options for transborder access in some detail.[10] In October 1999, the G8 Justice and Interior Ministers adopted "Principles on Transborder Access to Stored Computer Data" during their

---

[7] Final Report, pages 86-89. http://www.oas.org/juridico/english/89-9&final%20Report.pdf

[8] "Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology" http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp

[9] For example, draft version 19 (April 2000): *"Recalling Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology, calling for, inter alia, the negotiation of an international agreement to regulate trans-border search and seizure;"* . This was dropped in subsequent versions.

[10] See for example the paper on options prepared by Donald Piragoff and Larissa Easson in 1997 for both the G8 and for the Council of Europe Committee of Experts on Crime in Cyberspace (PC-CY) that prepared the Budapest Convention.

Ministerial meeting in Moscow, Russian Federation.[11] These Principles include that States enable measures such as expedited preservation of stored computer data[12] and expedited mutual legal assistance.[13] The G8 Principles furthermore covered "transborder access to stored data not requiring legal assistance":

> Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:
>
> accessing publicly available (open source) data, regardless of where the data is geographically located
>
> accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.

18 The structure and content of this principle agreed upon in Moscow is similar to that which later on became Article 32b of the Budapest Convention, the main difference being that the idea that "consideration" should be given to "notifying the searched State" was not maintained.

19 This brief account shows that the opening for signature of the Budapest Convention in November 2001 had been preceded by more than 16 years of preparatory work at the Council of Europe and in other fora.[14] The question of transborder access had been part of these deliberations from the outset. With Article 32b, an exception to the principle of territoriality under very narrow conditions was finally agreed upon.

20 The drafters of the Convention did not consider that the door for additional possibilities for transborder access was closed. As noted in paragraph 293 Explanatory Report:

- The Parties agreed to hold further discussion and possibly to regulate situations other than those of Article 32 at a later stage when more experience had been gathered.
- Situations of transborder access other than those of Article 32 are "neither authorised, nor precluded".

21 The T-CY took up discussions on this matter in 2009/10, when it studied the experience of State Parties with respect to transborder access to data on the basis of replies to a questionnaire.[15]

22 This in turn led the T-CY in 23-24 November 2011 to establish the Transborder Group tasked with identifying further options to regulate transborder access to data.

---

[11] Released at the Ministerial Conference of the G-8 Countries on Combatting Transnational Organized Crime, Moscow, 19-20 October 1999.

[12] Subsequently reflected in greater detail in Articles 16, 17, 29 and 30 of the Budapest Convention.

[13] Later on reflected in Article 31 Budapest Convention.

[14] The Select Committee of Experts on Computer-related Crime that prepared Recommendation (R(89)9) had been set up in March 1985.

[15] Document T-CY(2010)01.

## 2.2 The need for transborder access

### 2.2.1 The need to access data for criminal justice purposes

23 The use of information and communication technology (ICT) evolved exponentially over the last ten years. For illustration, by the end of 2011 more than 2.3 billion people reportedly used the Internet and the number of mobile phone subscriptions had reach almost 6 billion.[16]

24 The expansion of ICT use worldwide is accompanied by increasing offences against computer systems and by means of computer systems. Moreover, evidence related to any crime increasingly takes the form of electronic evidence stored on a computer system.

25 Governments have the positive obligation to protect the rights of individuals, among other things through criminal law and law enforcement measures.[17] Retrieving evidence is essential in this respect. It is a primary goal of criminal investigations to prosecute offenders or prove the innocence of suspects. For this reason, the Budapest Convention contains a range of procedural law measures aimed at preserving electronic evidence, search, seizure or intercept data and others. These procedural law provisions are applicable to electronic evidence in relation to any crime.[18]

26 LEA – that is, prosecutors, investigators, police officers authorised to apply these powers – may need access to a wide range of electronic evidence:

- Any type of computer data, including content data (such as documents, images, emails that are often encrypted), software, data on the functioning of a system or others.[19]
- Any type of traffic data, such as data on the source, path and destination of a communication, on the type of communication service used, on the beginning and end of an Internet session, on the service used, on the name and contact details of a subscriber to whom an Internet Protocol (IP) address was allocated at the time of a communication, and others.[20]

27 Electronic evidence may be found on any type of computer system[21] ranging from a desktop to laptop to mainframe computers but also mobile phones, tablets and others or computer networks and related devices such as hubs, routers, servers and others, or on storage devices such as hard-disks, USB keys, memory cards and others, or peripheral devices, or audio/video recorders, portable media players, game consoles and others.

---

[16] Source: http://www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf

[17] As pointed out also by the European Court of Human Rights, for example, in K.U. v. Finland (no. 2872/02 of December 2008) in which reference was made to the Budapest Convention, in particular the procedural law powers.
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

[18] See Article 14

[19] See the broad definition of computer data in Article 1 Budapest Convention.

[20] See the definition of "traffic data" in Article 1 Budapest Convention.

[21] See the definition of "computer system" in Article 1 Budapest Convention. At its first meeting in 2006, the T-CY agreed on a broad meaning of this definition which would also encompass mobile phones and other devices that are capable of producing, processing and transmitting data. See page 2 of the meeting report at http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2006)%2011%20E.pdf

28 "Access" may involve the preservation and partial disclosure of traffic data (Article 17 Budapest Convention), search and seizure (Article 19 Budapest Convention), disclosure or production orders (Article 18) but also the real-time collection of traffic data (Article 20) or the interception of content data (Article 21). The expedited preservation of data (Article 16) is a provisional measure to facilitate the lawful search, seizure or disclosure.

29 In view of changes in technology, some LEA have expressed the view that they may increasingly need to intercept data and communications (including VOIP) at source, to obtain passwords, to install software on the systems of suspects or to apply other coercive measures to access computers and data of suspects. Not all of these proposals may find international consensus.

30 The question is how electronic evidence can be secured and what measures are possible if computers and data are physically located in foreign, unknown or multiple jurisdictions or moving between jurisdictions.

### 2.2.2 Changes in technology

31 Technology and with it the way computers are used – also by criminals – has changed considerably in recent years. Resulting law enforcement challenges include:

- The increasing amount of data that are saved, processed and transferred.
- Individuals may use not only one but multiple devices simultaneously or successively.
- Cybercriminals have become experienced in encrypting their data or in remaining anonymous when using ICT (use of proxies, TOR routers, "foreign IPs", Voice-over-IP and others).
- Computers of innocent users are compromised and used for criminal purposes, such as for botnet attacks.
- Criminals carry out offences remotely in third States or use the information infrastructure of a third State to commit crime, thus reducing the risk of law enforcement investigation.
- Even if a criminal commits an offence in his own country, electronic evidence (such as data stored, web service used, traffic data related to the path of communications) may be found in multiple other jurisdictions.
- Data, including electronic evidence, is increasingly volatile. Websites or URL's containing illegal data and electronic evidence can be moved to a different IP address within seconds.
- The increasing use of cloud computing and web-based services where data (including electronic evidence) is stored "somewhere in the cloud", that is, on servers – or scattered over several servers or being moved between servers – in varying locations and jurisdictions often unknown to users and to law enforcement.

32 Thus, solutions need to be found so that LEA can secure evidence that is volatile, unstable and scattered over multiple jurisdictions.

33 Furthermore, in exigent circumstances, LEA of most States are able – in domestic investigations – to take immediate action to prevent imminent danger to life, limb or property or the escape of a suspect or the destruction of evidence. In such exceptional situations, LEA may act without a judicial order. This may also need to apply to the search or seizure of electronic evidence if there is a risk that such evidence is lost or in other exigent circumstances.[22]

[22] For the US see page 27 ff at. http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

34 The question is whether and under what conditions the securing of electronic evidence or other measures that fall under the exigent circumstances exception in domestic situations would be permitted in international situations where data is stored in a foreign or unknown jurisdiction.

### 2.2.3 The "loss of location"

35 It can be argued that these changes in technology, in particular cloud computing, have led to a "loss of location".[23] Data are moving between servers and jurisdictions or may be mirrored for reasons of security and availability, and may thus be located in different jurisdictions at the same time. The content of a website may be composed of a web of dynamically interlinked sources of information.[24]

36 Law enforcement powers, including in particular coercive powers, to retrieve electronic evidence are normally linked to a specific location. Location determines which law enforcement agency under which law can investigate and apply coercive powers. It also helps determine the rights of suspects or aggrieved parties to defend themselves. If data is stored within the same State, LEA can apply the powers foreseen under domestic laws.

37 If the data is stored in a foreign jurisdiction, LEA would need to resort to international cooperation. The basic rule of international law regarding the exercise of coercive powers is the principle of territorial sovereignty. No State may enforce its jurisdiction within the territory of another sovereign State.[25] As a consequence, international cooperation is dependent on international treaties – such as the Budapest Convention on Cybercrime – or bilateral agreements between the States concerned.

38 Within the context of cloud computing and web-based services, location is not stable. The concept of data stored on a computer system in a given location or on a specific territory may now be of more limited relevance. This raises important questions regarding the value of the principle of territoriality as the basis for determining the jurisdiction to enforce.

### 2.2.4 Access via providers and other private sector entities

39 Instead of accessing data stored abroad directly transborder or by means of international judicial cooperation, LEA may also access data physically stored abroad via Internet service providers or other private sector entities either through the legal representation of such entities in their countries or possibly by contacting the entity abroad.

40 It has been argued that such access may infringe the sovereignty of the foreign State unless it is accepted by that State.[26]

41 Scenarios, current practices, issues and possible options will be discussed in more detail later on in this report.

---

[23] See: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

[24] Sansom, Gareth (2008), "Website Location: Cyberspace vs. Geographic Space" (Draft: 3 April 2008), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/Gareth%20Samson%20Website%20Location.pdf

[25] Cf. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10

[26] Sieber 2012: C147/148.

### 2.2.5 Conclusion: the need for common solutions

42 The provisions of the Budapest Convention on Cybercrime remain valid, even if technology has changed and if ICT play an ever more important role in societies. Effective implementation and application of the procedural law tools and provisions on international cooperation will help address many of the challenges mentioned so far.

43 With respect to the specific question of transborder access to data, two articles are of particular relevance, namely, Article 19.2 on empowering LEA to extend searches and seizures to computers accessible from the initial system "in its territory" and Article 32 covering transborder access to publicly available data (32a) and to stored data with consent (32b).

44 As this report will show, the legislation and practices of a number of States go beyond these provisions in terms of direct transborder access to data or access via private sector entities. Practices seem to vary considerably between different States.

45 There seems to be a case, therefore, to formulate common solutions that provide guidance to the Parties to the Budapest Convention.

## 2.3 Human rights and rule of law concerns raised by expanded transborder access

46 Crime affects the rights of people. This is also true for cybercrime. An attack against the confidentiality, integrity and availability of computer data and systems (Articles 2 to 6 Budapest Convention), for example, violates privacy and other rights. As underlined by the European Court of Human Rights, governments therefore have the positive obligation to protect people, among other things through criminal law and enforcement measures, including the measures foreseen in the Budapest Convention.[27] At the same time, the rights of people are to be protected when investigating cybercrime.[28]

47 Therefore, and though computers and the Internet have helped crime to transcend borders and jurisdictions, there are reasons to be cautious before moving ahead with increased transborder access by law enforcement authorities. States share much common ground relating to issues such as the protection of individuals and legitimate interests of third parties, but for legal and policy reasons they still differ in their applicable regimes. Many of the issues and difficulties that prevented consensus beyond Article 32b in the past may still be relevant.

[27] As pointed out also by the European Court of Human Rights, for example, in K.U. v. Finland (no. 2872/02 of December 2008) in which reference was made to the Budapest Convention, in particular the procedural law powers.
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

[28] See Article 15 Budapest Convention on conditions and safeguards.

### 2.3.1 Legal and policy concerns for States

48 International cooperation in criminal matters is based on a number of principles, including that of dual criminality or the possibility to refuse cooperation if it is contrary to the public order of the requested State. Transborder access may be used to circumvent such principles.

49 This could include, for example, a situation where police of State A suspect that a person in State B has committed an act that is a crime in State A but not a crime in State B. If the police of State A reach into State B to gather evidence against the person in State B, this may raise significant legal and policy interests for State B. Initially, State B may as a general matter require dual criminality to provide assistance, or it may require it in cooperation treaties it has signed with countries with significantly different legal systems. Even where it does not require dual criminality, it may reserve the right to deny assistance in situations in which it considers that providing cooperation would be contrary to its public order. For example, State B, whose people exercise broad freedom of expression, may not want State A to reach into State B to gather evidence of defamatory conduct that would be protected under its own legal system. It may object either on the ground that defamation is not a crime in State B, or because it considers cooperation to be contrary to its public order.

50 Situations may also include that the police in State B operate under different requirements to conduct a search than the police in State A, and are subject to criminal, civil, or administrative liability for failing to respect these requirements. It may be a difficult legal and/or policy issue for State B to authorise State A to conduct a direct search of computer systems in its territory under legal standards for search that vary from its own.

51 Thus, before the issues discussed below are considered, there are important and difficult legal and policy matters States will have to grapple with in crafting a transborder search regime beyond what is permitted under Article 32.

### 2.3.2 Implications for individuals

52 An extremely important concern raised by transborder access is the difficulty that foreign authorities would have in applying the applicable protections for individuals under the law of the State in which the computer system being searched is located. Everyone agrees that transborder access must protect individuals by setting conditions and safeguards on computer and network searches by law enforcement entities.[29] However, States diverge in their views of what safeguards and protections should apply. Well-known examples include differences on the scope of freedom of expression or the requirements on police to obtain an order authorizing a search. The people[30] in a particular State normally expect, at a minimum, the protections afforded to them by this State; they do not expect to be searched according to the standards of a State they do not live in and may never have been in. In turn, the State has an obligation to respect individuals' rights and freedoms incorporated into its domestic law. Thus, the question is which State's safeguards and protections apply to transborder access?

---

[29] See, Article 15 of the Convention on Cybercrime and associated explanatory notes. These same principles should apply to any law enforcement access to data. For a discussion on Article 15 of the Convention on Cybercrime, see, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf.

[30] In the context of this section, "people" refers to natural persons and legal persons, to the extent that legal persons are afforded the rights and protections presented here.

53 Transborder access could also raise significant legal and policy issues when a law enforcement entity gathers evidence in a manner that is unlawful in the State where the data is located. In addition to the examples already given, State G might prohibit interception of electronic communications and may be unwilling to permit State F to use transborder access for interceptions. State H may permit a prosecutor to order a search, while State I may require a judicial warrant for the same search.

54 The location of the person and place of the crime are likely to change the equation. Fewer concerns may arise if the person and crime are located in the same State and only data resides in another State. As long as the law enforcement authority complies with conditions and safeguards established in its own domestic law, the person would be adequately protected.

55 Further, extending transborder search may lend itself to misuse by States that are less committed to following the rule of law. For example, transborder access might be used in the guise of legitimate law enforcement activity as a means to improperly investigate political dissidents and chill legitimate political activity: State J may see a blogger as a sympathetic political dissident while State K sees the blogger as inciting to public disorder or even terrorism.

56 Transborder access thus raises many issues about the protection of individuals subject to a search. In simple terms, people expect application of a predictable regime of protections. Alleviating concerns about the application of safeguards and protections by different States will be a difficult and necessary step in considering expanding transborder access.

57 Action by LEA of States that are Parties to the European Convention on Human Rights may be challenged before the European Court of Human Rights as an exercise of (extraterritorial) jurisdiction by that State pursuant to Article 1.[31] Individuals affected by such LEA action may thus benefit from the protection regime of the European Convention on Human Rights.

### 2.3.3 Implications for third parties

58 Transborder access could also have an impact on the rights of third parties, especially system operators and service providers. Third parties expect to be able to operate under the rules of the State in which they are located or do business. States have conditions and safeguards on computer and network searches that take into account the legitimate interests of third parties[32]. However, transborder access could put third parties in jeopardy, both legally and practically.

59 Service providers and other businesses with websites that can be used by persons in other countries, and other third parties that hold data for or about a person, are already struggling to comply with disparate and sometimes conflicting laws of different States. For example, it is usually a criminal offense in the United States for a commercial service provider to disclose to anyone (including a foreign government) the contents of an electronic communication[33]. In France, French law prohibits any national or person who usually resides on French territory and any employee of an entity having a head office or establishment in France from communicating to foreign public authorities documents or information relating to economic, commercial,

[31] http://www.echr.coe.int/NR/rdonlyres/DD99396C-3853-448C-AFB4-67240B1B48AE/0/FICHES_Juridiction_Extraterritoriale_EN.pdf
[32] See Article 15, paragraph 3, of the Convention on Cybercrime and associated explanatory notes.
[33] United States Code, Title 18, Section 2701, available at http://uscode.house.gov/download/title_18.shtml

industrial, financial or technical matters, that is capable of harming the sovereignty, security or essential economic interests of France or contravening public policy.[34]

60 Yet, US or French service providers may receive judicial orders from other countries to disclose such information. Direct application of foreign laws, including privacy frameworks, have far-reaching implications for service providers everywhere. Expanded transborder access would likely make business even more complicated.

61 As an expansion of transborder access would affect private sector entities and others, the views of the private sector and civil society should be sought when negotiating additional instruments.

### 2.3.4 Risks to the protection of personal data

62 Personal data are increasingly stored by private entities, including cloud service providers. Access by law enforcement to or the disclosure to LEA of personal data stored in a foreign jurisdiction by such private sector entities may violate data protection regulations.

63 To the extent that IP data are considered personal data, this also applies to traffic data.

64 This risk has been pointed out by the EU's Article 29 Working Party:

> Lack of confidentiality in terms of law enforcement requests made directly to a cloud provider: personal data being processed in the cloud may be subject to law enforcement requests from law enforcement agencies of the EU Member States and of third countries. There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur. [35]

65 The European data protection framework is currently under reform. The Council of Europe is modernising its Data Protection Convention 108.[36] The European Union Commission in January 2012 presented "its data protection package" consisting of a directly applicable general Regulation[37] and of a Directive covering data protection in the criminal justice area.[38] The drafts of both instruments are under discussion.

66 Regarding access to data via providers or other private sector entities, recital 90 (draft Regulation) reads as follows:

---

[34] *Loi* of 26 July 1968, amended by the loi of 17 July 1980 and ordonnance of 19 September 2000, available (French) at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000501326 .

[35] Article 29 Data Protection Working Party (2012): Opinion 05/2012 on Cloud Computing" (adopted 1 July 2012) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[36] www.coe.int/dataprotection

[37] "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (Brussels, 25.1.2012 COM(2012) 11 final) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[38] "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data" (Brussels, 25.1.2012 COM(2012) 10 final) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

> (90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.

67 Issues may also arise with regard to purpose limitation. If a company transfers data to another country for technical or other legitimate purposes but is then forced by law in that country to disclose data to law enforcement, data protection rules in the country of origin may be violated.

68 Concerns have been expressed that the draft Regulation and Directive may prevent effective international law enforcement cooperation, and that international agreements may need to be re-negotiated:[39]

> Article 60 [draft Directive] - Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police co-operation
>
> International agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.

69 This may also affect the Budapest Convention which obliges Parties to cooperate with each other "to the widest extent possible" (Article 23) and which limits the grounds for refusal of assistance. The Explanatory Report (paragraph 269) notes that "refusal of assistance on data protection grounds may be invoked only in exceptional cases".

70 The further evolution of the European Union's data protection framework will need to be kept in mind when considering means to make international cooperation against cybercrime more efficient in general and additional solutions for transborder access to data in particular.

### 2.3.5 Risk to property

71 A law enforcement entity's reaching into a foreign computer network introduces practical concerns, including means of entry, access to proprietary or private data, and protection of customers. Not only might the foreign law enforcement entity examine data in a third party computer network – troubling enough in itself if the examination is not legitimate – but the actions of the law enforcement entity may damage data or the system itself. Any expansion of transborder access would have to address the risk to property, including the risk to intellectual property.[40]

---

[39] For example at the Interparliamentary Committee Meeting on "The reform of the EU Data Protection framework – Building trust in a digital and global world" held at the EU Parliament, Brussels, 9-10 October 2012.

[40] Which falls under article 1 of Protocol No.1 to the European Convention on Human Rights. See in particular the report "Internet: Case law of the European Court of Human Rights", Research Division of the Court, 2011, available at http://www.echr.coe.int/ECHR/EN/Header/Case-Law/Case-law+analysis/Research+reports/

### 2.3.6 Risk to law enforcement operations

72 In addition to affecting individuals and third parties, transborder access could pose a risk to domestic and international law enforcement operations. Investigations often rely on secrecy and the cooperation of third parties. Transborder access could create situations where a law enforcement entity of another State fails to coordinate, data becomes unavailable to domestic law enforcement entities, or a suspect is notified of an investigation. As has occasionally happened, law enforcement entities within a State or from different countries could find themselves investigating each other because they mistake legitimate law enforcement activities for criminal activities.

### 2.3.7 Conclusion: Need for safeguards and procedures limiting transborder access

73 Solutions to the protection of individuals and other third parties or of law enforcement operations will have to overcome the practical difficulties of expanding rules for transborder access. Participating States will have to agree on the minimum conditions and safeguards that apply when a law enforcement agency reaches into another State to obtain electronic information. States must develop and agree on procedures for coordinating transborder access and communicating with each other on such activities. A significant consideration will be the domestic laws and procedures of the State where the data or subject is located, including data protection regulations. For a State to agree to transborder access, it must be satisfied that the access will comport with laws and key policies ranging from constitutional protections for individuals and the substantive criminal law related to computers and networks to protection of private property. States must also agree to enforcement mechanisms that deter improper use of transborder access.

74 In the end, expansion of transborder access will require States to give up some sovereignty. Before States will do so, it will be necessary to resolve the above-described legal and policy issues; thus far this has not proven possible. No matter the urgency or importance of improving law enforcement's ability to investigate and prosecute crimes facilitated by computers and the Internet, States will have to be satisfied that their interests, and the interests of their people, will be protected from undue access by other States.

# 3 Explaining relevant provisions of the Budapest Convention

## 3.1 Overview

75 The Budapest Convention requires Parties to

- criminalise offences against the confidentiality, integrity and availability of computer data and systems (Articles 2 – 6) and offences committed by means of computers (Articles 7 – 10), to provide for ancillary liability and sanctions (Articles 11 – 13), and to establish jurisdiction over offences related to Articles 2 – 11 (Article 22)

- establish procedural law powers to allow for effective investigations and securing of electronic evidence, such as search and seizure, preservation and real time collection and interception of computer data (Articles 16 – 21)

- engage in efficient international cooperation (Articles 23 – 35).

76 The Convention adapts, on the one hand, traditional procedural measures to the new technological environment. In addition to that, new methods have been created, such as the expedited preservation of data,[41] in order to ensure that procedural measures remain effective in a volatile technological environment.

77 Some of the procedural measures to be taken at the domestic level are mirrored in the chapter on international cooperation[42] in order to ensure that evidence can be secured effectively through international cooperation.

78 Article 14 provides for a broad scope of the procedural law measures. According to this Article their application is not restricted to the prosecution of the criminal offences listed in the Convention. It creates the explicit obligation for Parties to apply these procedural powers with regard to all criminal offences committed by means of a computer system and the collection of evidence in electronic form. This broad scope – with exceptions – also applies to international cooperation.[43] The text of the Convention makes it clear that States should incorporate into their domestic law the possibility and potential to ensure that information contained in electronic form can be used as evidence before a criminal court, irrespective of the nature of the criminal offence.[44]

79 Under Article 15, the establishment and application of the procedural provisions shall be subject to conditions and safeguards that are provided for under national legislation.[45] The aim is to adequately protect human rights and freedoms, such as the rights and obligations deriving from the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms or other international human rights instruments. The principle of proportionality shall

[41] Articles 16 and 17 of the Convention.

[42] Article 16 on expedited preservation in Article 29, Article 17 on partial disclosure in Article 30, Article 20 on the real-time collection of traffic data in Article 33, Article 21 on the interception of content in Article 34.

[43] See paragraph 243 Explanatory Report.

[44] See also paragraph 141 of the Explanatory Report to the Convention.

[45] For a study on Article 15 see http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

be incorporated. In the end, Parties have to determine which of the powers and procedures possess a degree of intrusiveness that makes additional safeguards necessary in order to protect fundamental rights at stake.

80 According to Article 15.3, States shall consider the impact of procedural powers upon the rights, responsibilities and interests of third parties. Steps can be taken to mitigate such impacts, for example upon liability for disclosure or proprietary interests or with regard to service providers.[46]

81 Thus, it is important to retain that:

- the Budapest Convention offers a range of measures to effectively secure electronic evidence in relation to any crime at domestic and international levels
- human rights and rule of law principles are to be respected when investigating cybercrime and securing electronic evidence.

82 When dealing with crimes with transnational elements, national prosecuting authorities need effective, expedited and reliable ways to obtain information and evidence from abroad. Such access needs to be legal to allow the use of evidence obtained in court. The standard international procedure for obtaining evidence from abroad is through mutual legal assistance.

83 The Budapest Convention, in Articles 23 to 35, contains a range of general and specific provisions on international cooperation regarding cybercrime and electronic evidence.. The approach consists of a combination of provisional measures to secure electronic evidence in an expedited manner (Articles 29 and 30 together with Article 35 as an operational mechanism to apply these in practice) with traditional mutual legal assistance.

84 A subsidiarity principle applies, that is, Parties should cooperate with each other on the basis of other bi- or multilateral agreements, and the Budapest Convention may supplement such cooperation agreements or be used if other agreements are not in place. Such other agreements shall not conflict with the principles of the Budapest Convention (Articles 23 and 39). Parties may go beyond the provisions of the Budapest Convention in their international cooperation.

85 Discussions before, during and after the negotiations of the Budapest Convention underlined that – given concerns with respect to procedural and privacy rights of individuals as well as national sovereignty – preference should be given to making mutual assistance more efficient, in particular the specific measures foreseen in Articles 29 to 34.[47]

86 On the other hand, in cyberspace national borders and competences may not be distinguishable. Often, a LEA accessing stored data via an electronic network is not in a position to determine whether a specific dataset is physically stored in the State from which he is accessing the Internet or whether it is stored abroad. The increased use of external hosting providers and the application of cloud computing devices and services further complicate the matter.

[46] See also paragraph 148 of the Explanatory Report.

[47] For this reason, the T-CY (in November 2011) decided to assess implementation by the Parties of the expedited preservation articles 16, 17, 29 and 30, and proposed (in June 2012) to focus the next round of assessments on expedited mutual assistance (Article 31).

87 With Article 32 on transborder access an exception to the principle of territoriality was, therefore, regulated in an international instrument.

## 3.2 Transborder access to data: relevant provisions

### 3.2.1 Article 32

88 The question of whether a State and its authorities shall be permitted to access unilaterally electronic data stored abroad by domestic law or international agreements has been discussed for more than two decades, including during the negotiation of the Budapest Convention. As noted in the Explanatory Report, in relation to Article 32, on transborder access to data:

> 293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.
>
> 294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

89 Article 32 is thus the most important provision on transborder access foreseen in the Convention. The practice of some State Parties shows that Article 19.2 on extending searches to connected computer systems may also be relevant. Finally, the issue of jurisdiction (Article 22) requires further discussion.

90 It is important to retain that according to paragraph 293 Explanatory Report:

- The Parties agreed to hold further discussion and possibly to regulate situations other than those of Article 32 at a later stage when more experience had been gathered
- Situations of transborder access other than those of Article 32 are "neither authorised, nor precluded".

### 3.2.2 Article 32a – Transborder access to publicly available data

91 Article 32a addresses the situation where the data sought transborder is publicly available (open source data):

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
>
> a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or …

92 Investigating authorities shall be permitted to directly access stored information that, for example, has been published on a website. They may download the data, take screenshots or similarly secure such data and use them as evidence in criminal proceedings without the need for mutual legal assistance or the permission of the State where the computer system hosting the website is located.

93 Article 32a thus allows access to data that technically may be stored on a foreign territory. It may be assumed that such access to publicly accessible data for criminal justice purposes has become accepted international practice and thus part of international customary law, "due to the general, worldwide use of the Internet, the often lacking knowledge of users of the physical location where data is stored as well as the low intensity of the intrusion when public data is accessed in cyberspace".[48]

### 3.2.3 Article 32b – Transborder access with consent

94 Article 32b addresses the situation where LEA of one State accesses data stored in another State with the voluntary consent of the person lawfully authorised to disclose the data but without the need to involve the authorities of that State.

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
> ....
> b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

95 As indicated earlier, Article 32, and in particular Article 32b, is the result of lengthy discussions. The States negotiating the Budapest Convention did not regulate this provision in great detail but left "constructive ambiguity" so that it could address different situations. The Convention deliberately did not exclude that Parties go beyond Article 32.

96 Regarding the elements of Article 32b a number of questions have been raised.

---

[48] Sieber (2012, page C144/145). See also Seitz (2004, page 9/10 at http://www.ijclp.net/files/ijclp_web-doc_2-cy-2004.pdf).

#### 3.2.3.1 What is "transborder", what is "location"?

97 According to Paragraph 293 Explanatory Report to the Budapest Convention, transborder access means "to unilaterally access computer data stored in another Party without seeking mutual assistance".

98 It is a measure that can be applied between the Parties. It is presumed that the Parties to the Convention form a community of trust and that certain rule of law and human rights principles are respected in line with Article 15.

99 Article 32b refers to "stored computer data located in another Party". This suggests that it is known where the data is located.

100 Article 32b, in turn would not cover situations where a person provides consent but where the data are not stored in another Party or where it is uncertain where the data are located.

101 Given that Article 32b does "neither authorise, nor preclude" other situations, in such situations States may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.

#### 3.2.3.2 What is access without the authorisation of the other Party?

102 As indicated above, this means "to unilaterally access computer data stored in another Party without seeking mutual assistance".

103 The Budapest Convention does not require a notification of the other Party, unlike the relevant Principle adopted by the G8 in Moscow in October 1999 which suggested that consideration be given to "notifying the searched State". At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

#### 3.2.3.3 What constitutes consent?

104 Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived.[49] What constitutes consent is to be governed by the domestic law of the Party to whom consent is given, that is, the Party seeking transborder access.

105 Subject to domestic legislation, a minor may not be able to give consent, or persons because of mental or other conditions may also not be able to consent.

106 In most Parties, cooperation in a criminal investigation would require explicit consent. For example, general agreement by a person to terms and conditions of an online service used

[49] The Gorshkov/Ivanov case of 2000 is often cited as an example of the use of Article 32b. This, however, is not correct, since the plaintiffs did not consent to provide access voluntarily. In any case, the Budapest Convention was only adopted in 2001, that is, one year later, it only entered into force in 2004 and the USA only became a Party in 2006.
(See: United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, *2 (W.D.Wash. May 23, 2001). Discussed in http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf).

would not constitute explicit consent even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse.

#### 3.2.3.4 **What law applies?**

107 Article 32b does not specify whose laws apply to determine "lawful consent" and whether a person is "lawfully authorised" to disclose data.

108 In both respects, for practical purposes "lawful" seems to mean the law of the searching Party. In urgent situations of transborder access it would not seem feasible that the searching LEA is able to verify the rules governing the use of the data in the other Party, and in any case, LEA would normally act on the basis of the laws of their own State.

109 However, if it is obvious that the disclosure or providing of access would violate the laws of the other Party or the rules on the use of the data, LEA would be discouraged from pursuing transborder access.

110 In this respect, it is conceivable that domestic legislation could make it unlawful altogether to disclose information to foreign authorities that could be used in criminal proceedings and without involving domestic authorities. Under the "French blocking statute" of 1980:[50]

> Article 1 bis (Créé par Loi 80-538 1980-07-16 art. 2 II JORF 17 juillet 1980)
> Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci.

111 However, as this provision is subject ("sous reserve …") to international agreements, this particular statute would not block cooperation under Article 32b.

#### 3.2.3.5 **Who is the person who can provide access or disclose data?**

112 As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances and rules applicable. Paragraph 294 Explanatory Report offers a simple example of a person providing access to his email account or other data that he stored abroad.

113 The person providing access may also be an Internet or cloud service provider or another private sector entity holding data of an individual, for example, if the terms of service permit this or if the service provider has become the owner or has the power of disposal of the data. In this

---

[50] Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre economique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères Version consolidée au 01 janvier 2002
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000501326
This law was applied in 2007 in a US discovery case. A French attorney ("Christopher X"), acting on behalf of his American client in a Californian proceeding, contacted a French national in France to obtain information. He was indicted and convicted on the basis of Article 1 bis of the French blocking statute. The Cour de Cassation confirmed the judgment
http://www.easydroit.fr/jurisprudence/Cour-de-cassation-criminelle-Chambre-criminelle-12-decembre-2007-07-83-228-Publie-au-bulletin/C85945/

case, to be in line with Article 32b, a service provider would have to provide access voluntarily and lawfully, that is for example, without violating privacy or other rights. Therefore, this would usually only be possible for data owned by the private sector entity, such as traffic data, subscriber information or other network data, while it may not be possible to disclose content generated by users voluntarily and lawfully. A judicial order for the seizure or production of data would not fall under Article 32b.[51]

#### 3.2.3.6 Where is the person located when consenting to provide or when providing access?

114 Article 32b is not specific as to where the person providing access is located at the moment of consenting to disclose data or when actually providing access.

115 The standard hypothesis is that the person providing access is physically located on the territory of the requesting Party. In this situation, that person falls under the jurisdiction and is subject to the laws of the investigating State.[52] This had also been the working hypothesis of the PC-CY Committee that elaborated the Budapest Convention.[53] This assumption was later on not specifically reflected in the adopted Convention.

116 In fact, multiple situations are possible. It is conceivable that the physical or legal person is located on the territory of the requesting LEA when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access. The person may also be physically located in a third country when agreeing to cooperate or when actually providing access. If the person is a legal person (such as a private sector entity), this person may be represented on the territory of the requesting LEA, the territory hosting the data or even a third country at the same time.

117 In 2009-2010, the T-CY carried out a first survey on the question of transborder access.[54] Replies to a questionnaire received at that time suggest, that for most Parties it was not relevant where the person was located when providing access.

118 However, most (but not all) Parties would object – and some even consider it a criminal offence – if a person who is physically on their territory is directly approached by foreign LEA authorities who seek his or her cooperation.

---

[51] For different scenarios see for example page 11-12 in: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

[52] Kaspersen, Henrik (2009): Cybercrime and internet jurisdiction (Discussion Paper prepared for Council of Europe / Global Project on Cybercrime), page 27. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

[53] Up to version 19 (April 2000), Article 27 (the precursor of Article 32) had a footnote attached to it: *"This paragraph assumes that the accessing State will limit its own contact to persons within its territory (though such persons may themselves need to contact people in other territories in order to obtain such consent or authority). This could be explicitly added by the insertion of the bracketed text or be explained in the explanatory memorandum."*

[54] Replies were received from 18 countries (Bosnia and Herzegovina, Chile, Cyprus, Czech Republic, Finland, Estonia, Germany, Hungary, Japan, Lithuania, Moldova, Montenegro, Norway, Portugal, Poland, Sweden, Turkey, United States of America) and were compiled in T-CY(2010)01 and draft analysis was made available in T-CY(2010)05 dated 15 June 2010.

### 3.2.4 Article 19.2 – Extending a search

119 One of the key provisions regarding procedural law is article 19 of the Convention. It obliges Parties to provide for legislation that enables competent authorities to search, access, seize and secure computer systems, data or storage media that are located in their territory. Computer data shall, as is the case regarding "traditional" pieces of evidence, be made tangible and available for the purposes of criminal investigations and proceedings. It is, however, left to Parties to make sure that the principles of data protection and secrecy of communication are adhered to.[55] States may, for example, consider an email stored on a server of a service provider as data in transfer and part of a communication[56] until it is retrieved or downloaded by the user or addressee.

120 Article 19.2 is to allow LEA to expeditiously extend the search or similar access to other computer systems which are lawfully accessible from the primal system in cases where there are grounds to believe that the data sought may be stored in that other system.

> 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.

121 The Explanatory Report underlines that Article 19 refers to measures at the domestic level and that the computer to which the search may be extended is to be located on "its territory":

> 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)

[55] See paragraph 190 of the Explanatory Report.

[56] Consequently, the content of the stored message may be obtained by the authorities through the application of the power of interception, only.

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.

122 While extending a search under Article 19.2 is thus designed to constitute a domestic measure, it nevertheless raises the question as to what rules apply in situations where LEA extend the search to computer systems in a foreign territory without being aware of it or if it is unclear in the course of a search on which territory a computer system is located and thus to whom to address a request for international assistance.

### 3.2.5 Article 22 – Jurisdiction

#### 3.2.5.1 General principles of the Budapest Convention

123 The Budapest Convention establishes general principles on jurisdiction:

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

124 Article 22 of the Convention specifies a number of criteria under which Parties are required to prosecute and punish the commission of crimes according to articles 2 through 11 of the Convention. Paragraph 1b through 1d is based on the principles of flag[57] and nationality. These provisions may be, according to paragraph 2, subject to reservations by the Parties.

125 Paragraph 1a is based upon the principle of territoriality and constitutes a mandatory provision. According to the Convention, Parties are obliged to establish jurisdiction over offences when committed on their territory. With regard to "traditional" crimes, the process of deciding whether a crime has been committed on a specific territory usually does not pose major problems.

126 The situation may, however, be different when it comes to crimes committed by electronic means or against a computer system. With regard to stored computer data or a person acting via web-based connections, it may often not be clear in which location or territory an act has been executed or an effect has taken place. The situation becomes even more complicated when technological possibilities such as cloud computing or external storing devices are being used. When using cloud computing, data are, partly or as a whole, constantly shifting from one location or server to another. Data may be mirrored in order to raise availability and security of the information stored. It may become unfeasible, for authorities and even for the owner of data, to decide upon the current location of computer data that have to be retrieved.

127 As indicated earlier in this report, it is a challenge for Parties and prosecuting authorities dealing with cybercrime to cope with the situation where a so-called "loss of location" leads to significant incertitude with regard to the place where sought computer data is being stored.

#### 3.2.5.2 **The question of jurisdiction[58] (to enforce)**

128 The primary jurisdiction issue to be addressed in relation to transborder access is that of the jurisdiction to enforce versus the principle of territoriality.

129 The experts drafting Council of Europe Recommendation R95(13)[59] acknowledged that transborder investigations were technically feasible and that investigators were not always aware that the systems and data were located on a foreign territory, but shared a common understanding

> that investigative activity of law enforcement authorities of a State Party in international communication networks or in computer systems located in the territory of another state may amount to a violation of territorial sovereignty of the state concerned, and therefore cannot be undertaken without prior consent of the State concerned.[60]

[57] With regard to ships and aircrafts.

[58] For a discussion of jurisdiction issues related to the Budapest Convention see http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

[59] Council of Europe / Committee of Ministers (1995): Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology"

[60] Kaspersen, Henrik (2009): Cybercrime and internet jurisdiction (Discussion Paper prepared for Council of Europe / Global Project on Cybercrime) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

130 The principal rule of international customary law regarding the jurisdiction to enforce is still considered to be reflected in the Lotus case of the Permanent Court of International Justice (PCIJ) of 1927:

> The first and foremost restriction imposed by international law upon a State is that - failing the existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or convention.[61]

131 While the experts drafting Recommendation R95(13) and those negotiating later on the Budapest Convention on Cybercrime were concerned that transborder access by means of ICT "may" infringe national sovereignty and the principle of territoriality, they were not affirmative that transborder access by means of ICT without a physical presence on the territory of the other State would indeed represent a violation of the principle of territoriality in the sense of the Lotus decision of 1927. The solution agreed upon was that under the Budapest Convention transborder access would be allowed under the narrow conditions of Article 32.[62]

132 In the sense of the Lotus decision, Article 32 is thus "a permissive rule derived from international custom or convention".

133 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.[63]

134 While the principle of territoriality remains predominant, doubts as to its applicability in virtual "cyberspace"– where data are moving between, are fragmented over, are dynamically composed from, or are mirrored on servers in multiple jurisdictions – are increasing. It is not possible to apply the principle of territoriality if the location of data is uncertain. A "paradigm shift" has therefore been called for.[64]

135 When discussing additional "permissive rules" and further exceptions to the principle of territoriality – such as transborder access without consent – the following questions may stimulate reflection and help qualify the principle of territoriality:

- Is transborder access indeed an act of exercising power "on" a foreign territory if the investigating LEA is accessing data from his own territory?[65]

---

[61] Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10, at 18 (1927).

[62] Article 32 will be discussed in more detail later on in this report.

[63] Budapest Convention Explanatory Report, paragraph 293.

[64] Discussions at Octopus Conference 2012 (www.coe.int/octopus2012). See also Salt, Marcos (2012): Acceso trasfronterizo de datos almacenados en soportes informáticos en los países de America Latina (contribution to Council of Europe Octopus Conference 2012)

[65] On the one hand, accessing computer data is not a *concrete* act of enforcement that could be compared, for instance, to the seizure of material. But under international law, an exercise of state authority does not necessarily refer to the use of *material/tangible* means. For instance, in the field of the law of immunities, the International Court of Justice (ICJ) considered in the *Arrest Warrant* case that "*the issuance*, as such, of [an] arrest warrant represents an act by the […] judicial authorities". (Case of the "Arrest Warrant of 11 April 2000" (Democratic Republic of the Congo v. Belgium), Judgment, *ICJ Reports* 2002, §70. See also the joint separate opinion of Judges Higgins, Kooijmans and Buergenthal : "An international arrest warrant […] is

- What is the link between the data and the territory in which the data is stored? For example, to what extent does the principle of territoriality apply in a situation of transborder access
  - if the person having the power of disposal over data is physically present on the territory of the investigating LEA while the data accessed are stored in another State?
  - if the IP addresses linked to a communication investigated are related to the territory of the investigating LEA while the actual data accessed are stored in another State?
- How does the principle of territoriality apply
  - if it is unknown in which State the data accessed is physically stored?
  - if multiple copies of data are stored in different States?
  - if data are moving between different States?
  - if data are fragmented over different States or dynamically compiled from sources in multiple States?
- To what extent is the investigating LEA intervening in the domestic affairs of the State where the data is located?
- What is the impact of the transborder access on the interests of the State where the data is located?
- What is the impact of transborder access on the rights of a suspect? Does it make a difference to what extent the procedural and privacy rights of the person whose data are accessed are protected under the laws of the State carrying out the transborder search?
- Does it make a difference if the access to the data by LEA is lawfully ordered in the LEA's State and subject to conditions and safeguards such as those foreseen under Article 15 Budapest Convention?
- Does it make a difference if data obtained transborder relates to traffic data and subscriber information or to content data?
- What is the impact of the transborder access on the interests of 3rd parties?
- How intensive or intrusive is the measure taken transborder? Does it make a difference if LEA access publicly available data or retain a copy of non-publicly available data or interfere with the data (for example delete or alter data) or the system (disable, block or otherwise hinder the functioning of the system) located in another State? Does it make a difference if LEA obtain access via a lawfully obtained password or other access credentials or if LEA needs to "hack" data?
- Would transborder access without consent be permitted in exigent circumstances? Does is make a difference if the offence investigated is serious crime or if there is an immediate threat to life and limb?
- To what extent do principles such as reciprocity or dual criminality apply?

---

analogous to the locking-on of radar to an aircraft: it is already a statement of willingness and ability to act and as such may be perceived as a threat so to do" (Joint Sep. Op., § 69)).

# 4 Scenarios of transborder access

136 This section summarises the results of a T-CY survey in 2009-2010, practices reported by States as well as information on transborder access via service providers or other private sector entities.

## 4.1 Direct LEA access to data: Practices reported in 2009 - 2010

137 In 2009-2010, the T-CY carried out a survey on direct transborder access to data and data flows. The responses suggest that law enforcement authorities of many States carry out transborder searches but that conditions and practices differ. In many cases, practices have evolved since. It should be stressed that it was not based on the analysis of the practices of all Parties to the Convention.[66] The questions were related to five scenarios.

### 4.1.1 Scenario A – Transborder access during search of premises

> Executing a search warrant on the premises of a suspect, your law enforcement agency finds a computer which is still turned on. The agency lawfully obtains from the apprehended suspect the necessary password for accessing computer data stored on a computer system located elsewhere with alleged illegal content or other incriminating evidence belonging to the suspect.

138 In most responding States[67], LEA can directly access the computer data from the suspect's own computer, if it is not apparent in which jurisdiction the computer data are stored. Most of them can also obtain access to data from the suspect's own computer using his/her password.

139 If it is clear that computer data are stored in another jurisdiction, LEA of seven countries[68] can still access the data, while in ten countries[69] that would not be permitted anymore, unless a suspect cooperates voluntarily as foreseen in Article 32b. This applies similarly to access with the password of the suspect.

140 In nine States, the data thus obtained can be used in criminal proceedings even if the procedure is not based on a specific permission under international law such as article 32b of the Budapest Convention.[70] In the other responding States, this depends on the specific circumstances.

141 In almost all countries, urgency or the risk of loss of evidence does not make a difference as to whether or not transborder access is permitted under the above scenario.

142 In some States, the foreign authorities would have to be notified[71] while in others this is not necessary[72] or depends on the specific circumstances.

---

[66] Replies were received from 18 countries (Bosnia and Herzegovina, Chile, Cyprus, Czech Republic, Finland, Estonia, Germany, Hungary, Japan, Lithuania, Moldova, Montenegro, Norway, Portugal, Poland, Sweden, Turkey, United States of America) and were compiled in T-CY(2010)01 and draft analysis was made available in T-CY(2010)05 dated 15 June 2010.

[67] Finland, Lithuania, Portugal, Poland, Sweden, Turkey, Chile, Bosnia and Herzegovina, Montenegro, Cyprus, Japan, Hungary, USA. With respect to the Czech Republic, Estonia and Germany it depends on the specific circumstances.

[68] Finland, Portugal, Poland, Chile, Montenegro, Japan, USA.

[69] Czech Republic, Lithuania, Germany, Sweden, Turkey, Bosnia and Herzegovina, Japan, Hungary, Estonia and the Netherlands. In Cyprus, it depends on the type of data. For social networks it would be permitted.

[70] Finland, Norway, Portugal, Poland, Sweden, Turkey, Japan, Chile, Estonia (if the suspect is cooperating).

[71] Czech Republic, Portugal, Poland, Chile, Bosnia and Herzegovina, Montenegro.

### 4.1.2 Scenario B – Transborder access through lawfully obtained password

> Your law enforcement agency has lawfully obtained a password for accessing computer data with alleged illegal content or incriminating evidence.

143 The LEA of almost all responding countries can access the data from their own computer systems if it is not apparent in which jurisdiction the data is stored.

144 If it is clear that the data is stored in a foreign jurisdiction, the LEA of most countries can still access the data from their own computer system.[73]

145 As under the previous scenario, in most States the data thus obtained can be used in criminal proceedings even if the procedure is not based on a specific permission under international law such as article 32 b of the Budapest Convention[74]. In the other responding States, it depends on the specific circumstances.

146 And again, in almost all States, urgency or the risk of loss of evidence does not make a difference as to whether or not transborder access is permitted under the above scenario.

147 And as mentioned above, in some States the foreign authorities would have to be notified while in others this is not necessary or depends on the specific circumstances.

### 4.1.3 Scenario C – Transborder access through special software or technical means

> During criminal investigations your law enforcement agency has obtained knowledge of a computer system with alleged illegal content or other incriminating evidence.

148 The LEA of certain States are permitted to obtain remote access to data by means of special software (key loggers, sniffers) or other technical means if it is not apparent in which jurisdiction the computer system is located. However, in the majority of States this is not possible or only under very limited circumstances.

149 If it is clear that the computer system is in a foreign jurisdiction, such measures are not permitted in almost all responding States.[75]

150 In almost all States it is doubtful whether evidence thus obtained can be used in criminal proceedings.

### 4.1.4 Scenario D – Transborder access with consent (article 32b)

> During criminal investigations your law enforcement agency has obtained the lawful and voluntary consent of a person to access computer data stored in another jurisdiction that may represent important evidence.

151 The LEA of almost all States can access and secure (download) data in this case, if the person providing access is physically located on the territory of the LEA.

---

[72] Lithuania, Sweden, Turkey.

[73] Exceptions include Czech Republic, Lithuania, Sweden, Hungary, Estonia and the Netherlands.

[74] Finland, Norway, Portugal, Poland, Sweden, Turkey, Japan, Chile, Estonia.

[75] Exceptions are Bosnia and Herzegovina, Japan and possibly Chile.

152 If the person providing access is physically located in the State where the data is stored, this would still be possible for LEA of most States[76] while in others this would be excluded, doubtful or subject to additional conditions or is not clearly regulated.

153 In most States[77], it is of relevance whether the person providing access has the lawful authority to disclose the data under the laws where the data is stored. Only in two responding States[78] would LEA need to notify the other State. In situations where the LEA do not know where the data is, States may still act in good faith.

154 In most responding States, evidence thus obtained can be used in criminal proceedings, even if it is not based on a permission under international law (such as article 32b) or a request for mutual legal assistance.

### 4.1.5 Scenario E – Information provided by a service provider[79]

> During criminal investigations your law enforcement agency must obtain technical information from an Internet service provider concerning a suspect.

155 In all responding States, service providers are obliged to provide technical information to law enforcement where the data concern a national and are located and administered on the same territory as the LEA.

156 If the data concern a national of the State of the LEA, but are located and administered in a foreign jurisdiction, most LEA would require a mutual legal assistance request. The same applies if the data concern a foreign national who has committed an offence on the territory of the LEA and are stored and administered in another State.

157 The LEA of most States face technical and legal difficulties in obtaining such data stored and administered in another State.

158 In some States, service providers may answer directly to requests received from LEA of another country.

[76] Czech Republic, Finland, Portugal, Poland, Sweden, Japan, Chile, Bosnia and Herzegovina, Hungary, Estonia, USA.

[77] Czech Republic, Finland, Portugal, Poland, Sweden, Chile, Montenegro, Hungary, USA. It is of no relevance in: Bosnia and Herzegovina, Cyprus, Japan and Lithuania.

[78] Bosnia and Herzegovina and Poland. However, in other states this is handled on a case by case basis.

[79] Note: This information was provided in 2009. However, it seems that in the meantime some transnational providers changed their policies and are now prepared to disclose subscriber and traffic data to national LEA under certain conditions and if a lawful request is received, even if the data is stored in another jurisdiction.

## 4.2 Direct law enforcement access to data: State-specific examples

159 Law enforcement authorities of many States of different regions of the world reportedly access data transborder in a foreign jurisdiction in the course of domestic criminal investigations.[80] Only few examples are documented. The following information was provided to the Transborder Group by some of the Parties.

### 4.2.1 Belgium[81]

160 Under the "theory of objective ubiquity" an offence is located in all places where there is a constitutive element of the offence. Combined with the "theory of indivisibility", a court can claim competence over all elements linked to the offence. Belgium applies a combination of different jurisdiction theories (criminal event theory, theory of instrument, direct consequence theory).

161 Regarding the jurisdiction to enforce, that is, to search computer systems, a specific solution was introduced in the year 2000, namely, Article 88ter of the Belgian Criminal Code of Procedure.

**162** On 28 November 2000, one year prior to the opening for signature of the Budapest Convention on Cybercrime, the Belgian legislator adopted the Law on Informatics Crime. This law created Article 88ter of the Belgian Criminal Code of Procedure (BCCP). Article 88ter BCCP is a response to the above mentioned Articles 19.2 and 32 of the Budapest Convention on Cybercrime.

163 Article 88ter BCCP allows the investigating judge (that is, a judge with the specific duty to lead the investigation and with special investigative powers), when he orders a search in a computer system, to extend the search to another computer system or to a part of another computer system located elsewhere.

164 This competence is attached to conditions. The investigating judge can only decide this extension when it is:

(1) necessary to find truth in an investigation and

(2) when

(i) other investigation measures are not proportionate – for example different search warrants have to be issued for different premises – or

(ii) there is a clear risk that proof would disappear (a condition that is almost always fulfilled in cybercrime cases as digital proof is very volatile).

165 Since the Belgian legislature was concerned with the fact that the police would be able to go too far too easily (for example from the bank account of a suspect to all the bank accounts of the same bank), an additional condition was added in the sense that the investigating judge has to restrict the extended search to the parts of another computer system to which the users of the

[80] For example, LEA of many countries of Latin America reportedly access data on computer systems abroad from the computer located in their own country for which they have the lawful authority to access it. They would normally do so with the consent of the person having the authority to disclose the data, or by voluntary cooperation of private sector entities or by lawfully obtained passwords or access codes (but would not resort to hacking systems). See: Salt, Marcos (2012): Acceso trasfronterizo de datos almacenados en soportes informáticos en los países de America Latina (contribution to Council of Europe Octopus Conference 2012)

[81] Summary of a contribution by Jan Kerkhofs (prosecutor) and Philippe Van Linthout (investigating judge), Belgium, April 2012.

initial system have access (this condition is mostly met when the investigating judge allows the police to enter another computer with the login and password of the suspect; this login and password define the restriction of the access).

166 After the extended search, the person responsible for the computer system has to be informed by the investigating judge if he or she can reasonably be identified (most of the time this is not the case).

167 But the most innovative part of Article 88ter BCCP lies in its last subsection of paragraph 3, which states that when it seems that the data discovered is not stored on Belgian territory, the data is only copied. When this has happened, the investigating judge only needs to inform the Ministry of Justice through the Public Prosecutor Office; the Ministry of Justice informs the State involved, if it can reasonably be determined (it is rarely the case).

168 In accordance with Article 39bis BCCP, the copied data is as valuable as evidence before court as the original data (the data is not physically seized, but is considered to be seized).

169 For example, it means that Belgian police can collect evidence starting from Belgian computers (not necessarily the computer of the suspect) and go from there to servers located in any country. They can start examining an account, the moment they have password and login.

170 This is clearly an advantage to save precious time and in order not to lose the digital evidence while processing paperwork.

171 It has to be pointed out that, however powerful Article 88ter BCCP seems at first sight, classical police work remains just as important. Without traces of login and passwords, for example discovered by a classical wiretap, a webmail account would not be accessible except if the law were to offer the legal possibility to "hack" the account.

172 In any case, the Belgian solution offers great opportunities to handle data stored in "the cloud". Companies and private persons are storing not only data but also processing systems in "the cloud", and by consequence do not themselves know where the data is stored exactly or in which State data is stored. Thus, the Belgian solution makes clear that it is not important to know where the data is stored, but from where it is accessible.

### 4.2.2 Netherlands

#### 4.2.2.1 **Legal situation in the Netherlands**

173 When it comes to searches for investigative reasons, articles 125 i, j and o and 126 l and m of the Dutch Code of Penal Procedure (CPP) are the most relevant provisions. They were drafted to conform to the Budapest Convention and were enacted in 2006. Articles 125 j and 126 l are particularly important. Article 125 j states that in case of a search (of a house or office)[82] it is possible to search computers present on that location, when the warrant allows that much. Searches must be done on location. Network searches or continued searches are also allowed (within certain limits), as far as it is granted by the rightful owner. Otherwise, the examining judge can order the passwords to be given (except for the suspect who is not obliged to incriminate himself). Still, article 126 l allows – within certain parameters – to record confidential information that is "communicated" through a computer linked to a network. Obviously, this power cannot be used for tracing "stored" information. Consequently and

[82] Searches are only allowed for certain serious crimes (carrying high maximum prison sentences).

concretely, it is assumed that this investigative power cannot be used, for example to obtain information about a password needed for gaining access to encrypted data.

174 For searches to continue on systems outside the Netherlands, the explanatory note of the Dutch Cyber Crime Act explicitly stipulates that this is "not" allowed; this can only be done through methods of public international law. In practical terms, law enforcement should resort to mutual legal assistance.

175 Article 24 of the Intelligence and Security Act allows for far larger powers to be applied in order to gain access to a computer in order to obtain information stored in it.[83] However, the information gathered from these searches cannot be used in a criminal case. Nothing is said about the possibility to conduct these searches cross-border.

#### 4.2.2.2 **The need to enhance investigations - perspective of Dutch Prosecution and Police**

176 In the Netherlands, a prosecutor is in charge of the investigation of a crime. In order to expedite and to enhance the effectiveness of cybercrime investigations the Dutch Prosecutor's office, both in their regular contacts with the Ministry of Security and Justice and publicly via media, has called for more investigative powers and the possibility to use them cross-border.

177 This call is based on several grounds. The prosecutor's office and the police observe the overall noted trend of the evolving digital society. More and more data are saved, processed and transferred. Different computer devices are simultaneously or successively used by the same person (stand alone, network, laptop with Wi-Fi and other mobile devices such as tablets and smartphones). More and more use is made of web-based services and thus of cloud computing. More and more computers of innocent civilians are compromised by malware and form a part of massive botnets threatening both personal users and businesses as well as national infrastructure. Computer users, including cybercriminals, have become experienced in encrypting their data and are "masters" in "going dark" on the net (anonymous surfing by using "foreign IP addresses", proxies, The Onion Router - TOR). It has become increasingly difficult to get a hold on data for the use as evidence or as "leads" for investigation. This is true for "domestic" cybercriminals, who target victims in the Netherlands or abroad, using "foreign IP addresses" or proxies and TOR, and is true for "foreign" cybercriminals that target victims in the Netherlands or use the Dutch IT infrastructure. Cybercrime is by nature borderless.

178 The prosecutors and the police are in need of access to:

- Computer data:
  - E.g. building up a collection of child abuse images in [encrypted] containers on a computer or on a data carrier;
  - Encrypted collection of passwords, information on personal financial accounts, that were hacked or phished
  - Planning of (e.g.) sabotage recorded in computer programs (MS or Apple);
  - Forging of financial book keeping in software.

[83] Article 24, among other things, states that "services are empowered to gain access to a computer whether it be by making use of technical appliances, false signals, false keys, by have an agent impersonating someone he isn't ." Intelligence services have to power to break any security system i.e. by using any technical facility to intercept passwords in order to gain access to encrypted information.

- Traffic data:
  - Use of new messaging techniques (e.g. blackberry messenger) instead of texting or calling via mobile phone;
  - Downloading data from www.

179 The Dutch Prosecutor's office has launched suggestions of law reform, such as the power to conduct "online searches" and to "counterhack" computer systems from which a cybercrime (DDOS attack, hack, infection with malware) originates. These techniques include the digital entering from a distance of computers, in order to install key loggers, or to look into data or even copy them, without the knowledge of the owner. The media and academia also point at the use of "police spyware" (be it Bundestrojaner or something else). The Dutch Prosecutor's office explicitly points at the fact that such changes in domestic law will only be effective if there is an international agreement to use such powers cross-border.

180 In practice (see below), there have been several operations in which the Dutch Prosecutor's office and the police have tried to conduct innovative investigations cross-border within the existing legal framework. Their call for better and enhanced national and international legal frameworks, however, remains.

#### 4.2.2.3 **Legal practice – the Bredolab case**

181 The Bredolab case, concluded in 2010, resulted in the takedown of a large botnet that made use of at least 143 servers hosted by a provider in the Netherlands. Its origins and much of its bots, however, were foreign. This botnet had infected more than 30 million computers. What was unique to the case was that Dutch law enforcement took over the botnet and informed – by sending a text message – every infected computer that it was infected by this botnet, and in the end shut down the servers in use by the botnet. Even if the magistrate consented to it beforehand, whether this action is allowed under Dutch law remains questionable as the message sent by Dutch police may be considered an illegal access to a computer.

#### 4.2.2.4 **Legal practice – the Descartes case**

182 In the Descartes case, a child pornography case that is still running, the magistrate allowed for a search of so-called TOR (The Onion Router) servers that were known not to be located in the Netherlands (but probably the USA). On these servers, there were very violent child abuse images. Via a bulletin board on the servers it was even possible to "order" the execution of sexual child abuse and the recording of the abuse in images. Digital copies of the incriminating information to be used in the criminal case later on were made in the process of search and seizure of the TOR servers, and the data on the servers were destroyed. Furthermore, in conformity with Dutch law (article 125 o CPP), access was blocked so that no future access could be obtained to the information, which in fact constituted a criminal offence in the Netherlands (article 240 b CCP on child pornography).

183 The investigation contains two risks that may relate to article 32b of the Budapest Convention. This includes a possible breach of the sovereignty of other countries and the fact that the information on the servers – which in fact constitute a criminal offence according to Dutch law – was made inaccessible.

184 As to the issue of sovereignty, Dutch law enforcement authorities sought close cooperation with the USA, as it was thought that the servers containing the criminal information were located in that country. Information copied was shared with US law enforcement.

185 As to the question of making the criminal information inaccessible, a Dutch judge agreed to this action beforehand. Moreover, persons trying to gain access to the information – and thus failing to do so – were notified by a message by the Dutch law enforcement authorities stating that the information they were trying to seek constitutes a criminal offence in the Netherlands and was, consequently, made inaccessible.

#### 4.2.2.5 Legal practice – using a webmail access to read e-mails hosted by a foreign service provider

186 In this case from 2009, a Dutch prosecutor issued a production order to a foreign service provider requesting email data related to a specific email account. The prosecutor had acquired via an "informant" the username, login and password of an e-mail account in which e-mails were present containing information on drug trafficking to the Netherlands. Apparently the response of the service provider took too long and the prosecutor instructed the police to access the email account via "webmail". From the thus acquired emails, it could be deducted that drugs were to be smuggled via Rotterdam port. Subsequently, a Dutch suspect was arrested. During his trial the (lower) court ruled that the policeman was not allowed to enter the email account without consent of the rightful owner. Secondly, the court ruled that extraterritorial execution of this power was also not allowed. The appeal court ruled against the lower court's decision. Since the email account did not belong to the suspect, the rights of that suspect were not violated ("Schutznorm"). A reduction of sentence of that suspect was therefore overruled. One might argue that the access to the email account was considered justified.

#### 4.2.2.6 Dutch views on safeguards for investigative powers in the digital world

187 The Ministry of Security and Justice adheres to a Dutch parliamentary decision named "Motie Franken". This decision stipulates the following criteria for the justification of breaches of privacy:

- Necessity, effectiveness and feasibility of the measure
- Proportionality of the breach
- An assessment beforehand on the risk's that such a measure constitutes
- Appropriate and independent control of the measure.

188 Concerning the last criteria, Dutch legal practice in similar situations uses extra criteria, such as:

- Measure is to be enacted by law
- Approval beforehand by a magistrate
- Transparency by notification as soon as possible to the Party / State involved
- Transparency by logging all actions by law enforcement.

### 4.2.3 Norway

189 The Norwegian Criminal Procedure Act from 1981 regulates when and how law enforcement agencies may get access to evidence, including electronic evidence. The provisions are general, and electronic evidence as such is not regulated specifically, apart from a few specific provisions in the Electronic Communications Act Section 2-9 that states that law enforcement agencies may get customer information directly from the service provider, without a court order.

190 As of now, there is no available Norwegian case law regarding the use of data acquired by transborder access as criminal evidence.

191 According to Norwegian legal theory,[84] Norwegian law enforcement may access electronically stored data in the same way as the account owner legally could, as long as there is a valid search warrant, and as long as the user name and access codes are available.

192 No statistics are available as to how often this is done. Based on general experience, the typical case of access to data stored in other countries concerns email and social media, and is based on consent by the suspect in accordance with Article 32 of the Budapest Convention.

193 A smaller number of cases concerns situations where the account is open, typically data available via a smartphone. These investigations may start with a police response to suspicious activity. A few years ago, the data in question would have been stored only on the mobile phone handset. With smartphones, more data is stored via "always on" cloud solutions. In a few cases, the suspect may have written down the password and the username for the service on a piece of paper which is located during a search.

194 In one case, the police had issued a search warrant against the Norwegian branch of a company that did business in Norway. During the search, it was discovered that the company did not store any data in Norway; all the business files were stored in a third State and accessed via thin clients. The terminals were switched on when the police arrived. Due to technical limitations, it was not possible to secure the data in question in or from Norway (a part from a few paper printouts), but according to Norwegian legal theory, it would have been legal to access and secure the data in question, and the data could then be used as evidence in the criminal case.

195 In other cases, the investigation is based on requests for expedited preservation and later requests for mutual legal assistance, for example to obtain content data from social media or webmail providers. In one case, anonymous third parties had broken into one of the email accounts of a suspect, stored all available email and gave this to the police. The police did not use this data as evidence in the case, but requested legal assistance from the police in the State where the email provider had their head office, to get the emails and related data in question. In this case, it was clear that the files would be used as evidence, and not just as background material. It was also – obviously – necessary to have the data verified by the data provider.

### 4.2.4 Portugal

#### 4.2.4.1 The legal framework and its scope

196 The Portuguese Law on Cybercrime (Law nº 109/2009, from 15 September 2009) contains rules describing so-called "cybercrimes" and also rules regarding the obtaining of electronic evidence. In general terms it can be said that the structure and the content of the law follows very closely the structure and the content of the Budapest Convention.

197 According to Article 11 of the Law on Cybercrime, most of the procedural provisions shall apply also, in addition to investigations of the crimes described under that Law, to offences "committed by means of a computer system" and to offences which investigation requires "to collect evidence in electronic form". This was inspired by Article 14.2 of the Budapest Convention. The exceptions of this extension are the interception of communications and undercover investigations, which are submitted to the general rules, but can also be used in investigations of crimes described under this law.

[84] "Lov og rett i cyberspace", Inger Marie Sunde, 2006, p. 274

#### 4.2.4.2 **Transborder searches**

198 Transborder access to data is allowed, under the Law on Cybercrime, in the context of the search of computer data. Rules on searches are inspired, both by the Portuguese Penal Procedural Code and the Budapest Convention, and they are described mostly in Article 15 of the Law on Cybercrime. According to Article 15.1, the judicial authority can authorize a search in a computer system, when, during the proceedings, it is necessary for the gathering of evidence, in order to ascertain the truth, to obtain certain and specific data stored in a given system.

199 Moreover, Article 15.5, states that when, during a of search, there are reasons to believe that the information sought is stored in another computer system or in a different part of the previous system, but that these data are lawfully accessible from the initial system, the search can be extended by authorisation of the competent authority. The text of the article does not establish any "geographic" or jurisdictional limits to this procedural tool. Thus, this extension applies both to remote systems located within Portuguese borders or outside them.

200 In practical terms, this extension, described under Article 15, can apply to searches of large systems (for example, searches within a system of a large company), when it is discovered that the required data are physically stored in a distant location. Or it applies also to access to webmail accounts. In both cases, it is possible to access systems physically located inside or outside Portuguese territory. Of course, this legal possibility depends on the fact that the access to the original system is lawfully authorised.

201 This provision clearly transposes to Portuguese internal law the content of Article 19.2 of the Budapest Convention, which requires each Party to the Convention to adopt the necessary measures to ensure that, within a computer search, this search can be extend to other computer system, if there are reasons to believe that the data sought are stored in that computer system – of course, if those data are lawfully accessible from the initial system. However, Article 19.2 only creates the obligation for Parties to extend the search to data stored in the territory of that Party.

202 On this particular point, the Portuguese legal framework goes beyond the requirements of the Budapest Convention: Article 15.5 of the Law on Cybercrime does not establish any difference between extensions of searches to "national" systems and systems physically located outside Portuguese territory. Thus, it is legitimate for a Portuguese law enforcement officer, to access data physically stored in a remote system, in a foreign State, if a proper order (normally from the prosecutor, but in certain cases from the judge – as described under Article 15.1 and 15.6) was duly obtained.

203 Regarding the validity of the evidence obtained by such a process, in the absence of a specific regulation, the general rule of Article 125 of the Portuguese Code of Criminal Procedure applies. Article 125 states that all the evidence that is not forbidden by law is admissible.

204 As mentioned before, it is allowed, in internal investigations, to access data physically stored in any other jurisdiction, by means of extending a search. And this procedural possibility is also legitimate when a law enforcement agent from another State accesses data physically stored in the Portuguese territory. In such a case, Article 25 of the Law on Cybercrime states that the

> competent foreign authorities may, without prior authorisation from the Portuguese authorities, access data stored in a computer system physically located in Portugal. This is allowed when the data are publicly available (Article 25 littera a) and also when it was obtained, by the authorities

of that state, the legal and voluntary consent of the person legally authorized to disclose the data (Article 25b).

205 This provision transposes to the Portuguese internal law the content of Article 32 of the Budapest Convention.

206 The definition of "computer system", under Portuguese law, is very broad. According to Article 2a of the Law on Cybercrime, "computer system" means any device or set of connected or related devices, in which one or more of them runs software or develops automated processing of data. This enlarged definition amplifies also the possibilities for extending searches.

#### 4.2.4.3 **Transborder seizure of data**

207 Another aspect is the regulation of seizure of computer data. In general terms, according to Portuguese Code of Criminal Procedure, seizure is a procedural measure used to secure evidence of a crime or to freeze or confiscate the proceeds of a crime. The Law on Cybercrime describes specifically the seizure of computer data under Article 16. This relates to the transborder access to computer data.

208 In fact, by its nature, a search is a procedural measure the final goal of which is the seizure of evidence or proceeds of crime. Thus, any search of computer systems has also, as objective, the seizure of data.

209 On the other hand, seizure can also be executed without a search if, for any reason, the authorities believe that there is a need to secure evidence or proceeds of a crime. It will be the case in the digital environment, for example, with any voluntary consent to access a system. This voluntary consent will exist if the owner of the system or the person legally authorised to consent to the access to a system authorises the law enforcement agents to do it. According to Portuguese law this applies to systems physically located within the Portuguese borders or outside them, if the access to those systems is lawfully authorised. Once access has been obtained, the seizure can be executed.

210 By this mechanism, Portuguese legislation adopts, with respect to its internal criminal investigations, the content of Article 32b of the Budapest Convention.

211 This procedural measure requires an order issued by the prosecutor – or in special cases, for example in case of seizures of email messages, approval by a judge (Article 17 of the Law on Cybercrime). The intervention of a judge is always required in cases of seizure of computer data or computer documents where content is likely to disclose personal or intimate information, that would jeopardize the privacy of its owner or a third party.

212 According to Article 16, 7 of the Portuguese Law on Cybercrime, seizure of data may take different forms. It can be made physically, seizing the physical device where the data are stored, or by copying of the data, or by preservation of the integrity of those data (without copying or removing) and, finally, it can be made by removing in a non-reversible way or by blocking access to the data.

213 According to Portuguese law, "computer data" is broadly defined and means any representation of facts, information or concepts in a format capable of being processed by means of a computer system, including programmes able to make a computer system to perform a function.

### 4.2.5 Romania

#### 4.2.5.1 **Legal basis**

214 Romanian law distinguishes between computer search and the access to a computer system. While the computer search[85] is performed in the presence of the defendant and his lawyer, if possible, the access to a computer system is considered a special mean of investigation, similar to the interception of a communication, and can be executed covertly.

215 Article 57 of Law no. 161/2003 assimilates access to a computer system to the interception or recording of communications. This measure requires a court order. Conditions are:

- the measure is necessary to find the truth
- the facts or identification or localization of the perpetrators cannot be achieved on the basis of other evidence
- it relates to serious crime.[86]

216 In urgent cases, for example if obtaining a court order would much delay the criminal pursuit, the prosecutor may order for a 48 hours period the interception of any communication or the access to a computer system. The provisional ordinance issued by the prosecutor has to be presented within 48 hours after its expiration to the court for validation. The judge may or may not agree the prosecutor's decision regarding the emergency. If the judge agrees, a new authorization is issued for 28 days. If not, the ordinance is dismissed and the materials obtained are to be destroyed.

#### 4.2.5.2 **Practice**

217 The procedural law applies with regard to a territory, a person and in relation to a certain offence. When asserting jurisdiction, a prosecutor will consider substantive jurisdiction (offence, national or foreign perpetrator operating at domestic level or abroad, etc.) as well as territorial jurisdiction according to the administrative division within Romania or based on the residence of the perpetrator if the offence was committed abroad.

218 With respect to interception and recording of a telephone conversation or communication by other means, if such a request made by the prosecutor is granted, the order could foresee:

- the interception and recording of a communication terminal (IMEI) using a Romanian identification number (IMSI) operating within Romania or in roaming (voice/data)
- the interception and recording of a communication terminal (IMEI) using a foreign identification number (IMSI) operating in roaming in Romania (voice/data)
- the access to a computer system if the connection to that computer can be established from Romania using national or interconnected networks (roaming principle applies; the main service is provided from Romania or from abroad but is interconnected with the national network, meaning the service is available from Romania.

[85] Some of the conditions set forth for house searches are applicable for computer searches as well (article 100 and the following from RCPC).

[86] "Serious offence" is defined by Law no.39/2003, Article 2 littera b, in the form of a list of offences. Point 20 of this list indicates as serious offence any other offence for which the law stipulates the punishment of prison whose specific minimum is at least 5 years. Point 18 nominates as being serious crime offences committed through digital or communication systems and networks.

219 The order is executed within Romania by the prosecutor or the police with the technical help of a special unit or the provider of the service located in Romania.

220 When the measure cannot be technically executed within Romania, the order will be subject to a rogatory letter that will be sent to the competent judicial authority where its execution can be properly handled.

### 4.2.6 Serbia

#### 4.2.6.1 **Legal Framework**

221 In Serbia, the Law on the Organization and Competences of Government Authorities for Combating Cybercrime was adopted by the National Assembly in June 2005, resulting in the creation of specialised authorities within the Ministry of Interior, the public prosecution and the judiciary. The first authority to be established was the Special Public Prosecution Office for High-Tech Crime in early 2006 followed by the Special Department for High-Tech Crime within the Special Service for Combating Organised Crime of Ministry of Interior and special investigative and trial departments of the Higher Court in Belgrade. These authorities have nationwide competence for combating criminal cases as stipulated by Article 3 of this Law.

222 In addition to this Law, provisions of other laws also apply with regard to cybercrime, such as of the Criminal Code, Law on Public Prosecution, existing Criminal Procedural Code, Law on Electronic Communications, Law on International Legal Assistance in Criminal Matters and others.

223 With regard to access to computer data during pre-criminal or criminal proceedings aforementioned authorities are obliged to follow definitions and the criminal procedure envisaged by the Criminal Code and Criminal Procedural Code where movables are also defined as including computer data and computer programmes. The Serbian CPC is very clear with regard to the search and seizure of premises and objects related to the execution of a criminal act: searches of the above and other premises of accused persons or other persons may be conducted only where it is probable that the search will lead to the capture of the accused person or the detection of evidence of a criminal offence or objects of importance for criminal proceedings.

224 Searches shall be ordered by a court by way of a written and substantiated search warrant. Objects which must be seized under the Criminal Code, or which may serve as evidence in criminal proceedings, shall be seized and placed with the court for safekeeping, or their safekeeping will be secured in another way.

225 The Serbian CPC, in the current version, envisages special investigative techniques which can be used for access to the computer and related data, such as supervision and recording of telephone and other communications by other technical means and automated computer searches of personal and other data and related data. The new version of the CPC (which is already being used by the Organized Crime and War Crimes Prosecution Offices) envisages even more investigative techniques and measures at the disposal to LEA and Public Prosecution in order to gain access to computer data in related to criminal acts.

226 The Serbian CPC recognises computer data as such and does not makes a difference between data which is present in computers and computer systems in Serbia or abroad if that data will lead to the detection of the evidence of a criminal offence or represents the objects in electronic

form which will be of the importance for the criminal procedure provided that other requirements for search and seizure of the CPC are fulfilled as long as that perpetrator of the criminal act can be prosecuted under the provisions of the Criminal Code and Criminal Procedural Code of Serbia.

227 Provisions of the Electronic Communications Law are in addition regulating the confidentiality of the electronic communications, lawful interception and data retention. Very important obligations of Internet service providers are stipulated by this Law which facilitates reliable access to data during criminal proceedings.

#### 4.2.6.2 **Transborder access in practice**

228 Transborder access is possible in different situations and is carried out by the Special Department for High-Tech Crime, that is, transborder access during the search of premises, transborder access through lawfully obtained passwords, transborder access with consent, information provided by a service provider, with the exception of transborder access through special software or technical means.

229 Transborder access through lawfully obtained password and transborder access with the consent are the ones most often applied in practice by Serbian LEA. This practice has not been challenged so far.

230 One of the main underlying assumptions is that while the initial computer inquiry may happen on a server or system potentially abroad, the actual presentation and access to the data themselves represents an access to packages of computer data which have been transferred to the computer on the premises of the perpetrator in Serbia. Data are thus temporarily or permanently stored within the territorial jurisdiction of the Serbian authorities.

### 4.2.7 USA

231 Investigators and prosecutors in the United States use narrowly defined legal and procedural authorities to reach outside of US territory to obtain stored computer data. In practice, these laws and procedures significantly limit transborder access by US law enforcement officials.

232 Most frequently, US law enforcement officials obtain computer data stored in another State by collaborating with the Government of that State. The mechanisms for obtaining this evidence are generally through mutual legal assistance requests or letters rogatory, or by way of joint efforts involving law enforcement officials of both States. These collaborative means of transborder access provide US investigators and prosecutors with nearly all of the data, especially stored content, obtained from other States.

233 United States law enforcement officials also collect data stored abroad using methods set forth in Article 32 of the Convention on Cybercrime. A common investigative practice in the US is to access data publicly available on the Internet, regardless of the location of the website, the website hosting service, or the person[87] that owns or controls the data. This practice is regulated by the general laws applicable to criminal investigations, including Constitutional protections of individual rights, the federal criminal code and rules of procedure,[88] and judicial decisions that interpret these laws. In addition, the US Department of Justice and other law enforcement entities promulgate specific guidance for online investigations.

[87] In this section, "persons" refers to natural persons and legal persons.

[88] United States Code, Title 18, *Crimes and Criminal Procedures*.

234 Another practice of US investigators is to access data located in a computer in another State after obtaining the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer. Most often this type of transborder access occurs when an investigator obtains consent from an individual or business located in the US but controlling data related to the investigation stored in another State. Generally, the investigator and the person who owns or controls the data work together to access and retrieve the data. As with access to publicly available data, US laws and procedures govern this practice, with significant judicial interpretation of the nature and scope of voluntary consent. Article 32 of the Convention on Cybercrime also provides a basis for this practice. However, US laws limit the ability of third parties to voluntarily disclose data to the government.[89] When US law prohibits voluntary disclosure, consensual transborder access is not available to US investigators because the person (such as a service provider) does not have authority to disclose the data, no matter where it is stored.

235 Article 18 of the Convention on Cybercrime and US law permit the government to seek, through the issuance of an appropriate order, the disclosure of data stored in another State that is related to the investigation and controlled by a person or entity physically present located in the US. The strong preference of the US government is to collaborate with other States to obtain data stored abroad, when practicable. Thus, the US Department of Justice requires prosecutors to obtain the approval of a high-ranking Department of Justice official before seeking an order compelling the production of such data. The issue of when a person present in a jurisdiction can be compelled to produce data that is in its possession or control — but which is stored in another jurisdiction — long predates not only the convention but computers themselves. As a result, the US has controlled such law enforcement requests since long before the advent of the Internet.

236 United States law enforcement officials may infrequently engage in other transborder access, particularly in situations in which the location of the stored data is not known or investigators do not anticipate that a search would extend beyond US territory. Article 39 of the Convention on Cybercrime (together with Explanatory Memorandum paragraphs 293 and 314) provides that any transborder search scenarios that may arise beyond those governed by Articles 18 and 32 are neither specifically authorised nor precluded.

[89] For example, see the Stored Communications Act (codified at United States Code, Title 18, Sections 2701-2712); the Right to Financial Privacy Act (codified at United States Code, Title 12, Sections 3401-3422); and the privacy rule of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191 and United States Code of Federal Regulations, Title 45, Parts 160 and 164).

## 4.3 Access via providers and other private sector entities

### 4.3.1 Practices

237 The previous sections described scenarios whereby LEA primarily access stored computer data directly transborder. It would seem, however, that the more frequent scenario is that LEA cooperate with service providers or other private sector entities to obtain access to data stored abroad.

238 As indicated earlier in this report, Article 32b does not exclude that the person providing "lawful and voluntary consent" to disclose data is a private sector entity controlling data.

239 For example, in some European States, a number of US-based service providers with branch offices in Europe have made voluntary arrangements ("criminal compliance programmes") between their European offices and the LEA of specific European governments, to disclose data under certain conditions and without requiring these European LEA to go through a mutual legal assistance procedure via the US Department of Justice. Conditions for voluntary compliance with requests may typically include:

- The request would need to be lawful and come from a competent authority that has jurisdiction over the case being investigated; a clear legal framework for the investigation of cybercrime and the collection of electronic evidence is to be in place
- The data requested may need to be related to the territory of the requesting LEA (such as IP addresses of a communication, the country top-level domain of a webmail account or similar)
- The conduct investigated would also constitute an offence in the USA (a type of dual criminality principle to exclude political offences or free speech-related investigations)
- In most cased, only data owned and controlled by providers – such as traffic data and subscriber information – would be disclosed but not content generated by users (for content an MLA request through official channels would be required)[90]
- The criminal justice system of the State is trusted to respect international human rights and rule of law standards, including the protection of privacy.

240 Private sector entities may also be formally requested to comply with search, seizure and production orders under the laws of the States in which they operate.[91]

241 The requirement to comply with such judicial orders may fall under domestic powers in line with Articles 18 and 19 Budapest Convention but would not represent "voluntary consent" in the sense of Article 32b.

242 It is understood that private sector entities operating in different countries are subject to the laws of multiple jurisdictions, and that compliance with legislation in one country may bring them in conflict with that of others. This includes in particular conflicts with human rights and rule of law principles.

---

[90] It appears that some providers may also disclose content if a formal judicial order is issued and if the user has registered under the terms and conditions in the state of the requesting LEA.

[91] Such formal requests are not covered by Article 32 Budapest Convention but provisions on domestic powers, such as search and seizure (Article 19) or production orders (Article 18) – if the request is related to a criminal investigation. A major concern seems to be that requests for data may be issued under laws related to intelligence or national security under which rule of law and human rights safeguards are limited.

### 4.3.2 Concerns

243 Concerns have been expressed by a number of stakeholders such as the following.[92]

#### 4.3.2.1 **Global Network Initiative**

244 The GNI summarises the problem as follows:

> All over the world – from the Americas to Europe to the Middle East to Africa and Asia – companies in the Information & Communications Technology (ICT) sector face increasing government pressure to comply with domestic laws and policies in ways that may conflict with the internationally recognized human rights of freedom of expression and privacy.[93]

245 A set of principles has been adopted by GNI that companies should follow to protect freedom of expression and privacy.

246 Recently proposals were made that for requests for data stored in servers abroad, a mutual legal assistance procedure should always be followed.[94]

#### 4.3.2.2 **Policy statement of the International Chamber of Commerce (ICC)**

247 The International Chamber of Commerce (ICC) in 2012 issued a policy statement noting that:

> Companies processing data in multiple countries face increasing government pressure to comply with law enforcement and other regulatory requests for access to personal data that conflict with data protection and privacy laws in other countries in which they operate[95].

248 Example given by the ICC:

> Example 1: Company X does business in many countries, including Country A, a country that lacks sufficient legal protections for personal data. It transfers personal data regarding transactions from countries all over the world to its central database located at its headquarters in Country B. Company X has taken the necessary steps so that its data processing activities are valid under the legal requirements of the countries where it does business. These legal requirements include that Company X will only process data for purposes defined at the time of collection; that it will provide a legal basis for onward transfers of the data to third parties; and that it will only transfer the data to third parties if steps are taken to provide adequate protection in the country to which the data are transferred. In addition, the consumer privacy policy of Company X states that it will use personal data only for limited specified purposes and provide adequate protection for onward transfers of personal data.

---

[92] These concerns are listed here for further discussion. They do not necessarily reflect the views of the Transborder Group.

[93] http://www.globalnetworkinitiative.org/

[94] Brown, Ian/Korff, Douwe (2012): Digital Freedoms in International Law – Steps to Protect Human Rights Online (report prepared for the Global Network Initiative, GNI) https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

[95] ICC Policy Statement: "Cross-border law enforcement access to company data – current issues under data protection and privacy law" (February 2012), available at http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-policy-statement-on-cross-border-law-enforcement-access-to-company-data---current-issues-under-data-protection-and-privacy-law/

Law enforcement authorities in Country A approach Company X stating that they have suspicions that certain individuals with which Company X has transacted business may be involved in illegal activities. The individuals are citizens of multiple countries, including those of Country A. These authorities then request Company X to turn over to them all records Company X holds involving transactions with such individuals over the last three years, including those stored at its database in Country B. The request is not based on a judicial order, and does not list any further details beyond the names of the individuals and the timeframe in which the relevant transactions took place. The authorities state that if this request is not complied with, they will initiate criminal proceedings against the management board of Company X's subsidiary in Country A.

249 According to the ICC, such pressure may lead to conflicts with privacy and data protection laws, to a violation of commitments to individuals, employees and customers, risks of political tensions and impact on business decisions.

250 ICC therefore "urges law enforcement authorities and governments to take the following actions":

- Take into account the possibility that law enforcement requests may violate the data protection or privacy law of other countries.
- Make requests for access to data only in writing and in accordance with written law and/or local regulation, rather than through informal requests. State clearly in any request the specific legal basis for it and the name of the requesting responsible authority.
- Make cross-border requests for data stored in another country through mutual legal assistance treaties and procedures (MLATs) within existing frameworks, ensuring appropriate involvement of authorities in the countr(ies) where data are stored. Improvements should also be made to existing MLATs so that they (1) cover evolving IP-based communications services; (2) deliver requested data in timeframes satisfactory for law enforcement authorities; (3) increase legal certainty for compliance with respective national laws; (4) give companies sufficient information to interact with the MLAT process in an efficient manner; and (5) create a single point of contact with law enforcement authorities in each country.
- Give companies the opportunity to ascertain the legitimacy of the request and inform the authorities (including their own national authorities) about their obligations under data protection and privacy law, when this is required.
- Be as specific and concise as possible about the scope of the request (such as which data the authority is seeking and for which timeframe), and minimize the amount of data requested.
- Avoid developing mechanisms that compel companies to enter into supposedly "voluntary" agreements to deliver up information under threat of significant, penal, financial, or tax sanctions or local business suspension if they do not.
- Allow companies to limit potential liability, for example by anonymizing or shielding personal data of third parties that are not under investigation.

Implementation of these recommendations would allow more efficient compliance with legitimate public and law enforcement requests, better allow companies to cope with conflicting legal obligations, promote compliance with data protection and privacy laws, and strengthen the flow of international commerce by giving companies the increased legal security they need to plan investments.

#### 4.3.2.3 **White Paper on governmental access to data in the cloud**[96]

251 According to this "Hogan Lovells White Paper"[97] many governments can request cloud providers in their territory to provide information stored on servers on foreign territories:

- Australia: Requests for data issued to Australian companies and organizations extend to data held in cloud servers located outside of Australia, provided that the suspected criminal offense or security matter that is the subject of the warrant occurred wholly or partly in Australia or concerns persons who are Australian citizens or residents. Therefore, the Australian government can require a cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

- Canadian requests for data are not limited to data located in Canada. Generally, a company subject to Canadian jurisdiction must turn over any relevant data over which it has "custody or control," either because it can access the data itself or because it can cause a third party, such as a subsidiary corporation, to access or obtain the data. Therefore, the Canadian government can require a cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

- Denmark: If a Danish cloud service provider stores customer data on servers located in another State, the government can access data located on those servers with a search warrant, provided that the data can be reached and searched from the site of the Denmark-based provider. Otherwise, the extent to which the Danish government may access data on servers located in other countries depends on the level of judicial cooperation between the concerned States.

- France: French law expressly permits governmental authorities to obtain all information relevant to an investigation from a computer system so long as the data are accessible from that computer system. Therefore, the French government can require a cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

- Germany and Japan: It is not possible to access data abroad.

- Ireland: So long as there is an entity in Ireland over which the Irish government can assert jurisdiction, Irish authorities can require the entity to produce customer data from a cloud server located in another State but under the entity's control. Therefore, the Irish government can require a cloud service provider to obtain data from both domestic and foreign servers through the preceding legal mechanisms.

- UK: Where British governmental authorities have a warrant or order to obtain electronic data, they have the power to require the search of any information contained in the computer and accessible from the premises. In other words, as long as foreign

---

[96] Maxwell, Winston/Wolf, Christopher (2012): A Global Reality: Governmental Access to Data in the Cloud (Hogan Lovells White Paper, 23 May 2012) http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf

[97] Winston Maxwell, the co-author of the paper, participated in the Octopus Conference (workshop on transborder access to data) in June 2012. Participants in that workshop wished to underline that the White Paper does not necessarily reflect the views of the relevant authorities of the States mentioned in the report.

cloud servers can be accessed from premises in the UK, the police could require the cloud service provider to also turn over data located on the foreign servers.

- USA: The United States, like other countries, takes the position that it can use its own legal mechanisms to request data from any cloud server located anywhere around the world so long as the cloud service provider is subject to US jurisdiction — that is, when the entity is based in the United States, has a subsidiary or office in the United States, or otherwise conducts continuous and systematic business in the United States.

252 In discussions on this paper during the Octopus Conference in June 2012[98] some of its conclusions were found controversial and overstating LEA powers. It appears that in most States numerous conditions are to be met before LEA can order a private sector entity to produce data. This may include that the IP address is linked to or that the suspect is on the territory of the LEA or that the request is subject to judicial supervision and others.[99] It would be wrong to assume that there is unrestrained access.

[98] www.coe.int/octopus2012

[99] With regard to the USA, the paper overstates the US view of its criminal jurisdiction. All US federal prosecutors must apply in writing for approval to assert jurisdiction when the only tie to the US is a subsidiary or office in the US. *See* the US Attorneys' Manual, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm. Such applications and approvals are unusual.

# 5 Options regarding transborder access beyond 32b

253 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".

254 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.

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

255 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.[100]

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

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

257 Under this proposal, a new provision could be included in the Budapest Convention (by means of an additional Protocol)

> 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.

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

258 Under this proposal, a new provision could be included in 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.

259 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.

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

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

260 As discussed earlier in this report, 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[101], 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.

261 It may be conceivable to drop this limitation.[102] However, specific criteria as well as safeguards would need to be defined.

**Proposal 5: The power of disposal as connecting legal factor**[103]

262 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.

263 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".

264 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 State, the LEA of this State may be able search or otherwise access the data.

265 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 State, and thus avoid "hacking" by LEA into computer systems located in other States.

---

[101] Emphasis added.

[102] Some argue that an extension of a search may also cover situations comparable to a "hot pursuit". Within the European Union, physical "hot pursuits" are possible across land borders between the States participating in the Schengen Agreement for a list of serious offences.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:EN:PDF

[103] 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.

# 6 Options regarding the type of instrument

266 The Transborder Group discussed a number of options as to the type of instrument that could be developed. It also sought – via the Secretariat – advice from the Council of Europe's Jurisconsult.

## 6.1 Possible options

267 The following options could be considered:

### 6.1.1 Amendment of Article 32b of the Budapest Convention

268 Such an amendment would affect all present and future Parties. The two possibilities for amendments are:

- Simplified procedure for Amendments as foreseen in Article 44 of the Budapest Convention:

  Article 44 – Amendments

  1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

  2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

  3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

  4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

  5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

- An Amending Protocol that would be prepared within the institutional framework and under the usual rule of the Council of Europe for the preparation of treaties. An Amending Protocol would only enter into force once it has been ratified by all Parties.

269 The advantages are that all Parties are involved in the decision-making (as they all need to accept the Amendment), that the Convention remains coherent in that the Amendment applies to all present and future Parties and that it creates legal certainty in that it is binding upon all Parties.

270 The disadvantage is that it would only have legal effect once accepted by all Parties which may take many years.

### 6.1.2 A Recommendation of the Committee of Ministers

271 The Statute of the Council of Europe – in its Article 15 – foresees that the Committee of Ministers adopts Recommendations addressed to Council of Europe member States. Such Recommendations are soft-law instruments of the Council of Europe.

272 Non-member States that are Parties to the Budapest Convention could thus participate in the elaboration of a Recommendation concerning the Budapest Convention but not participate in the final decision-making. On the other hand member States that are not Parties to the Convention would participate in the decision-making.

273 If the Recommendation were to propose solutions to problems common to all member States independent of the Budapest Convention on Cybercrime, it could be a suitable instrument.

274 However, if it were to address issues specifically related to the Budapest Convention, a Recommendation would not seem suitable:

- Committee of Ministers Recommendations are addressed to member States only and thus not necessarily to all Parties of the Convention (non-member States would receive it for information)
- Parties that are non-member States would not take part in the adoption of the Recommendation by the Committee of Ministers
- It is questionable why the Committee of Ministers should – via a Recommendation – become involved in following a treaty like the Budapest Convention where such a role of the Committee of Ministers is not foreseen.

### 6.1.3 Additional Protocol to the Budapest Convention on Cybercrime

275 An Additional Protocol could be considered if the intention is to adopt measures beyond those already contained in the present Convention and its Protocol on Xenophobia and Racism (CETS 189), and if there is no requirement that all Parties necessarily need to accept such a Protocol through ratification or accession. It could enter into force once a certain number of Parties has accepted it (as was the case with the Protocol CETS 189).

276 An Additional Protocol thus allows for certain flexibility and relatively early entry into force. On the other hand, it would only be binding upon those Parties that have accepted it and it may thus reduce the coherence of the regime of the Budapest Convention. The question as to whether an Additional Protocol could effectively address the question of transborder access would depend on the contents of a such a Protocol.

### 6.1.4 Interpretation of the Convention

277 Under international law, the basic principle is that the Parties are responsible for the interpretation of the treaties to which they are Parties.[104] The Consultations of the Parties (Article 46 Budapest Convention), that is, the Cybercrime Convention Committee would be the forum to reach agreement on the interpretation of specific provisions of the Convention.

[104] Article 45 foresees that the European Committee on Crime Problems (CDPD) be kept informed of the interpretation and that Parties may also submit disputes to the CDPC.

278 Two types of instruments could be foreseen:

- A formal Agreement on Interpretation would be possible in line with Article 31.3.a of the Vienna Convention on the Law of Treaties.[105] Such an Agreement would have to be formally accepted by all Parties by unanimity. In practice, the procedure would be similar to that of an Amending Protocol (see above). Rather than an Agreement on Interpretation it may be more appropriate to pursue a simplified Amendment under Article 44.

- Guidelines or similar could be adopted by the T-CY and addressed to Parties of the Budapest Convention and their operational services in order to facilitate the application of certain provisions of the Convention. This appears to be frequent practice by Committees of the Council of Europe. Such Guidelines, however, are not binding upon State Parties. On the other hand, they can be effective if Parties form a "community of trust".

## 6.2 Options to be pursued

279 The Transborder Group is of the opinion that the following options should be pursued:

- A Guiding Note by the T-CY providing a better understanding of the current possibilities under the Budapest Convention for transborder access to data. Such a Guiding Note would need to be carefully considered by T-CY members, may require consultations with private sector and other stakeholders, but could come into effect within a short period of time.

- A Protocol on additional measures that are considered necessary based on practices already applied by a number of States and comprising conditions and safeguards. Such a Protocol will take time to negotiate and in particular to be ratified by a sufficient number of Parties to become effective.

280 Such a "dual" approach would help clarify matters regarding transborder access in the near-term while allowing for long-term solutions under international law. This approach seems justified given technological changes, increasing levels and complexity of transnational crime involving computer systems as well as diverging practices by States that access data transborder beyond the possibilities foreseen in the Budapest Convention. Careful consideration would need to be given to human rights and rule of law safeguards and to the legitimate rights and interests of individuals and third parties as well as legal and policy concerns of States.

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

# 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:

## 7.1 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 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.

## 7.2 Concerns

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

- Legal and police 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[106]
- 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.

## 7.3 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).[107]

---

[106] 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.

[107] 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.[108]

[108] Budapest Convention Explanatory Report, paragraph 293.

## 7.4 Practices[109]

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.

[109] 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.

## 7.5 Solutions proposed

### 7.5.1 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.

### 7.5.2 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.

### 7.5.3 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.

### 7.6 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.[110]

- 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.

---

[110] The draft Mandate would then be submitted to the Committee of Ministers via the European Committee on Crime Problems (CDPC) for approval.

# 8 Appendix

## 8.1 T-CY Guidance Note on transborder access (Article 32) – Draft Elements

### [Introduction

[The purpose of this Note is to provide guidance to Parties to the Budapest Convention on Cybercrime when applying Article 32 on transborder access to data.

[It reflects a common understanding of the T-CY.

[Other situations are neither authorised nor precluded.

### [Article 32 Budapest Convention

Text of the provision:

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
>
> a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
> b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Extract of the Explanatory Report:

> 293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.
>
> 294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in

another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

## [T-CY interpretation of Article 32

[With regard to Article 32a (transborder access to publicly available (open source) stored computer data) no specific issues have been raised and no further guidance by the T-CY is required at this point.

[With regard to Article 32b (transborder access with consent) the T-CY shares the following common understanding:

### [On the notion of "transborder" and "location

[Transborder access means to "unilaterally access computer data stored in another Party without seeking mutual assistance".[111]

[The measure can be applied between the Parties.

[Article 32b refers to "stored computer data located in another Party". This implies that Article 32b may be made use of if it is known where the data are located.

[Given that Article 32b does "neither authorise, nor preclude" other situations, in situations where it is unknown or not certain that data are stored in another Party, States may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.

### [On "consent"

[Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived. What constitutes consent is to be governed by the domestic law of the Party to whom consent is given, that is, the law of the Party seeking transborder access.

[As Article 32b relates to transborder access for the purposes of criminal investigations, consent should be explicit.

### [On the applicable law

[With regard to "lawful consent" and "lawfully authorised" to disclose data, for practical purposes "lawful" means the law of the searching Party as law enforcement authorities would normally act on the basis of the laws of their own State. In urgent situations of transborder access it would not be feasible that the searching law enforcement authority is able to verify the rules governing the use of the data in the other Party.

[However, if it is obvious that the disclosure or providing of access would violate the laws of the other Party or the rules on the use of the data, law enforcement authorities should be discouraged from pursuing transborder access.

[111] Paragraph 293 Explanatory Report to the Budapest Convention.

**[On the person who can provide access or disclose data**

[As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances and rules applicable.

[It may be a physical individual person providing access to his email account or other data that he stored abroad.

[The person providing access may also be an Internet or cloud service provider or another private sector entity holding data of an individual, for example, if the terms of service permit this or if the service provider has become the owner or has the power of disposal of the data. In this case, to be in line with Article 32b, a service provider would have to provide access voluntarily and lawfully, that is for example, without violating privacy or other rights. Therefore, this would usually only be possible for data owned by the private sector entity, such as traffic data, subscriber information or other network data, while it may not be possible to disclose content generated by users voluntarily and lawfully. A judicial order for the seizure or production of data would not fall under Article 32b.

**[On the location of the person consenting to provide access or disclose data**

[The standard hypothesis is that the person providing access is physically located on the territory of the requesting Party. In this situation, that person falls under the jurisdiction and is subject to the laws of the investigating State.

[However, multiple situations are possible. It is conceivable that the physical or legal person is located on the territory of the requesting law enforcement authority when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access. The person may also be physically located in a third country when agreeing to cooperate or when actually providing access. If the person is a legal person (such as a private sector entity), this person may be represented on the territory of the requesting law enforcement authority, the territory hosting the data or even a third country at the same time.

[It should be taken into account that many Parties would object – and some even consider it a criminal offence – if a person who is physically on their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation.

**[General considerations and safeguards**

[Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.[112]

[112] 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.

[It is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention. The rights of individuals and the interests of third Parties are to be taken into account when applying the measure.

[The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.

[….]

---

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.

## 8.2 Terms of reference of the Transborder Group[113]

The Cybercrime Convention Committee (T-CY),

Having regard to:

a. Article 46 (1) (a) and (c), of the Convention on Cybercrime (ETS No. 185);
b. the decision of the fifth meeting of the Cybercrime Convention Committee to instruct the Bureau to *"prepare terms of reference for its future standard-setting work on jurisdiction and transborder access to data and data flows and submit it to the Committee with a road map for implementation, at the earliest convenience"*.

Having considered that:

a. During the last 25 years, which includes the decade since the "birth" of the Budapest Cybercrime in 2001, there has been a significant evolution of information and communication technologies and specifically of the role of the Internet in our societies. We have moved from a real to a virtual or digital world which is borderless by nature. The development of ICT brings much positive innovation. At the same time, ICT have also become highly attractive to criminals. In general terms, criminality evolved from traditional crime with the aid of computers to high tech crime originating from and targeted at ICT. The internet provides criminals with a high degree of anonymity. The Internet allows criminals to target potential victims from anywhere in the world, and enables mass victimisation with relative ease. Attacks against "cloudstorage" systems of ISPs would affect computer data and systems of a large number of end-users.

b. Increasingly data is stored on computer systems in locations and jurisdictions other than the physical location of the suspect or of his or her computer. Often, the precise location of data stored in the "cloud" is unknown to law enforcement lawfully investigation an offence or even to the user. The evolution towards cloud computing thus impedes the securing of electronic evidence or the rapid pursuit and prosecution of offenders.

c. An important issue to be addressed is to find a proportional and practicable balance between privacy, data protection and other fundamental rights of users on the one hand and on the other hand the need for law enforcement action that is sufficiently efficient to allow criminal justice authorities to meet their obligation of protecting users.

d. Whilst cyberspace itself is borderless, the authority of law enforcement is in general bound to a specific jurisdiction. At the same time, trans-border investigations are necessary and are often carried out already. However, it is important to develop clearer rules as to what is and what is not allowed in each jurisdiction with regard to trans-border investigations and cross-border co-operation. This would enhance the effectiveness of the fight against cybercrime in line with human rights and rule of law principles.

e. The existing text of Article 32 of the Budapest Convention was a compromise solution adopted in 2001. At that time, there was a lack of concrete experience at the international level regarding such trans-border situations, and this prevented rules going further than the provision of Article 32 b. The wording of paragraph 293 of the explanatory report of the Convention makes it clear that Article 32 must be understood as a minimum text to which all parties, at the time, agreed. The Explanatory Report leaves it open to countries to go beyond this provision: "Other situations [than mentioned in article 32] are neither authorised, nor precluded." Article 39.3 of the

[113] Approved by the T-CY at its 6th session, 23-24 November 2011

Convention states that "Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party".

f. Reaching an agreement on additional procedures and powers allowing for more direct and effective trans-border investigations by law enforcement with the necessary conditions and safeguards is a major challenge. The Cybercrime Convention Committee is nevertheless prepared to address this challenge.

Has decided:

a. To set up, from among its members, an ad hoc sub-group to examine the following issues:

   i. the use of Article 32 (b), of the Convention on Cybercrime;
   ii. the use of transborder investigative measures on the Internet;
   iii. the challenges to transborder investigations on the Internet posed by applicable international law on jurisdiction and State sovereignty.

b. To instruct the ad hoc sub-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.

c. To instruct the ad hoc sub-group to take into account the questionnaire, replies and debates in T-CY plenary sessions since 2009.

d. To instruct the ad hoc sub-group to submit a report to the second T-CY plenary of 2012.

e. That the ad hoc sub-group shall be composed of no more than 10 members of the Committee with the necessary subject-matter expertise. The defrayal of expenses is subject to the availability of funds. The ad hoc group may draw upon external expertise.

f. To propose that the European Committee on Crime Problems (CDPC) may send a representative to meetings of the ad hoc sub-group, without the right to vote and at the charge of the corresponding Council of Europe budget sub-head.

g. That the Secretariat shall be provided by the Council of Europe.

h. That these Terms of Reference will expire on 31 December 2012.

## 8.3 References


Article 29 Data Protection Working Part (European Union) (2012): Opinion 05/2012 on Cloud Computing" (adopted 1 July 2012)
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Brown, Ian/Korff, Douwe (2012): Digital Freedoms in International Law – Steps to Protect Human Rights Online (report prepared for the Global Network Initiative, GNI)
https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

Council of Europe / European Committee on Crime Problems (1990): Computer-related crime (Final report on Recommendation (R(89)9 of the Committee of Ministers)
http://www.oas.org/juridico/english/89-9&final%20Report.pdf

Council of Europe / European Committee on Crime Problems (1990): Extraterritorial criminal jurisdiction.

Council of Europe / Committee of Ministers (1995): Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology"
http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp

Council of Europe / PC-OC Committee (2008): Replies on Mutual Legal Assistance in Computer-Related Cases / Réponses sur L'entraide judiciaire dans les affaires liées à l'informatique (PC-OC (2008) 08 rev)

Council of Europe / PC-OC Committee (2008) : Replies on Mutual Legal Assistance in Computer-Related Cases (Austria / France) / Réponses sur l'entraide judiciaire dans les affaires liées à l'informatique (Autriche / France) (Addendum to PC-OC (2008) 08 Rev)

Council of Europe / PC-OC Committee (2009): Summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases (PC-OC (2009) 05)

Council of Europe / Project CyberCrime@IPA (2012): Article 15 – Conditions and Safeguards under the Budapest Convention on Cybercrime (Discussion paper with contributions by Henrik Kaspersen, Joseph Schwerha and Drazen Dragicevic)
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

Council of Europe / T-CY Committee (2010): Transborder access to stored computer data (discussion paper December 2010)

Council of Europe / T-CY Committee (2010): Replies of the state parties to the draft questionnaire on the need for direct transborder access to data and data flows where other measures are not adequate or fail (T-CY (2010) 01)

Council of Europe / T-CY Committee (2010): Answers to questionnaire on the need for direct transborder access to data flows where other measures are not adequate or fail (T-CY (2010) 01 Addendum

Council of Europe / T-CY Committee (2010): Direct transfrontier access to data and dataflows under international law (Fifth meeting, Paris, 24 - 25 June 2010) (T-CY (2010) 05 Confidential)

Council of Europe / T-CY Committee (2011): Ad hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows: Draft Terms of Reference (T-CY (2011) 5 E

Court of New York (USA): US District Judge of New York, Post-indictment Protective Order (Nov 2011), US *v.* John Doe

European Court of Human Rights (2012): Extra-territorial jurisdiction of ECHR Member States – Factsheet
http://www.echr.coe.int/NR/rdonlyres/DD99396C-3853-448C-AFB4-67240B1B48AE/0/FICHES_Juridiction_Extraterritoriale_EN.pdf

G8 Justice and Interior Ministerial (October 1999): Principles on Transborder Access to Stored Computer Data
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf

IGP (USA): In Important Case, RIPE-NCC seeks legal clarity on how it responds to foreign court orders (John Doe *v.* Bootnet)
http://blog.internetgovernance.org/blog/_archives/2011/11/23/4944811.html

International Chamber of Commerce (ICC Commission on the Digital Economy) (2012): Cross-border law enforcement to company data – current issues under data protection and privacy law. Policy Statement. Document No. 373/507 – (7 February 2012)
http://www.iccwbo.org/uploadedFiles/Law_enforcement_access_to_company_data_final_20March12.pdf

ISS World Americas (2011) : Cloud Lawful Interception and Data Retention, including Lawful Interception as a Service (LIaaS), Data Retention as a Service (DRaaS), Law Enforcement Monitoring Facility as a Service (LEMFaaS), by Tony Rutkowski, VP, Yaana Technology

Kaspersen, Henrik (2009): Cybercrime and internet jurisdiction (Discussion Paper prepared for Council of Europe / Global Project on Cybercrime)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

Kromann Reumert Publication (2012): Government Access to Information in "the Cloud".
http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf

Lakatos, Alex (2012): The USA Patriot Act and the Privacy of Data Stored in the Cloud.
http://www.mayerbrown.com/files/Publication/ce02dec6-f143-46ec-a0a3-53c06d770707/Presentation/PublicationAttachment/f56ea23a-7fd4-40bb-9b78-57e0787774dc/12057.PDF

Maxwell, Winston/Wolf, Christopher (2012): A Global Reality: Governmental Access to Data in the Cloud (Hogan Lovells White Paper, 23 May 2012)
http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf

Microsoft (2010): Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing (Brad Smith, General Counsel)

Piragoff, Donald/Easson Larissa (1997), Department of Justice Canada: Computer-Related Investigations: Search And Seizure - Options Paper (Summit of the Eight, Senior Experts Group on Transnational Organized Crime (Lyon Group), Subgroup on High-Tech Crime)

Piragoff, Donald/Easson Larissa (1997a), Department of Justice Canada: Computer-Related Investigations: Search And Seizure - Options Paper (version prepared for Council of Europe Committee of Experts on Crime in Cyberspace (PC-CY(97)40), 24 September 1997.

Planken, Erik (2010): Cybercrime investigations and state sovereignty: Some thoughts on the way forward

Planken, Erik (2012): Preparatory paper for the first meeting of the ad hoc Working Group on transborder investigations in cybercrime

Poullet, Yves/ Van Gyseghem, Jean-Marc/ Gérard, Jacques/Gayrel, Claire/ Moiny, Jean-Philippe (2010): Cloud computing and its implications on data protection (Discussion paper prepared for the Council of Europe/Global Project on Cybercrime)
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1c.pdf

Salt, Marcos (2012): Acceso trasfronterizo de datos almacenados en soportes informáticos en los países de America Latina (contribution to Council of Europe Octopus Conference 2012)

Sansom, Gareth (2008): Website Location: Cyberspace vs. Geographic Space (Draft: April 3, 2008)

Schwerha, Joseph (2010): Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers" (Discussion paper prepared for Council of Europe / Global Project on Cybercrime)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

Seitz, Nicolai (2004): Transborder Search: A new perspective in law enforcement? In: International Journal of Communications Law & Policy, Issue 9 – Special Issue on Cybercrime, Autumn 2004
http://www.ijclp.net/files/ijclp_web-doc_2-cy-2004.pdf

Sieber, Ulrich (2012): Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag. München.
Extract: http://www.beck-shop.de/fachbuch/leseprobe/Deutscher-Juristentag-djt-Straftaten-Strafverfolgung-Internet-9783406630729_1907201206155217_lp.pdf

Soukieh, Kim (University of NSW) (2011): Cybercrime – the shifting doctrine of jurisdiction (published in Canberra Law Review (2011) Vol. 10)
http://www.canberra.edu.au/faculties/law/attachments/pdf/the-canberra-law-review-articles/Kim-Soukieh-CLR-2011-Vol.-10.pdf

Spoenle, Jan (2010): Cloud computing and cybercrime investigations: territoriality vs the power of disposal. Strasbourg (report prepared for Council of Europe / Global Project on Cybercrime)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

Yaana Technologies LLC (2011): Elements of Cloud Lawful Interception and Retained Data (Anthony Rutkowski / LI(11)0028)