Production Orders under Article 18 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.

One of the most important provisions of the Budapest Convention is Article 18, which provides the legal framework for the implementation into the national law of the Parties to the Budapest Convention of **two types of domestic measures that, according to some Parties, may have cross-border (extraterritorial[3]) effects**.

The text of the Article 18(1) provides as follows:

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

According to the Budapest Convention, Parties are not entitled to make any reservations to Article 18[4].

Although not binding, Guidance Note #10, adopted by the Cybercrime Convention Committee (T-CY) in 2017, provides the Parties to the Budapest Convention with a common way of interpretation of Article 18.

2. SCOPE

- **Types of crimes covered**

Production orders pursuant to Article 18 of the Budapest Convention (Article 18 Production Orders) are applicable to "specific criminal investigations or proceedings"[5] 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,

[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 #10. However, for the purposes of the present document, the term is to be understood to refer to a domestic order with potential cross-border effects.
[4] Budapest Convention, Article 42.
[5] Budapest Convention, Article 14(1).

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.

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 18(1)(a) is not restricted to "subscriber information" and covers **all types of computer data**[7] stored in a computer system or computer-data storage medium. The provision only covers **stored and existing data** and does not include any future data[8] or existing data which is in transit.

Article 18(1)(b) applies only to the production of **subscriber information**. The term "subscriber information" is defined for the purposes of Article 18 of the Budapest Convention in paragraph 3 of the article. "Subscriber information" includes any information held by the administration of a service provider relating to a subscriber to its services (other than traffic data or content data) by means of which can be established:

- The type of communication service used, the technical provisions[9] taken thereto and the period of time during which the person subscribed to the service (Article 18(3)(a));
- The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement[10] between the subscriber and the service provider (Article 18(3)(b)); or
- Any other information concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement (Article 18(3)(c)).

> ⚠ It is notable that **the definition of "subscriber information"**, as per Article 18(3) of the Budapest Convention, **may also include information that under the domestic law of some EU Member States is considered as traffic data**.

"Subscriber information" may be in the form of computer data, but also in any other form, such as paper records[11]. As in the case of Article 18(1)(a), Article 18(1)(b) does not include data that has not yet come into existence[12]. Also, the provision is only applicable to the extent that the service provider

[6] Budapest Convention, Article 14(2)(a)-(c).
[7] Guidance Note #10, p. 6.
[8] Explanatory Report, para. 170.
[9] The term "technical provisions" includes all measures taken to enable a subscriber to enjoy the communication service, including the reservation of a technical number or address (for example, telephone number, website address / domain name, e-mail address) and the provision and registration of communication equipment used by the subscriber (for example, telephone devices, call centres, LANs). See Explanatory Report, para. 179.
[10] The reference to a "service agreement or arrangement" includes any kind of relationship on the basis of which a client uses the service provider's services. See Explanatory Report, para. 183.
[11] Budapest Convention, Article 18(3); Explanatory Report, para. 177.
[12] Explanatory Report, para. 170.

subject to the production order maintains the requested data[13].

> The term "subscriber" is intended to include clients with paid subscriptions, paying on a per-use basis, as well as those receiving free services. It also includes information concerning persons entitled to use the subscriber's account[14].

- **Entities covered**

Article 18(1)(a) applies to **any "person"**. The scope of the provision is therefore broad and may include **both natural and legal persons, i.e. service providers**[15].

Article 18(1)(b) applies to **"service providers"**. The term "service provider" is broadly defined for the purposes of the Budapest Convention in Article 1(c) and includes:

- Any public or private entity that provides to users of its service **the ability to communicate** by means of a computer system; and
- Any other entity that **processes or stores computer data** on behalf of such communication service or users of such service.

> Both providers of electronic communication services and of internet society services are covered by the definition of "service provider" included in Article 1(c) of the Budapest Convention[16].

3. DEFINING THE TOOLBOX

Article 18 of the Budapest Convention provides the legal framework for the implementation into the national law of the Parties to the Budapest Convention of **two types of domestic measures that, according to some Parties, may have cross-border (extraterritorial) effects**:

- Domestic production orders for any type of data when a person (including a service provider) is in the territory of a Party, even if the data sought is stored in another jurisdiction (Article 18(1)(a)); and
- Domestic production orders for subscriber information where a service provider is not necessarily present in the territory of a Party but is offering a service in the territory of such Party and the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party (Article 18(1)(b)).

For the application of Article 18, see also Annex I.

Article 18 Production Orders thus have the advantage that the **location of the data sought is no longer the determining factor** for establishing jurisdiction. Therefore, they offer 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**, but rather in foreign, multiple or unknown locations.

However, Article 18 of the Budapest Convention does not provide a basis for enforcement in case of a lack of response to production orders issued pursuant to the provision, as further explained in section Enforceability.

A- ARTICLE 18(1)(A) – PRODUCTION ORDER WHEN A PERSON (INCLUDING A SERVICE PROVIDER) IS IN THE TERRITORY OF A PARTY

Article 18(1)(a) provides a basis for competent authorities to order a person (including a service provider) **in their territory** to disclose computer data **in that person's possession or control**.

The term "possession or control" refers to **physical possession** of the data in the ordering Party's

[13] Article 18 does also not impose an obligation on service providers to ensure the correctness of the subscriber information in their possession so, for example, service providers are not obliged to verify the identity of their subscribers or to prohibit the use of pseudonyms by users (Explanatory Report, para. 181).
[14] Explanatory Report, para. 177.
[15] Guidance Note #10, p. 6.
[16] Guidance Note #10, p. 5, footnote 6.

territory, as well as to situations where the data is outside of the person's physical possession but the person can **freely control its production** from within the ordering Party's territory[17]. This includes for example data stored remotely but within the person's online account[18].

B- ARTICLE 18(1)(B) –PRODUCTION ORDER WHEN A SERVICE PROVIDER IS OFFERING ITS SERVICES IN THE TERRITORY OF A PARTY

Article 18(1)(b) provides a basis for competent authorities of a Party to order a service provider **offering its services in their territory** to disclose subscriber information **relating to such services** which is in that service provider's **possession or control**.

- **Offering their services in the territory of a Party**

According to Guidance Note #10, a service provider can be considered to be "offering its services" in the territory of a Party when:

- It enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and
- It has established a **real and substantial connection** to a Party. In this respect, relevant factors include the extent to which the service provider orients its activities towards subscribers from the territory of the Party (e.g. by advertising locally and/or in the local language), makes use of the subscriber information or associated traffic data in the course of its activities and interacts with subscribers in the Party[19].

For an example of the application of the above criteria, see the Belgian *Yahoo!* case, where the competent Belgian court found that Yahoo!, as a provider of a free webmail service, is present on Belgian territory, despite being based in the United States of America, because it actively participates in Belgian economic life, including by using the .be domain, by showing publicity in the local language and by being reachable for users in Belgium via a complaint mailbox and a helpdesk.

A similar reasoning was applied by a different Belgian court in the *Skype* case, albeit in the context of the application of a different procedural tool (interception of communication), where the relevant court also found that Skype was present on Belgian soil by actively participating in the economic life in Belgium.

Accordingly, competent authorities can issue Article 18 Production Orders targeting service providers offering their services in their territory which are otherwise **not physically present and do not have a legal establishment** in their territory[20]. When implemented into domestic law, the provision thus establishes a **legal basis for direct cooperation** between competent authorities in one Party and service providers located outside of its territory without going through the mutual legal assistance (MLA) process.

- **Subscriber information relating to the services offered in the Party's territory**

The subscriber information which can be sought through an Article 18 Production Order must be **related to the services offered** in the ordering Party's territory. Therefore, if for example, a service provider offers one type of service in Country A but not in Country B, competent authorities in Country B cannot issue a production order for subscriber information pertaining to users of services offered in Country A.

- **Possession or control of subscriber information**

Similarly as in the case of Article 18(1)(a), Article 18(1)(b) applies to subscriber information **in the service provider's "possession or control"**. This

[17] Explanatory Report, para. 173.

[18] On the other hand, the mere technical ability to access remotely stored data, for example via a link, does not necessarily constitute "control" within the meaning of Article 18(1)(a) where the data is not within the person's legitimate control. See Explanatory Report, para. 173.

[19] Guidance Note #10, p. 8. See also *Yahoo!* Judgment, paras 7-8.

[20] Guidance Note #10, p. 6.

includes subscriber information in the service provider's physical possession, as well as subscriber information stored remotely (for example at a remote storage facility provided by another company located in another jurisdiction) but under the service provider's control[21].

4. CONDITIONS AND SAFEGUARDS

- **Purpose limitation**

In addition to what is noted above (see section Scope), the reference to "specific" criminal investigations and proceedings implies that production orders are to be used in individual cases concerning, habitually, particular subscribers. They cannot be used for ordering disclosure of indiscriminate amounts of information maintained by a service provider about groups of subscribers (for example, for the purpose of data-mining[22]).

- **Protection of human rights**

Article 15(1) of the Budapest Convention requires Parties to ensure that the powers and procedures established under the Budapest Convention – thus including Article 18 Production Orders – are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or minimum safeguards arising pursuant to a Party's obligations under applicable international human rights instruments[23].

- **Principle of proportionality**

Article 15(1) of the Budapest Convention further requires Parties to apply the principle of proportionality. This will be done in accordance with each Party's relevant domestic law principles. In the case of European countries, these principles will be derived from the European Convention on Human Rights (ECHR) and related jurisprudence, meaning that production orders must be **proportional to the nature and circumstances of the offence**[24]. Other Parties may apply related domestic law principles, such as **limitations on overly broad production orders**[25] or **exclude the application** of production orders **in cases concerning minor crimes**[26].

- **Other conditions and safeguards**

Pursuant to Article 15(2) of the Budapest Convention, applicable conditions and safeguards include, as appropriate, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. Other safeguards that must be addressed under domestic law include: the right against self-incrimination, legal privileges, specificity of individuals or entities subject to the production order, and privileged data or information[27].

Moreover, national laws may specify different competent authorities and additional safeguards concerning the production of certain types of data or subscriber information held by specific categories of persons or service providers[28]. For example, for some categories of data, such as publicly available subscriber information, a Party may permit law enforcement authorities to issue a production order while in other situations a court order may be required[29].

- **Rights of third parties**

In accordance with Article 15(3) of the Budapest Convention, when implementing the provisions of

[21] Explanatory Report, para. 173.
[22] Explanatory Report, para. 182.
[23] 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).
[24] Explanatory Report, para. 146.
[25] Ibid.
[26] Explanatory Report, para. 174.
[27] Explanatory Report, paras 147, 174.
[28] Explanatory Report, para. 174.
[29] Explanatory Report, para. 174; Cybercrime Convention Committee (T-CY), 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. 102.

Article 18, Parties shall first consider the sound administration of justice and other public interests (for example public safety, public health, the interests of victims, respect for private life). To the extent that it is consistent with these interests, consideration shall also be given to the impact of production orders on the rights, responsibilities and legitimate interests of third parties, which may include, for example, protection from liability for disclosure[30].

5. ISSUING PARTY

A - ISSUING AUTHORITIES

The national legal system of a Party will establish which authority is competent to issue an Article 18 Production Order, which may also depend on specific factors, such as the type of data sought (see also section Conditions and safeguards).

B - ISSUING PROCEDURE

Article 18 Production Orders are issued by the competent authority directly to the person or service provider concerned. They are by nature **domestic measures** to be provided for under the national law of the ordering Party and therefore need to respect the domestic legislation of the issuing Party and remain subject to legal safeguards (see also section Conditions and safeguards).

6. ENFORCEABILITY

Article 18 of the Budapest Convention does not provide a basis for enforcement in case of a lack of response to production orders issued pursuant to the provision.

Production orders issued under **Article 18(1)(a)**, which are directed at a person located within the Party's territory, are issued and enforceable by the competent authorities in the Party in which the order is sought and granted[31].

Production orders under **Article 18(1)(b)** issued against a service provider established outside the territory of a Party will lack any enforcement mechanism[32]. However, a refusal to provide the required information **may constitute an offence** in accordance with the domestic law of the issuing Party[33].

7. IMPLEMENTATION OF ARTICLE 18 OF THE BUDAPEST CONVENTION IN THE EU MEMBER STATES

The national legislation of the majority of EU Member States allows for the issuance of domestic production orders towards service providers situated abroad, but offering their services in the territory of that particular Member State, where such service providers are in possession or control of the sought information. For more information on some of the EU Member States' legislation implementing Article 18, see Annex II.

8. CHALLENGES

- **Limited scope of application**

In addition to constituting domestic measures without any specific enforcement mechanism (see section Enforceability), Article 18 Production Orders can only be issued towards persons, including service providers, present within a Party's territory (Article 18(1)(a)) or towards service providers offering their services within the territory (Article 18(1)(b)). Moreover, Article 18(1)(b) Production Orders only allow for the production of subscriber information. Therefore, whenever a **territorial link** between the entity in possession or control of the data sought and the territory of the requesting Party **cannot be established**, as well as in instances where **traffic or content data is sought**, competent authorities must resort to other modalities for data acquisition.

- **Potentially conflicting legal obligations for service providers**

Specifically as concerns Article 18(1)(b) Production Orders, service providers who may be addressees

[30] Explanatory Report, para. 148.
[31] Guidance Note #10, p. 6.
[32] See also Guidance Note #10, p. 6, stating that agreement to the Guidance Note "does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State".
[33] See *Yahoo!* Judgment, paras 3-6.

of such orders stemming from foreign authorities remain subject to legal requirements in their country of establishment[34]. The domestic legal framework of their place of establishment may either **allow, prohibit or not specifically regulate** whether service providers may comply with direct requests for data from foreign competent authorities.

The current state of play can cause problems for globally-active service providers which may be addressees of direct requests for cooperation, including production orders with cross-border effects. Specifically, service providers may be put in situations where **abiding by the laws of one country** (e.g. the country issuing an Article 18 Production Order, which may establish that non-compliance with the order constitutes an offence under domestic law) **may make them in breach of the laws of another country** (e.g. their country of establishment, which may prohibit them to respond to direct requests from foreign authorities) and the other way around[35].

8. THE WAY FORWARD

The Budapest Convention was drafted before the rise of cloud computing, when the vast majority of electronic (and other) evidence critical to criminal investigations was held within one's own territorial borders. Considering, among other things, the increased importance of cross-border access to electronic evidence and the need for greater clarity and legal certainty for service providers regarding the circumstances in which they may respond to direct requests for disclosure of electronic data from foreign authorities[36], the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Second Protocol), which was opened for signature to the Parties to the Budapest Convention in May 2022[37].

Among other things, the Second Protocol provides a basis for direct cooperation between competent authorities in one Party and:

- Entities providing domain name registration services in another Party for disclosure of domain name registration information in their possession or control (Article 6); and
- Service providers in another Party for the disclosure of subscriber information in their possession or control (Article 7).

Both provisions have a slightly wider scope of application when compared to Article 18 Production Orders, by **no longer requiring a territorial link with the issuing Party**, but only with another Party to the Second Protocol.

The Second Protocol also requires Parties to "adopt such legislative and other measures as may be necessary" for an entity or service provider subject to an Article 6 or Article 7 order to disclose the requested information[38]. If implemented into national law, these provisions may help address the issues arising from the differing national laws pertaining to whether service providers may respond to direct requests for disclosure of electronic data from foreign authorities.

More information about the Second Protocol, as well as Article 6 and Article 7, is available in the dedicated SIRIUS Quarterly Reviews.

[34] Ibid.
[35] SIRIUS EU Digital Evidence Situation Report 2021, November 2021, p. 35.
[36] Second Protocol, Preamble, p. 1.
[37] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.
[38] Second Protocol, Articles 6(2) and 7(2)(a).

ANNEX I:
APPLYING ARTICLE 18 WITH RESPECT TO SUBSCRIBER INFORMATION[39]

<table>
<tr><td colspan="3">IF
The criminal justice authority has jurisdiction over the offence;</td></tr>
<tr><td colspan="3">AND IF
the service provider is in possession or control of the subscriber information;</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td>Article 18.1.a
The person (service provider) is in the territory of the Party.</td><td>OR</td><td>Article 18.1.b
A Party considers that a service provider is "offering its services in the territory of the Party" when, for example:

- the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);
and
- the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td></td><td></td><td>- the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party.</td></tr>
</table>

[39] Guidance Note #10, p. 9

ANNEX II
DOMESTIC LEGISLATION OF SOME EU MEMBER STATES IMPLEMENTING ARTICLE 18 OF THE BUDAPEST CONVENTION

AUSTRIA

Code of Criminal Procedure

Section 76a – Information on master and access data[40]

(1) Providers of communication services and other service providers (§ 3 Z 2 ECG) are obliged, at the request of criminal police authorities, public prosecutors and courts, in relation to the clarification of the concrete suspicion of a crime committed by a particular person, to provide information on master data of a user (Section 181 Paragraph 9 Telecommunications Act - TKG 2021, Federal Law Gazette I No 190/2021) or users of another service (Section 3 Z 4 ECG).

(2) The same shall apply at the order of the public prosecutor's office (Section 102) for information on the following data mentioned in Section 167 para. 5 Z 2 TKG 2021:

1. The name, address and subscriber identifier of the user to whom a public IP address was assigned at a given time, specifying the underlying time zone, unless this would capture a larger number of subscribers;

2. The user ID assigned to the user when using e-mail services;

3. Name and address of the user to whom an e-mail address was assigned at a particular time; and

4. The e-mail address and the public IP address of the sender of an e-mail.

The provisions of section 138 paragraphs 5 and 139 shall apply *mutatis mutandis* to this order.

BELGIUM

Code of Criminal Procedure

Article 46bis[41]

§ 1. In investigating crimes and offences, the public prosecutor may, by a reasoned and written decision, proceed or make proceed on the basis of any data in his possession, or by means of access to the files of the clients of the actors referred to in the first and second indents of paragraph 2, to:

1) the identification of the subscriber or usual user of a service referred to in the second indent of paragraph 2, or of the means of electronic communication used;

2) identification of the services referred to in the second indent of paragraph 2 to which a specified person is subscribed or which are usually used by a specified person.

To this end, he may, if necessary, require, directly or through the police service designated by the King, the cooperation of:

- the operator of an electronic communications network, and

- any person who makes available or offers, within the Belgian territory, in any way, a service which consists in transmitting signals via electronic communications networks or allowing users to obtain, receive or disseminate information via an electronic communications network. This includes the provider of an electronic communications service.

The justification shall reflect the proportionality with respect to privacy and the subsidiary nature of any other investigative act.

In case of extreme urgency, the public prosecutor may orally order this action. The decision shall be confirmed in writing as soon as possible.

[40] The following constitutes a courtesy translation.
[41] The following constitutes a courtesy translation.

For offences that are not likely to result in a primary correctional sentence of one year or a heavier sentence, the public prosecutor may demand the data referred to in paragraph 1 only for a period of six months prior to his decision.

§ 2. The actors referred to in § 1, paragraph 2, indents 1 and 2, who are requested to communicate the data referred to in paragraph 1 shall communicate the data to the public prosecutor or the judicial police officer in real time or, where applicable, at the time specified in the request, in accordance with the rules determined by the King, on a proposal from the Minister of Justice and the Minister responsible for Telecommunications.

The King determines, after consulting the Committee on the Protection of Privacy and on a proposal from the Minister of Justice and the Minister responsible for Telecommunications, the technical conditions for access to the data referred to in § 1 and available to the public Prosecutor and the police service designated in the same paragraph.

Any person who, by virtue of his function, has knowledge of the measure or provides his assistance to it, shall be bound to keep it secret. Any breach of secrecy shall be punished in accordance with Article 458 of the Penal Code. Any person who refuses to communicate the data or who does not communicate them in real time or, if necessary, at the time specified in the request shall be punished by a fine from twenty-six euros to ten thousand euros.

CYPRUS

Law 183(I)/2007 – Telecommunications Data Retention Act 2007 for the Investigation of Serious Criminal Offenses

Article 4

(1)(a) Subject to the provisions of subsection (2) and (3), and notwithstanding the provisions of paragraph (b), an investigating police officer may gain access to data relating to the investigation of a serious criminal offence, provided that a relevant order is made by the Court.

(b) In case of abduction of a person, the investigating police officer may, by a letter addressed to the telecommunications service provider, be given data relating to the investigation of the abduction of the said person, without receiving in advance an order made by the Court, provided that for this purpose, he has in advance received in writing the approval of the Attorney-General of the Republic and provided that he has placed before him the information and details requested in accordance with subsection (3) for the purposes of the affidavit.

Provided that within forty-eight (48) hours from the date of access to data, as above, the investigating police officer is obliged to receive a relevant order from the Court and in case the Court refuses to make such order, the investigating police officer is obliged, within forty-eight (48) hours form the date of refusal of the Court, to destroy the data which he received and notify immediately the supervisory authority prescribed in the provisions of section 15.

(2) The Attorney-General of the Republic may, following the request of an investigating police officer, approve an application to make the order prescribed in subsection (1), if he is satisfied that the making of an order may provide or has provided evidence for the commission of a serious criminal offence.

(3) The application to make an order prescribed in subsection (1) is written, approved by the Attorney-General of the Republic and accompanied by an affidavit of the investigating police officer, containing the following information and details:

(a) Full status of the investigating police officer;

(b) Full and detailed statement of facts and circumstances upon which the application is based, which shall include:

(i) details of the serious criminal offence committed, is being committed or is expected to be committed,

(ii) general description of the period of time for which access to data is required,

(iii) identity of the person who has committed or is expected to commit the offence and to whom the data access is sought,

(iv) name, address, and profession, if known, of all persons to whom access to their data is considered reasonable to assist the investigation of a serious criminal offence.

(c) report as to which period of time access to data is deemed appropriate and full description of the facts supporting reasonable suspicion or belief that it may be possible that additional data communications will follow of which access is deemed appropriate in investigating a serious criminal offence;

(d) statement of facts concerning all previous applications filed for the making of an order, in which any persons involved are referred to in the application thereof;

(e) statement laying down the results so far of the investigation or logical explanation of the failure to receive such results, when the application concerns extension of the order in force.

Provided that the Judge may require to be provided with further details, or information or evidence in support of the application in the form of a supplementary affidavit or deposition of a witness or otherwise.

(4) The Judge may make the order prescribed in the provisions of subsection (1) as required with the application or with such amendments or with such terms, by which access to data is authorised, only if he is satisfied that based on the facts submitted:

(a) there is reasonable suspicion or possibility, that a person commits, committed or is expected to commit a serious criminal offence;

(b) there is reasonable suspicion or possibility that specific data are connected or are related to a serious criminal offence.

ESTONIA

Code of Criminal Procedure

Section 90[1] – Requiring data from an electronic communications undertaking

(1) A proceedings authority may make an enquiry to an electronic communications undertaking concerning the data required to identify an end user linked to certain identification tokens used in a public electronic communications network, with the exception of data relating to the fact of communication of a message.

(2) On an application of the Prosecutor's Office and with the authorisation of the pre-trial investigation judge in pre-trial proceedings – or of the court in judicial proceedings – an investigative authority may make an enquiry to an electronic communications undertaking concerning data that are listed in subsections 2 and 3 of § 111(1) of the Electronic Communications Act and that are not mentioned in subsection 1 of this section.

(3) An enquiry provided for by subsection 2 of this section may be made if the criminal offence is one listed in subsection 2 of § 1262 of this Code and if it is ineluctably necessary for achieving the purpose of criminal proceedings. In relation to a criminal offence not mentioned in the list, such an enquiry is permitted if it is ineluctably necessary for achieving the purpose of criminal proceedings, justified by the gravity and nature of the offence and does not unjustifiably interfere with personal rights.

(4) An authorisation for an enquiry concerning communication data states:

1) the data that are allowed to be collected by the enquiry;

2) the reason for collecting the data;

3) the period of time concerning which collection of the data is allowed.

(5) An order of the pre-trial investigation judge – or a court order – that disposes of the application of the Prosecutor's Office may be made as a note on the application.

(6) In a situation of urgency where it is not possible to obtain, at the proper time, an authorisation of the pre-trial investigation judge or of the court, an enquiry mentioned in subsection 2 of this section may be made under an authorisation of the Prosecutor's Office which has been given in a form that is reproducible in writing and

contains at least the particulars provided for by clauses 1 and 3 of subsection 4 of this section. In such a case, a reasoned application for allowing the enquiry must be filed with the court within the first business day following its making. The pre-trial investigation judge decides on allowing the enquiry by an order that may be made as a note on the application of the Prosecutor's Office.

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.

Electronic Communications Act

Section 111 – Obligation to preserve data

(1) A communications undertaking is required to preserve the data that are necessary for the performance of the following acts:

1) tracing and identification of the source of communication;

2) identification of the destination of communication;

3) identification of the date, time and duration of communication;

4) identification of the type of communications service;

5) identification of the terminal equipment or presumable terminal equipment of a user of communications services;

6) determining of the location of the terminal equipment.

(2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:

1) the number of the caller and the subscriber's name and address;

2) the number of the recipient and the subscriber's name and address;

3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialed and the subscriber's name and address;

4) the date and time of the beginning and end of the call;

5) the telephone or mobile telephone service used;

6) the international mobile subscriber identity (IMSI) of the caller and the recipient;

7) the international mobile equipment identity (IMEI) of the caller and the recipient;

8) the cell ID at the time of setting up the call;

9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;

10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

(3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data:

1) the user IDs allocated by the communications undertaking;

2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network;

3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

4) the user ID or telephone number of the intended recipient of an Internet telephony call;

5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services;

6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID;

7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone;

8) the Internet service used in the case of electronic mail and Internet telephony services;

9) the number of the caller in the case of dial-up Internet access;

10) the digital subscriber line (DSL) or other end point of the originator of the communication.

[…]

Section 112 – Obligation to provide information

(1) If an agency or authority specified in subsection 111 (11) of this Act submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent, if adherence to the specified terms is possible based on the substance of the request, the agency or authority with information concerning the data specified in subsections 111 (2) and (3) of this Act.

(2) A request specified in subsection (1) of this section shall be submitted in writing or by electronic means. Requests concerning the data specified in clauses 111 (2) 1) and 2) and (3) 3) of the Act may also be submitted in oral form confirming the request with a password. Access to the data specified in subsection (1) of this section may be ensured, on the basis of a written contract, by way of continuous electronic connection.

(3) A communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority and the Police and Border Guard Board on the bases provided for in the Police and Border Guard Act with real time identification of the location of the terminal equipment used in the mobile telephone network.

(4) Access to the data specified in subsection (3) of this section must be ensured on the basis of a written contract and by way of continuous electronic connection.

FRANCE

Code of Criminal Procedure

Article 60-1[42]

The public prosecutor or the judicial police officer or, under the supervision of the latter, the judicial police officer may, by any means, require any person, any private or public institution or body or any public

[42] The following constitutes a courtesy translation.

administration that may hold information relevant to the investigation, including, subject to Article 60-1-2, those resulting from a computerized system or from the processing of personal data, to submit that information to it, in particular in numerical form, where appropriate in accordance with standards laid down by regulation, without being opposed to it, without legitimate grounds, the obligation of professional secrecy. Where the requisitions concern persons mentioned in Articles 56-1 to 56-5, the provision of information may only take place with their consent.

With the exception of the persons mentioned in Articles 56-1 to 56-5, failure to respond to this requisition as soon as possible and if necessary in accordance with the required standards shall be punished by a fine of 3,750 euros.

The evidence obtained by a requisition taken in violation of Article 2 of the Law of 29 July 1881 on Freedom of the Press may not be admitted into evidence on penalty of invalidity.

Article 99-3[43]

The investigating judge or the judicial police officer by him committed may, by any means, require any person, institution or body, private or public, or any public administration that is likely to hold documents relating to the investigation, including, subject to Article 60-1-2, those resulting from a computerized system or from the processing of personal data, to submit those documents to him, in particular in digital form, without being precluded, without legitimate reason, from the obligation of professional secrecy. Where the requisitions concern persons mentioned in sections 56-1 to 56-3 and in section 56-5, the delivery of documents may only take place with their agreement.

In the absence of a response from the person to the requisitions, the provisions of the second paragraph of article 60-1 shall apply.

The last paragraph of Article 60-1 shall also apply.

Where the requisitions relate to data mentioned in article 60-1-1 and issued by a lawyer, they may be made only on reasoned order of the judge of liberty and detention, seized for this purpose by the investigating judge, and the last three paragraphs of Article 60-1-1 shall apply.

GREECE

Code of Criminal Procedure

Article 251 – Tasks of the person who is the person who is responsible for the investigation - principle of proportionality[44]

1. Investigators responsible for investigating criminal investigations under Article 249(2) and (3) must without delay collect information on the crime and its perpetrators, examine witnesses and accused persons, and proceed to an action of self-examination on the spot after taking them with them; if necessary, forensic or other experts, to conduct investigations, to take up evidence and, in general, to act in whatever way is necessary for the collection and maintenance of evidence, and to ensure the trace of crime.

2. During any investigative measure, the investigating judge and the investigating officers must respect the principle of proportionality (Article 25(1) of the Constitution).

LITHUANIA

Code of Criminal Procedure

Article 97 – Exaction of the objects and documents relevant to investigation and prosecution of a criminal offence

A pre-trial investigation officer, a prosecutor and a court have the right to order natural and legal persons to submit objects and documents relevant to the investigation and prosecution of a criminal offense.

[43] The following constitutes a courtesy translation.
[44] The following constitutes a courtesy translation.

Article 155 – Prosecutor's right to access information

(1) The prosecutor, having adopted a decision and received the consent of the pre-trial judge, shall have the right to enter any state or municipal, public or private institution, undertaking or organisation and request access to the necessary documents or other necessary information, to make recordings or copies of the documents and information, or to receive specified information in writing, provided that such access is necessary for the purposes of the investigation of a criminal act.

POLAND

Article 218 – Obligation to hand over correspondence, parcels and data

(1) Offices, institutions and entities operating in the field of postal or telecommunications activities, customs and tax offices, and transport institutions and undertakings are obliged to hand over to the court or the public prosecutor, at the request of the order, the correspondence and parcels and the data referred to in Article 180c of the obligation to retain and store and Article 180d the obligation to ensure conditions for access to and recording of the processed data in the Act of 16 July 2004 – Telecommunications Law (Journal of Laws of 2021, item 576 and of 2022, item 501), if they are relevant to the ongoing proceedings. Only the court or the public prosecutor has the right to open them or order them to be opened.

(2) The order referred to in § 1 shall be served on the addressees of the correspondence and on the subscriber of the telephone or the sender whose list of calls or other communications of information has been issued. Service of the order may be postponed for a specified period of time necessary for the good of the case, but no later than until the final conclusion of the proceedings.

(3) Correspondence and parcels which are not relevant to the criminal proceedings must be returned without delay to the competent authorities, institutions or undertakings referred to in paragraph 1.

Article 236a – Appropriate application of the provisions of the Chapter to the information data or the information system

The provisions of this Chapter shall apply *mutatis mutandis* to the operator and user of a device containing information technology data or an information system, with respect to the data stored in that device or system or on a medium at his disposal or use, including correspondence sent by e-mail.

PORTUGAL

Cybercrime Law

Article 14 - Injunction for providing data or granting access to data

(1) If during the proceedings it becomes necessary for the gathering of evidence in order to ascertain the truth to obtain certain and specific data stored in a given system, the judicial authority orders to the person who has the control or availability of those data to communicate these data or to allow the access to them, under penalty of punishment for disobedience.

(2) The order referred to in the preceding paragraph identifies the data in question.

(3) In compliance with the order described in paragraphs 1 and 2, whoever has the control or availability of such data transmits these data to the competent judicial authority or allows, under penalty of punishment for disobedience, the access to the computer system where they are stored.

(4) The provisions of this Article will apply to service providers, who may be ordered to report data on their customers or subscribers, which would include any information other than the traffic data or the content data, held by the service provider, in order to determine:

a) the type of communication service used, the technical measures taken in this regard and the period of service;

b) the identity, postal or geographic address and telephone number of the subscriber, and any other access number, the data for billing and payment available under a contract or service agreement, or

c) any other information about the location of communication equipment, available under a contract or service agreement.

(5) The injunction contained in this article may not be directed to a suspect or a defendant in that case.

(6) The injunction described under this article is not applicable to obtain data from a computer system used within a legal profession, medical, banking, and journalists activities.

(7) The system of professional secrecy or official and State secrets under Article 182 of the Code of Criminal Procedure shall apply *mutatis mutandis*.

ROMANIA

Code of Criminal Procedure

Article 170 - Surrender of objects, documents or computer data

(1) In the event that there is a reasonable suspicion in relation to the preparation or commission of an offense and there are reasons to believe that an object or document can serve as evidence in a case, the criminal investigation bodies or the court may order the natural person or legal entity holding them to provide and surrender them, subject to receiving proof of surrender.

(2) Also, under the terms of para. (1), criminal investigation bodies or the court may order:

(a) any natural person or legal entity on the territory of Romania to communicate specific computer data in their possession or under their control that is stored in a computer system or on a computer data storage medium;

(b) any provider of public electronic communication networks or provider of electronic communication services intended for the public to communicate specific data referring to subscribers, users and to the provided services that is in its possession or under its control, other than the content of communications and then those specified by Art. 138 para. (1) item j).

(2^1) Natural persons or legal entities, including providers of public electronic communication networks or providers of electronic communication services intended for the public, can ensure the signing of the data requested under para. (2), by using an extended electronic signature based on a qualified certificate issued by an accredited certification service provider.

(2^2) Any authorized person transmitting data requested under para. (2) can sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification service provider, and which allows for an unambiguous identification of the authorized person, thus taking responsibility for the integrity of the transmitted data.

(2^3) Any authorized person receiving data requested under para. (2) can check the integrity of the received data and certify such integrity by signing them, by means of an extended electronic signature based on a qualified certificate issued by an accredited certification service provider, and which allows for an unambiguous identification of the authorized person.

(2^4) Each person certifying data based on an electronic signature shall be liable for the integrity and security of such data under the law.

(2^5) The stipulations of para. (2^1) - (2^4) shall be applied by following the procedures set by the implementation regulations for the applicability of this law.

SLOVAKIA

Code of Criminal Procedure Act no 301/2005 Coll.

Section 90 - Storage and Disclosure of Computer Data

1. If storage of saved computer data including traffic data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings, then the presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of:

a) store such data and maintain the integrity thereof,

b) allow the production or retention of a copy of such data,

c) prevent access to such data,

d) remove such data from the computer system,

e) surrender such data for the purposes of criminal proceedings.

[...]

SLOVENIA

Code of Criminal Procedure

Article 149b

(1) If there are grounds for suspecting that it has been committed, that an offence referred to in the fourth paragraph of the preceding article is being carried out or that an offence referred to in the fourth paragraph of the preceding article is being carried out and that it is necessary to obtain traffic data relating to the communication of the suspect, injured party or persons referred to in the second paragraph of the preceding article in order to detect, prevent or prove that this criminal offence or to detect the offender, on a reasoned proposal by the public prosecutor, the investigating judge may order an operator or information society service provider to communicate to the competent authority relevant information relating to such communication existing at the time when the order was issued. In an order, the investigating judge defines the categories of information it requests. The order shall be served on the operator or information society service provider in so far as it relates to it.

(2) The proposal and the order must be in writing and must contain data allowing the unique identification of the means of communication or user, a justification of the reasons, the relevant period of time for which the data are requested, other relevant circumstances justifying the application of the measure and an appropriate period for enforcement. The identification of the means of communication shall be sufficiently precise to limit the request to a pre-limited and identifiable list of persons.

(3) Exceptionally, if a written order cannot be obtained in time and there is a risk that human life or health would be endangered as a result of the delay, the investigating judge may, on an oral proposal from the public prosecutor, order the measure referred to in the first paragraph of this article to be executed by means of an oral order directly to the operator or information society service provider. The investigating judge makes an official note on the public prosecutor's oral application. The written order must be issued no later than 12 hours after the oral order was issued. If, in the course of the drafting of a written extract, it turns out that the imposed measure was not justified, it shall proceed in accordance with the fourth paragraph of Article 154 of this Act.

(4) An operator or an information society service provider shall not disclose to its user, subscriber or third parties that it has provided or will provide certain information in accordance with this article. It may not disclose this 24 months after the month during which the execution of the order ended. The investigating judge may, by order, set a different time limit, extend the time limit by a maximum of 12 months, but not more than twice, shorten the time limit or annul the prohibition of familiarisation.

(5) Data relating to the content of a communication may not be requested or obtained under this article.

Article 149c

(1) If there are grounds to suspect that it has been committed, that it is being enforced or that an offence is being prepared or organised, for which the offender is being prosecuted *ex officio* and which is punishable by one or more years of imprisonment and it is necessary to obtain traffic data relating to the suspect's communication in order to detect, prevent or prove that offence or to detect the offender, the injured party or persons referred to in the second paragraph of Article 149.a of this Act, or if the lawful user of the means of communication agrees, the investigating judge may, on a reasoned proposal by the public prosecutor, order the operator or information society service provider to start securing the necessary traffic data related to communication and communicating them to the competent authority. The investigating judge must specify in the order the categories of information he requests and the period for which the measure is ordered, which may not exceed three months. By new order, the investigating judge may order the extension of the measure for

three months. If a measure pursuant to Article 150 of this Act is also ordered against the means of communication, the judge may order measures under this article for the entire duration of the execution of the measures referred to in Article 150 of this Act against this means of communication. The order shall be served on the operator or information society service provider in so far as it relates to it.

(2) The proposal and order must be in writing and contain data allowing the unique identification of the means of communication or user, a justification of the reasons, the relevant period of time for which the measure is ordered, the frequency of communication of the information to the competent authority and other relevant circumstances justifying the application of the measure, including an explanation of proportionality. The identification of the means of communication shall be sufficiently precise to limit the request to a pre-limited and identifiable list of persons.

(3) The order may not require the transmission of data relating to the location of the means of communication or user, except for the offences referred to in the fourth paragraph of Article 149.a of this Act or with the consent of the legitimate user of the means of communication.

(4) An operator or an information society service provider shall not disclose to its user, subscriber or third parties that it has provided or will provide certain information in accordance with this article. It may not disclose this 24 months after the month during which the execution of the order ended. The investigating judge may, by order, set a different time limit, extend the time limit by a maximum of 12 months, but not more than twice, shorten the time limit or annul the prohibition of familiarisation. Notwithstanding the provisions of this paragraph, in the case of transmission of data on the basis of the consent of the lawful user, the operator or provider of the information society service shall inform the lawful user about the execution of the order within eight days of the transmission of the data.

(5) Data relating to the content of a communication may not be requested or obtained under this article.

Article 149č

(1) If there are grounds for the suspicion that a criminal offence prosecutable *ex officio* has been committed or is being prepared for which the perpetrator is prosecutable *ex officio* and if, for the purpose of detecting, preventing or proving this criminal offence or detecting the perpetrator, it is necessary to obtain the subscriber data on the owner or the user of a particular communication medium or information service, or on the existence and content of its contractual relationship with the IT operator or information service provider regarding the performance of communication activities or information services, the court, state prosecutor or the police may request in writing that the IT operator or information service provider transmit such information even without the consent of the data subject. The written request must include the legal instruction referred to in paragraph (2) of this article and an indication of the competent court. In the written request, the state prosecutor or the police must specify in detail the categories of requested subscriber data.

(2) The IT operator or information service provider may, for substantiated reasons and at its own expense, submit the requested information together with a copy of the written request to the competent court instead of to the police or the state prosecutor. Upon receipt, the court shall verify the legality of the categories of information stated in the request. If the request also contains information other than subscriber data referred to in paragraph (1) of this article or information that may not be transmitted pursuant to paragraph (4) of this article, the received information shall be destroyed; otherwise, it shall be forwarded to the state prosecutor or the police. In the event of destruction, the investigating judge shall make an official note thereof which shall be sent to the IT operator or information service provider, the head of the competent district state prosecutor's office or the state prosecutor, the ministry responsible for supervising police work and the police.

(3) The IT operator or information service provider may not disclose to its user, subscriber or third parties that it has or will transmit certain information in accordance with this article. Such information may not be disclosed for 24 months after the end of the month in which the data were transmitted. In the event that the IT operator or information service provider receives a court order within this period that refers to the information obtained upon the request referred to in this article, the period of the prohibited disclosure of that request shall be extended until the expiry of the time limit that might be set in the order received. By an order, the investigating

judge or court may set a different time limit, extend it by a maximum of 12 months, but not more than twice, shorten the time limit or remove the prohibition on disclosure.

(4) Under this article, it shall not be possible to request or obtain traffic data related to any identifiable communication, or data that must be obtained by processing data that can only be obtained pursuant to Articles 149b and 149c of this Act. Under this article, it shall also not be possible to request or obtain data relating to the content of communication.

SPAIN

Code of Criminal Procedure

Article 588 ter j. Existing data in the automated files of the service providers

1. The electronic data kept by the service providers or people who facilitate the communication in compliance with the legislation on data retention relating to electronic communications or on their own initiative for commercial reasons or of other nature and that are linked to communication processes, may only be handed over for incorporation into the process with judicial authorization.

2. When the knowledge of such data is indispensable for the investigation, the competent magistrate shall be requested for issuing the authorization to gather the information existing in the automated files of the service providers, including the cross or intelligent search of data, provided that the nature of the data to be known and the reasons justifying the transfer are specified.

Article 588 ter k. Identification through IP number

When in the performance of the duties of prevention and discovery of crimes committed on the internet, the judicial police officer has access to an IP address that was being used for committing a crime, and the identification and location of the equipment or the connectivity device or the user's personal identification data is not recorded, they will require the investigating judge to request the agents subject to the duty of collaboration under Article 588 ter e, the transfer of data allowing the identification and location of the terminal or the connectivity device and the identification of the suspect.

Article 588 ter l. Identification of terminals through capturing identification codes of the device or of its components

1. As long as within the investigation framework it had not been possible to obtain a certain subscriber's number and this was indispensable for the purposes of the inquiry, the Judicial Police officers may use technical devices that allow to gain access to the identification codes or technical labels of the telecommunication device or of some of its components such as IMSI or IMEI number and, in general, of any technical means which, according to the state of technology, is suitable to identify the communication equipment used or the card used to access the telecommunications network.

2. Once the codes allowing the identification of the device or of some of its components have been obtained, the judicial police officer may request the competent magistrate the communications intervention in the terms set forth in Article 588 ter d. The request shall inform the Court on the use of the devices referred to in the preceding subsection.

The Court shall issue a reasoned ruling granting or denying the request for intervention in the period specified in Article 588 bis c.

Article 588 ter m. Identification of the holders or terminals, or connectivity devices

When, in the exercise of their functions, the public prosecutor or judicial police need to know the ownership of a phone number or of any other communication means or, in the opposite sense, require the telephone number or the identifying data of any communication means, can turn directly to the providers of telecommunication services, of access to a telecommunications network or of services of the information society who will be obliged to meet the requirement, under penalty of incurring the offence of disobedience.