Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers

1. BACKGROUND

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention), which was opened for signature in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime and electronic evidence. After 20 years, it remains the most significant one in the area. Currently, 69 countries are Parties to the Budapest Convention, including 26 EU Member States [1].

The Budapest Convention aims at:

- Criminalising the conduct pertaining to cyber-related crime;
- Supporting the investigation and prosecution of these crimes as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form by providing necessary procedural tools; and
- Setting up a fast and efficient system for international cooperation[2].

The Budapest Convention is accompanied by an Explanatory Report which is intended to guide and assist Parties in its application.

More information about the Budapest Convention is available in the dedicated SIRIUS Quarterly Review here.

Article 32 constitutes the most important provision on trans-border access to data set out in the Budapest Convention. It provides a possibility for competent authorities from one Party to **unilaterally access computer data stored in another Party** with consent or where publicly available, without seeking Mutual Legal Assistance (MLA). As such, Article 32 constitutes **an exception to the principle of territoriality** as it establishes the cyber domain as a public domain (Article 32(a)) and provides for jurisdiction to enforce on a foreign territory under certain conditions (Article 32(b)). The provision carries the potential for cross-border (extraterritorial[3]) effects, allowing authorities to extend their reach beyond their national boundaries in certain circumstances.

The text of the Article 32 provides as follows:

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.

According to the Budapest Convention, Parties are not entitled to make any reservations to Article 32[4].

Although not binding, Guidance Note #3, adopted by the Cybercrime Convention Committee (T-CY) in 2014, provides the Parties to the Budapest Convention with a common way of interpretation of Article 32.

2. SCOPE

- **Types of crimes covered**

Article 32 is a measure to be applied in "specific criminal investigations and proceedings" within the

[1] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. All EU Member States, except for Ireland.
[2] Budapest Convention, Preamble; Explanatory Report, para. 16.
[3] It is noted that the term "extraterritorial" is not used in the text of the Budapest Convention itself, its Explanatory Report or Guidance Note #3.
[4] Budapest Convention, Article 42.

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

scope of Article 14 of the Budapest Convention[5], that is investigations and proceedings relating to:

- Criminal offences established in accordance with Section 1 of the Budapest Convention (illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights);
- Other criminal offences committed by means of a computer system; and
- The collection of evidence in electronic form of a criminal offence[6].

Therefore, the specific criminal investigations and proceedings covered include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that the provision applies either where a crime is committed by use of a computer system, or where a crime not committed by use of a computer system (for example a murder) involves electronic evidence.

This is also confirmed in Guidance Note #13, which states that: "The T-CY agrees that the procedural law provisions and the principles and measures for international co-operation of the [Budapest Convention] are applicable not only to offences related to computer systems and data but also to the collection of electronic evidence of any criminal offence."

- **Data covered**

Article 32 covers **all types of computer data** (thus excluding non-digital data). The provision only covers **stored and existing data** and does not include future data or existing data which is in transit.

3. DEFINING THE TOOLBOX

Article 32 of the Budapest Convention addresses two situations:

- Where the data being accessed is publicly available (Article 32(a)); and
- Where a Party accesses or receives data located outside of its territory through a computer system in its territory, having obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system (Article 32(b)).

By providing a limited exception from the principle of territoriality, Article 32 provides an important procedural tool to address some of the problems arising from cross-border criminality and the fact that **electronic evidence required in criminal investigations is often not located in the territory of the investigating authority**.

Article 18 of the Budapest Convention is another important procedural tool which provides the legal framework for the implementation into the national law of Parties to the Budapest Convention of two types of domestic measures that, according to some Parties, may have cross-border (extraterritorial) effects.

More information about Article 18 of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review here.

A- ARTICLE 32(A) – TRANS-BORDER ACCESS TO PUBLICLY AVAILABLE STORED COMPUTER DATA

Article 32(a) provides a basis for competent authorities in a Party to access **any data that the public may access**[7], including data that technically may be stored in foreign territory.

For this purpose, authorities may subscribe to or register for services available to the public[8]. Subject

[5] Guidance Note #3, p. 5 (referring to the scope of application of Article 32(b)); see also Budapest Convention, Article 23.
[6] Budapest Convention, Article 14(2)(a)-(c).
[7] Guidance Note #3, p. 4.
[8] Ibid.

to domestic law[9], they may also download the data, take screenshots or similarly secure the data and use it as evidence in criminal proceedings without the need for MLA or the permission of the State where the computer system hosting the data, e.g. the website from where the data is collected, is located[10].

If a portion of a public website, service or similar is closed to the public, then it is not considered publicly available within the meaning of Article 32(a)[11].

B- ARTICLE 32(B) – TRANS-BORDER ACCESS TO STORED COMPUTER DATA WITH CONSENT

Article 32(b) provides a basis for competent authorities in a Party to engage in **unilateral trans-border access to data located in another Party** if the data owner / possessor has **voluntarily consented** to such access.

Due to the wording "access or receive", the provision includes not only the case of competent authorities directly accessing data stored in another jurisdiction, but also receiving this data from a person who has the "lawful authority" to disclose it and has "voluntarily and lawfully consented".

Typical situations in which Article 32(b) may apply include, for example, a situation where a person's e-mail is stored in another country by a service provider, or a person intentionally stores their data in another Party. 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 it[12].

According to Guidance Note #3, another instance where Article 32(b) may apply is where a suspected criminal is lawfully arrested while his or her mailbox – possibly with evidence of a crime – is open on his or her tablet, smartphone or other device and the suspect voluntarily consents that law enforcement access the account (and the law enforcement authorities know that the data contained in the mailbox is located in another Party to the Budapest Convention)[13]. It is however noted that, whether the consent of a person provided in these circumstances may be considered voluntary will depend on the domestic laws of the Party regarding what constitutes lawful and voluntary consent (see also section Lawful and voluntary consent below).

Article 32(b) does not require notification of the Party in whose territory the data is located; however, the Budapest Convention also does not exclude such notification and the requesting Party may notify the other Party if deemed appropriate[14] (see also section Conditions and safeguards).

- **Data located in another Party**

The data that can be accessed under Article 32(b) of the Budapest Convention must be "located in another Party". This means that the provision covers only situations where **it is known where the data is located**[15] and where **the data is located in another Party to the Budapest Convention**. It does not cover situations where the data is not stored in another Party or where it is uncertain where the data is located[16]. A Party may also not use the provision to obtain disclosure of data that is stored domestically[17] (this is covered by Article 19(2) of the Budapest Convention).

It is of note that Article 32(b) "neither authorize[s], nor preclude[s]" other situations. Thus, in situations where it is **unknown or not certain whether data is stored in another Party**, Parties may need to evaluate themselves the legitimacy of a search or other type of access in light of domestic law, relevant international law principles or considerations of international relations[18].

[9] Domestic law may, for example, limit law enforcement access to or use of publicly available data (Guidance Note #3, footnote 3).
[10] T-CY Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder access and jurisdiction: What are the options?, 6 December 2012, para. 92.
[11] Guidance Note #3, p. 4.
[12] Explanatory Report, para. 293.
[13] Guidance Note #3, p. 5.
[14] Guidance Note #3, p. 6.
[15] Ibid.
[16] Ibid.
[17] Ibid.
[18] Ibid.

- **Entities covered**

Article 32(b) applies to any "person". The scope of the provision is therefore broad and may include both natural and legal persons[19], i.e. service providers.

- **Location of the person consenting to provide access or disclose data**

Article 32(b) is not specific as to where the person consenting to disclose data or providing access should be located at the moment of consent and / or disclosure of the data.

The standard hypothesis is that the person is **physically located** in the territory of the requesting Party. In this situation, that person falls under the jurisdiction of and is subject to the laws of that Party[20].

However, other situations are also possible. For example, the person concerned may be located in the territory of the requesting Party **when agreeing to disclose or actually providing access**, or **only when agreeing to disclose** but not when providing access. The person may also be **physically located in the Party where the data is stored or in a third country** when agreeing to cooperate or when actually providing access[21].

It is of note that many Parties would object – and some even consider it a criminal offence – if a person who is physically present in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation[22].

If the person is a legal person, it may be represented in the territory of the requesting Party, the territory of the Party hosting the data, or even a third country at the same time[23].

- **Lawful and voluntary consent**

Article 32(b) permits trans-border access to data where "lawful and voluntary consent" has been provided. What amounts to "lawful and voluntary" consent of a person will depend on the domestic law of the requesting Party. This will generally require that the person providing access or agreeing to disclose data **may not be forced or deceived**[24]. This implies that the person may not be obliged to disclose the data by means of, e.g. a judicial order for the seizure or production of data. Domestic law will also determine whether minors or persons suffering from mental or other conditions are able to provide consent[25], as well as whether consenting to avoid or reduce criminal charges or a potential prison sentence constitutes lawful and voluntary consent[26].

According to Guidance Note #3, in most Parties, cooperation in a criminal investigation would require **explicit consent**; therefore, a **general agreement** by the user **to the terms and conditions** of an online service used **might not constitute explicit consent** for disclosure of that user's data to competent authorities even if those terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse[27]. However, as far as service providers subject to EU law are concerned, according to the General Data Protection Regulation (GDPR), service providers may voluntarily consent to the disclosure of their users' data on legal bases other than the data subject's consent (see below).

- **Lawful authority to disclose the data**

As required under Article 32(b), the person consenting to disclose or provide access to data must have "lawful authority" to do so. The question as to who is the person "lawfully authorized" to

[19] Guidance Note #3, p. 7.
[20] T-CY Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder access and jurisdiction: What are the options?, 6 December 2012, para. 115.
[21] Guidance Note #3, p. 7.
[22] Guidance Note #3, p. 8.
[23] Guidance Note #3, p. 7.
[24] Guidance Note #3, p. 6.
[25] Ibid.
[26] Guidance Note #3, footnote 9.
[27] Guidance Note #3, p. 7. See also Article 29 Data Protection Working Party, Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime, letter to Council of Europe, 5 December 2013, p. 3.

disclose data will vary depending on the circumstances, the nature of the person and the laws and regulations applicable[28].

EU LAW REQUIREMENTS FOR SERVICE PROVIDERS UNDER THE GDPR

Service providers and other private sector entities which are **subject to the GDPR**[29] can lawfully consent to the disclosure of their users' data to competent authorities if: (a) they are controllers of such data; (b) there is a lawful basis for disclosure under Article 6 of the GDPR; and (c) it is necessary and proportionate to do so.

Article 6 of the GDPR sets out six lawful bases for the disclosure of users' data.

Consent under **Article 6(1)(a)** of the GDPR may provide a lawful basis for sharing a user's data, but only applies where the affected user has a **real choice** in freely agreeing to the sharing of data and is **able to easily withdraw consent**. Therefore, while a victim of crime may consent to the sharing of their personal data, an alleged perpetrator is unlikely to do so.

If a service provider is **required by a court order** or has a **statutory duty to report potential criminal acts** to the competent authorities, then the lawful basis for disclosure of a user's data is likely to be **Article 6(1)(c)** of the GDPR, which provides a lawful basis to share personal data where necessary to **comply with a legal obligation to which the service provider is subject**.

Service providers may also be able to rely on the **vital interests** clause in **Article 6(1)(d)** of the GDPR as a lawful basis for disclosure, if necessary, for example, to protect someone's life. However, this is only likely to be applicable in a limited range of circumstances, i.e. where **an individual's life is at risk**. The vital interests clause can be reflected in the emergency disclosure policies of different service providers that are based on the law of the United States of America pertaining to emergency, which protects similar kinds of interests[30].

Under **Article 6(1)(f)** of the GDPR, service providers may also consent to sharing their users' personal data when this is necessary for the **legitimate interests** of the service provider or those of a third party and when these legitimate interests **do not outweigh** the interests, right or freedoms which require the protection of personal data of the users.

There are also further requirements if the personal data to be shared consists of special category data (Article 9 of the GDPR) or criminal offence data (Article 10 of the GDPR).

4. CONDITIONS AND SAFEGUARDS

- **Purpose limitation**

As noted above (see section Scope), Article 32 is applicable to specific criminal investigations or proceedings relating to criminal offences established in accordance with Section 1 of the Budapest Convention, other criminal offences committed by means of a computer system and the collection of evidence in electronic form pertaining to any criminal offence.

- **Protection of human rights**

In accordance with Guidance Note #3, it is presumed that the Parties to the Budapest Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 of the Budapest Convention[31].

Article 15(1) of the Budapest Convention requires Parties to ensure that the powers and procedures established under the Budapest Convention are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or minimum safeguards

[28] Explanatory Report, para. 293; Guidance Note #3, p. 7.

[29] The GDPR is applicable to: (a) the processing of personal data by controllers and processors with an establishment in the EU, regardless of where the actual processing is carried out (GDPR, Article 3(1)); and (b) the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to the data subjects in the EU or to the monitoring of their behaviour, as far as their behaviour takes place within the EU (GDPR, Article 3(2)).

[30] 18 U.S. Code § 2702 C-4: A situation "*involving danger of death or serious physical injury to any person*" which requires "*disclosure without delay of information*".

[31] Guidance Note #3, p. 5.

arising pursuant to a Party's obligations under applicable international human rights instruments[32].

With regard to the application of **Article 32(b)**, competent authorities must apply the same legal standards when applying this provision as they would domestically. If access or disclosure would not be permitted domestically, it would also not be permitted under Article 32(b)[33].

- **Rights of individuals and interests of third parties**

Specifically as far as **Article 32(b)** is concerned, the rights of individuals and the interests of third parties are to be taken into account when applying this measure. Therefore, for example, the requesting Party may consider notifying relevant authorities of the country in which the data accessed or received is located[34].

5. IMPLEMENTATION OF ARTICLE 32 OF THE BUDAPEST CONVENTION IN THE EU MEMBER STATES

The national legislation of the majority of EU Member States allows competent authorities from that EU Member State to unilaterally access computer data stored in another Party with consent or where publicly available. For more information on some of the EU Member States' legislation implementing Article 32 see the Annex.

6. CHALLENGES

- **Limited scope of application and recent technological developments**

In addition to the limitations noted above (see section Defining the toolbox), situations where non-publicly available data is **stored on the territory of a non-Party** or where its **location is either unknown or uncertain** fall outside the scope of Article 32. In these situations, Parties need to determine the legitimacy of a cross-border search themselves[35].

This problem is further compounded by the fact that, due to recent technological developments, data will often not necessarily be stored within the borders of a single country but be located in the cloud (in servers in multiple or unknown locations), which may further limit the instances where Parties can rely on Article 32.

- **Requirement of "lawful and voluntary consent"**

Specifically as concerns Article 32(b), obtaining data stored in another Party under this provision may be difficult, especially outside of emergency circumstances. Depending on the person with lawful authority to disclose the data, on one hand, suspects of the investigation may not voluntarily consent to providing access to their data due to the risk of self-incrimination while, on the other hand, service providers subject to EU law may have only a very narrow margin of maneuver as concerns disclosure of their users' data under the GDPR.

7. THE WAY FORWARD

The Explanatory Report acknowledges that the drafters of the Budapest Convention found that it was **not yet possible**, at the time of drafting, to prepare a **comprehensive, legally binding** regime regulating instances where a Party may unilaterally access computer data stored in another Party without seeking MLA. Article 32 of the Budapest Convention thus provides a **minimum consensus** regarding situations where unilateral action is permissible[36].

Already in 2014, the T-CY Transborder Group[37] noted that, while Article 32 of the Budapest

[32] These instruments include the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and its additional protocols (in respect of European states that are parties them), other applicable human rights instruments, such as e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights (in respect of states in other regions of the world which are parties to them) and the 1966 International Covenant on Civil and Political Rights (Explanatory Report, para. 145).

[33] Guidance Note #3, p. 7.

[34] Guidance Note #3, p. 6.

[35] Ibid.

[36] Explanatory Report, para. 293.

[37] https://www.coe.int/en/web/cybercrime/tb.

Convention allows for trans-border access to data in limited situations, **States increasingly develop unilateral solutions** to access data in foreign or unknown jurisdictions beyond the provisions of the Budapest Convention. Such an approach may create **risks for both inter-State relations and the rights of individuals**[38].

The T-CY also repeatedly made a number of **recommendations concerning trans-border access to data** to be considered in a (future) protocol to the Budapest Convention[39].

While views on the question of trans-border access to data, later referred to as "extended searches / access based on credentials"[40], were exchanged during the negotiations of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Second Protocol),[41] no further provisions on the matter were adopted in the final text of the Second Protocol.

According to the Explanatory Report to the Second Protocol, the issue of "extension of searches" was found to require additional work, time and consultations with stakeholders and was therefore considered **not feasible within the time frame set** for the preparation of the Second Protocol[42]. Therefore, the drafters proposed that it be **pursued in a different format** and **possibly in a separate legal instrument**[43].

The Second Protocol contains a number of other substantive provisions concerning measures of investigatory assistance.

More information about the Second Protocol is available in the dedicated SIRIUS Quarterly Review here.

On 15 November 2021, the T-CY established a **Working group** on undercover investigation and **extension of searches**, tasked to prepare a report on, among other things, extension of searches, containing **draft options and recommendations for further action** by the T-CY (for example, guidance notes, documenting experiences and best practices, or negotiation of a binding instrument)[44].

[38] T-CY Ad-hoc Subgroup on Transborder Access and Jurisdiction, Transborder access to data and jurisdiction: Options for further action by the T-CY, 3 December 2014, p. 8. See also T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, 16 September 2016, para. 142.

[39] T-CY Ad-hoc Subgroup on Transborder Access and Jurisdiction, Transborder access to data and jurisdiction: Options for further action by the T-CY, 3 December 2014, pp. 12-14; T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, 16 September 2016, paras 143-144.

[40] T-CY, Report of the 3rd Meeting of the T-CY Protocol Drafting Plenary (Strasbourg 28 – 29 November 2018), footnote 1.

[41] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

[42] Explanatory Report to the Second Protocol, para. 24. The T-CY Protocol Drafting Group had previously noted that the inclusion of a provision on the extension of searches would entail the risk that some Parties may not be able to join the Second Protocol once it is opened for signature and regulating this measure in an international instrument would require careful consideration as such rules may limit measures currently available in many Parties, while other Parties' laws prohibit such measures in their territories (T-CY, Working group on undercover investigations and extension of searches: Terms of Reference, 15 November 2021, p. 2).

[43] Explanatory Report to the Second Protocol, para. 24.

[44] T-CY, Working group on undercover investigations and extension of searches: Terms of Reference, 15 November 2021, p. 1.

Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers

SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE | EUROJUST | EUROPOL

ANNEX
DOMESTIC LEGISLATION OF EU MEMBER STATES IMPLEMENTING ARTICLE 32 OF THE BUDAPEST CONVENTION

AUSTRIA

Article 32 of the Budapest Convention is directly applicable.

BELGIUM

Code of Criminal Procedure

Article 88ter[45]

The investigating judge may extend the search in a computer system or part thereof, begun on the basis of Article 39bis, to a computer system or part thereof which is in a place other than the place where the search is carried out:

- in case this extension is necessary for the manifestation of the truth in respect of the offence being investigated; and

- in case other measures would be disproportionate, or where there is a risk that, without this extension, evidence would be lost.

The extension of the search in a computer system may not go beyond the computer systems or parts of such systems to which the persons authorised to use the computer system which is the subject of the measure have specific access.

With regard to the data collected by the extension of the search in a computer system, which are useful for the same purposes as those provided for the seizure, the rules provided for in Article 39bis § 6 shall apply.

When it turns out that these data are not in the territory of the Kingdom, they may only be copied. In this case, the investigating judge shall immediately communicate this information to the Federal Public Service of Justice, which shall inform the competent authorities of the State concerned, if this can reasonably be determined.

In cases of extreme urgency, the investigating judge may orally order the extension of the search referred to in paragraph 1. This order shall be confirmed in writing as soon as possible, mentioning the reasons for the extreme urgency.

CYPRUS

Article 32 of the Budapest Convention is directly applicable.

CZECHIA

Article 32 of the Budapest Convention is directly applicable.

DENMARK

Article 32 of the Budapest Convention is directly applicable.

ESTONIA

The goal of Article 32 of the Budapest Convention can be achieved by relying on Section 215 of the Code of Criminal Procedure accompanied by the clear consent of the data subject.

[45] The following constitutes a courtesy translation.

Code of Criminal Procedure

Section 215 – Binding nature of orders and requirements issued by investigative authorities and the Prosecutor's Office

(1) Any orders or requirements issued by investigative authorities and the Prosecutor's Office in any criminal proceedings they are conducting are binding on everyone and are executed throughout the territory of the Republic of Estonia. Where the subject-matter of criminal proceedings is an act of a person serving in the Defence Forces, such orders or requirements are binding on members of the Defence Forces who are carrying out a mission abroad. The costs incurred to comply with a requirement or order are not subject to compensation.

(2) An investigative authority conducting criminal proceedings has a right to make a written request to another such authority for the performance of single procedural operations and for any other assistance. Such requests are fulfilled without delay.

(3) On an application of the Prosecutor's Office, the pre-trial investigation judge may enter an order by which they impose a fine on a party to proceedings, another person participating in the proceedings or a non-party who has failed to comply with the obligation provided by subsection 1 of this section. No fine is imposed on the suspect or accused.

FRANCE

Article 32 of the Budapest Convention is directly applicable with respect to publicly available information.

GREECE

Article 32 of the Budapest Convention is directly applicable.

HUNGARY

Article 32 of the Budapest Convention is directly applicable.

Act XC of 2017 on the Code of Criminal Procedure

The Scope of this Act

Section 9

(1) Criminal proceedings shall be conducted pursuant to this Act in cases falling within Hungarian criminal jurisdiction.

(2) A procedural act by the court, the prosecution service or the investigating authority may be conducted concerning data accessible through an information system that is in Hungary regardless of the location of such data. The procedural act may be conducted regarding that part of the information system that the court, the prosecution service and the investigating authority can access, on the basis of authorisation by law, without bypassing or circumventing the means or information technology solution protecting the information system.

(3) A procedural act conducted pursuant to paragraph (2) shall be without prejudice to any commitment undertaken by Hungary in an international treaty.

ITALY

Article 32 of the Budapest Convention is directly applicable.

LITHUANIA

Code of Criminal Procedure

Article 155 – Prosecutor's right to access information

1. The prosecutor, having adopted the order and received the consent of the judge of the pre-trial investigation, has the right to come to any state or municipal, public or private institution, company or organization and demand that he be allowed to familiarize himself with the necessary documents or other necessary information,

make records or to copy documents and information or to receive specified information in writing, if this is necessary for the investigation of a criminal act.

2. Persons who refuse to provide the prosecutor with required information or documents may be fined based on Article 163 of this Code.

3. The prosecutor may use the information obtained in accordance with the procedure established in paragraph 1 of this article only for the purpose of investigating a criminal act. The prosecutor must immediately destroy information that is not needed for the investigation of the crime.

4. By order of the prosecutor, the pre-trial investigation officer may also get acquainted with the information in accordance with the procedure established in this article.

5. Laws of the Republic of Lithuania may establish restrictions on the prosecutor's right to access information.

NETHERLANDS

Article 32 of the Budapest Convention is directly applicable.

POLAND

Article 32 of the Budapest Convention is directly applicable.

PORTUGAL

The Portuguese legal framework includes the below provision, which specifically allows foreign authorities to access data stored in Portugal when publicly available or with consent.

Cybercrime Law

Article 25 - Cross-border access to computer data stored when publicly available or with consent

The competent foreign authorities without prior request from the Portuguese authorities, in accordance with the rules on transfer of personal data provided by Law No. 67/98 of 26 October, may:

a) access data stored in a computer system located in Portugal, where publicly available;

b) receive or access through a computer system located in its territory, the data stored in Portugal, through legal and voluntary consent of the person legally authorized to disclose them.

ROMANIA

Code of Criminal Procedure

Article 168 – Computer search

(1) A computer system search or a computer data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

(2) During the criminal investigation, the Judge for Rights and Liberties of the court that would have the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office with which the prosecutor conducting or supervising the criminal investigation is working are located may order the conducting of a computer search, upon request by the prosecutor, when the investigation of a computer system or of a computer data storage medium is necessary for the discovery and collection of evidence.

(3) The prosecutor shall submit an application requesting the approval of a computer search together with the case file to the Judge for Rights and Liberties.

(4) Such application is ruled on in chambers, without summoning the parties. The prosecutor's attendance is mandatory.

(5) The judge orders, through a court resolution, to sustain the application, when this is well-grounded, to approve the computer search, and issues a search warrant forthwith.

(6) Such court resolution has to contain:

a) name of the court;

b) date, time and place of issuance;

c) surname, first name and capacity of the person who issued the warrant;

d) the time frame for which the warrant was issued and within which the ordered activity has to be performed;

e) purpose for which it was issued;

f) the computer system or computer data storage medium that is to be subject to search, as well as the name of the suspect or defendant, if known;

g) signature of the judge and stamp of the court.

(7) A court resolution through which the Judge for Rights and Liberties decides upon an application for the approval of a computer search is not subject to avenues of appeal.

(8) In the event that, on the occasion of a search of a computer system or of a computer data storage medium, it is found that the sought computer data is stored in a different computer system or a computer data storage medium, and is accessible from the initial system or medium, the prosecutor shall immediately order the preservation and copying of the identified computer data and shall request the issuance of a warrant on an emergency basis. The stipulations of para. (1) - (7) shall apply accordingly.

(9) In conducting the ordered search, in order to ensure integrity of the computer data stored on the seized objects, the prosecutor shall order the making of copies of them.

(10) If the seizure of objects containing computer data set under para. (1) seriously hinders the performance of activities by the persons holding such objects, the prosecutor may order the making of copies of them, which would serve as methods of proof. Copies are made with adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

(11) A computer system or computer data storage medium search is conducted in the presence of a suspect or a defendant, and the provisions of Art. 159 para. (10) and (11) shall apply accordingly.

(12) A computer system or computer data storage medium search is conducted by a specialist working with the judicial bodies or an external one, in the presence of the prosecutor or of the criminal investigation bodies.

(13) A computer search report has to contain:

a) name of the person from whom a computer system or computer data storage media is seized or name of the person whose computer system is subject to search;

b) name of the person having conducted the search;

c) names of the persons present during the search conducting;

d) a description and list of the computer systems or computer data storage media against which search was ordered;

e) a description and list of the performed activities;

f) a description and list of the computer data discovered on the occasion of the search;

g) signature or stamp of the person having conducted the search;

h) signature of the persons present during the search conducting.

(14) Criminal investigation bodies have to take steps in order to make sure that the search is conducted without making facts and circumstances of the private life of the person subject to search public in an unjustified manner.

(15) Computer data of a secret nature identified during such search is kept under the law.

(16) During the trial, computer search is ordered by the court, *ex officio* or upon request by the prosecutor, by the parties or the victim, in the situations set by para. (2). A warrant for a computer search ordered by the court shall be communicated to the prosecutor, who shall act as per para. (8) - (15).

The Romanian legal framework furthermore includes the below provision, which specifically allows foreign authorities to access data stored in Romania when publicly available or with consent.

Law 161/2003
Article 65

(1) A competent foreign authority can have access to public Romanian sources of computer data without requesting the Romanian authorities.

(2) A competent foreign authority can have access and can receive, by means of a computer system located on its territory, computer data stored in Romania, if it has the approval of the authorised person, under the conditions of the law, to make them available by means of that computer system, without requesting the Romanian authorities.

SLOVENIA

Code of Criminal Procedure
Article 219a

(1) A search of electronic and related devices, and electronic data storage devices (electronic devices), including network-connected and accessible information systems where data is stored, may be carried out for the purpose of obtaining information in electronic form if reasonable grounds for suspicion exist that a criminal offence has been committed and if it is likely that the electronic device contains electronic information:

- on the basis of which the suspect or the accused person may be identified, uncovered or apprehended, or the traces of the criminal offence that are important for criminal proceedings may be uncovered, or
- which may be used as evidence in criminal proceedings.

(2) The search shall be carried out with the prior written consent of the owner and the users of the electronic device known by and accessible to the police who have reasonable expectations of privacy (user) concerning such a device, or pursuant to a reasoned written warrant of the court issued upon a motion of the state prosecutor. When the search is carried out pursuant to a court warrant, a copy of such warrant shall be served on the owner or user of the electronic device which is to be searched before the beginning of the search. The search of an electronic device seized from an attorney, a candidate attorney or a trainee attorney may only be carried out pursuant to a court search warrant, reasoned in accordance with paragraph six of Article 220.

SPAIN

Article 32 of the Budapest Convention is directly applicable.

SWEDEN

Article 32 of the Budapest Convention is directly applicable.