Fiches Belges on electronic evidence

1. Definition of electronic evidence

Slovenian criminal procedure code (ZKP) contains several provisions which indirectly define electronic evidence as ***"information/data in an electronic format"*** (see for example Art. 219.a of ZKP)[1].

Moreover the following provisions of the Slovene Electronic Business and Electronic Signature Act (ZEPEP) are also relevant in terms of defining the scope and content of the term electronic evidence:
- *"information/data in an electronic format is data/information which is formatted, saved, sent, received or exchanged electronically"* (see Art. 2 of ZEPEP)
- *data/information in electronic format may not be denied validity or evidentiary value based on the fact that it is in an electronic format"* (see Art. 4 of ZEPEP)

In addition Slovenia ratified by law the Convention on Cybercrime known as the "Budapest convention" (see MKKDP[2]), which among other defines:
- *"computer data" as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; and*
- *"traffic data" as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.*

2. Which measures are possible in your Member State under International Judicial Cooperation?

All measures that are available in our national legislation regarding obtaining and securing electronic evidence for the purposes of identifying the suspect or accused, detecting or apprehending traces of the criminal offence that are important for criminal proceedings and which may be used as evidence in criminal proceedings are also available under International Judicial Cooperation via an MLA request or an EIO. Using the terminology of the Convention on Cybercrime (aka the "Budapest Convention") these would among others be:

- **Expedited preservation of stored computer data;**
- **Expedited preservation and partial disclosure of traffic data;**

[1] As part of Art. 219.a of ZKP reads: *"A search of electronic and associated devices, and electronic data storage device (electronic device) including over the network connected and accessible information systems where data is stored, may be conducted for the purpose of obtaining* ***information in an electronic format*** *when there are grounds for a suspicion a criminal offence was committed and it is likely that the electronic device contains electronic information:*

- *on the basis of which it would be possible to identify the suspect or accused, detect or apprehend traces of the criminal offence that are important for criminal proceedings; or*
- *which may be used as evidence in criminal proceedings. ..."*

[2] Act Ratifying the Convention on Cybercrime and Additional Protocol to the convention on Cybercrime, concerning the Criminalization of Acts of a Racist and Xenophobic Nature committed through Computer Systems (Official Gazette, nr. 17/04).

- **Production order (both for physical persons and for service providers);**
- **Search and seizure of stored computer data;**
- **Real-time collection of traffic data;**
- **Interception of content data;**

It should be noted however that installation of state-sponsored trojan software to users' devices for collecting and gathering of electronic evidence (at the source) is not allowed. Additionally it should also be noted that while the use of IMSI-Catcher devices as a means of intercepting traffic data has been implemented in the last amendments to the Slovene criminal procedure code in 2019 (ZKP-N), the provisions regarding so called IMSI-Catcher devices are currently under constitutional review by the Slovene constitutional court (see Constitutional court decision U-I-144/19-16 from 4.7.2019) and pending its decision the relevant articles are suspended (i.e. IMSI-Catchers are currently not allowed to be used either).

3. Procedure for obtaining electronic evidence

a. National procedures

Depending on how strongly a specific measure in connection to gathering and collecting of electronic evidence impacts/interferes with constitutionally guaranteed freedoms and rights, our Criminal Procedure Act (ZKP) provides for specific conditions and evidentiary standards for each of the available measures. Until such time that an updated translation of all the relevant articles of the Slovene Criminal Procedure Act (ZKP) is provided (see pt. 12 below for currently translated and available precise legal information) you are advised to turn to an EJN contact point for specific precise information regarding the evidentiary standards, thresholds and who can decide/order a specific measure.

In general terms, depending on the severity/intrusiveness of the measure, our legislator limited the availability of the specific measures by prescribing: 1. who decides and can order a specific measure (police/prosecutor/judge), 2. different applicable catalogues of crimes for which specific more intrusive measures are available, 3. specific evidentiary thresholds for using a specific measure (these are, listed in order from lower to higher threshold: *a. reasons for suspicion (razlogi za sum), b. grounded reasons for suspicion (utemeljeni razlogi za sum), c. reasonable suspicion (utemeljen sum))*, 4. limiting the time duration of a specific measure, 5. limiting the duration of the "gag order" prohibiting disclosure by the operator/service provider to the person whose data is being processed that his (data) was transmitted to the authorities.

With respect to disclosure of various data for example there are different regimes for who can order ***disclosure of subscriber data information***, that is the data relating to the owner or user of a specified electronic device and who can order ***disclosure of traffic data***. As a "golden" general rule, if the service provider given the input information (e.g. IP Address) *needs to process other traffic data to* identify the subscriber (e.g. in cases of dynamic IP addresses) it will always be a judge who decides on the production order. In cases where processing traffic data is not necessary to identify the subscriber/user of the electronic device, the police or the prosecutor can also order the service provider to identify and hand over subscriber information (but not the traffic data as well). The described normative framework is the result of our constitutional guarantees that interception of communication can only be ordered by a judge and the doctrine of our constitutional court that (transactional) traffic data even though not being content of communication itself is such

information which is, given its informative value, its functional and constitutional equivalent (i.e. traffic data can be even more revealing and a greater intrusion regarding to the constitutional right to communication privacy than the content of the communication itself - see constitutional court decision Up-106/05 from 2. 10. 2008, available at: http://odlocitve.us-rs.si/en/odlocitev/AN03128?q=106%2F05 the doctrine was further developed by the constitutional court in later decisions among others in U-I-65/13 from, available at: http://odlocitve.us-rs.si/en/odlocitev/AN03707?q=U-I-65%2F13) - meaning that (transactional) traffic data enjoys the same protective constitutional regime as does the content of the communication itself (court order is required).

Given that **temporary freezing/securing of (traffic) data** on its own is a less intrusive preliminary measure (as it does not involve possible later production of the frozen (traffic) data which can only be ordered by a judge), police and prosecutors can demand the so called "data freeze" themselves (Art. 149.e of ZKP). This measure is intended to prevent erasure of electronic evidence, whether they are stored by individuals or legal entities on electronic devices or by the operators of electronic communications or websites. It can be demanded for a list of criminal offences for the purposes of discovering, prevention or proving such offences or for discovering the perpetrators of such offences. The standard of ***reasons for suspicion (razlogi za sum)*** that such offence has been committed or is to be committed or is organized has to be met ***and it also has to be shown that it is likely that the data in question will otherwise be lost or altered by the time of the production order is issued by the court***. The data freeze can last for 30 days from the service of the demand until the receipt of the court order for obtaining such data and can be prolonged for another 30 days. After max 60 days the preservation of the data is abolished, if the court order is not obtained.

The **seizure and search of electronic device** is possible (Article 219.a and 223.a of the Criminal Procedure Act), if ***grounded reasons for suspicion (utemeljeni razlogi za sum)*** exist that the criminal offence was performed and probability exist that there are electronic data on the electronic device, on the basis of which the suspect or accused person can be identified, found, caught or the traces of the criminal offences can be found or that on the electronic device there are electronic data, which can be used as evidence in the criminal procedure. This measure can be carried out on the basis of the individual's consent or on the basis of a court order.

The so-called **subscriber data** can be obtained by the police, state prosecutor or court based on ***reasons for suspicion (razlogi za sum)*** that such offence has been committed or is to be committed or is organized (Article 149.č of the Criminal Procedure Act). According to the Criminal Procedure Act, the service provider is not allowed to inform his user, subscriber or third person that the data has been or will be provided within 24 months after the data has been provided. The judge can order a shorter duration of the "gag order" in any subsequent production order where the initial subscriber data was used and he can also extend it by 12 months, but only twice.

The so-called **traffic data** (Article 149.b of the Criminal Procedure Act, data regarding the communication of the suspect, victim or person for whose communication it is reasonable to suspect that could bring to identification of the suspect) can be obtained for a list of criminal offences, if there are ***reasons for suspicion (razlogi za sum)*** that such offence has been committed or is to be committed or is organized. ***Traffic data can be obtained on the basis of the court order only.*** In specific cases defined by the law this data can also be collected in real time on the basis of the court order (Article 149.c of the Criminal Procedure Act).

The law Criminal procedure code (ZKP) also provides for the possibility of:

- **monitoring of electronic communications using listening and recording devices** and the control and protection of evidence on all forms of communication transmitted over the electronic communications network *(real time interception of communications)*;
- **control of the computer systems of banks or other legal entities** which perform financial or other commercial activities *(real time monitoring of bank transactions)*;
- **listening to and recording of conversations** with the permission of at least one person participating in the conversation.

These measures are possible for the list/catalogue of offences if ***grounded reasons for suspicion (utemeljeni razlogi za sum)*** exist that a certain person has committed, is commiting or is preparing to commit or organizes such criminal offence ***and there is reasonable suspicion (utemeljen sum) that a certain communication means is being used for this offence and there are no other, milder measures that can be used for obtaining evidence (proportionality test)***. These mesures can be obtained on the basis of the court order only.

b. international procedures (including Available channels/ways to obtain electronic evidence from your Member State; urgent procedures; specialised networks to obtain electronic evidence e.g. 24/7 Budapest Convention/police channels)

Slovenia as requesting/issuing state:

In general, national procedures for obtaining e-evidence from abroad (i.e. when Slovenia is requesting or issuing state) are the same as obtaining e-evidence within Slovenia, which means that the same evidentiary standards apply, measures listed above apply for the same lists of offences and the same procedure is applied. If the evidence is to be obtained from abroad, the authority that is competent to issue the decision (e.g. court or prosecutor) is also competent to use the relevant international instrument, make the MLA request (or EIO) that is compliant with the international instrument used and send it to competent authority abroad.

Specifically regarding the **monitoring of electronic communications**, Cooperation in Criminal Matters with the Member States of the European Union Act (Article 77.k) provides for the obligation to notify the other EU Member State in accordance with Art. 31 of the EIO Directive, when monitoring of the electronic communication of a person is ordered in Slovenia, and the person is currently in that state, yet **no technical assistance** is required from this other state. Notification can be sent in advance or *ex post*, depending on the actual knowledge of the whereabouts of the person.

The national court can also issue an European investigation order (EIO) to monitor telecommunication devices in other Member State, whose **technical assistance is needed** in accordance with Art. 30 of the EIO Directive (Article 77.i of the Cooperation in Criminal Matters with the Member States of the European Union Act). National court can also ask the other Member State and its body to make the transcript of the tape or to decrypt it, if the latter agrees with it.

Slovenia as requested/executing state:

With EU Member States: In accordance with national legislation (Art. 65 and 66 of the Cooperation in Criminal Matters with the Member States of the European Union Act) the competent authority executes EIO requesting e-evidence in the same manner and under same conditions as the requested measure is ordered by national authority, i.e. the manner of execution of the requested measure and appropriate measures in accordance with national law (Criminal Procedure Act) are ordered by the authority that orders measure in the national proceedings (court). In cases when

issuing Member State asks for the measure to be ordered in a manner provided by the legislation of that country, the competent authority in Slovenia orders so if such a manner is in accordance with the fundamental principles of the national legal system.

Specifically regarding the **monitoring of electronic communications**, Cooperation in Criminal Matters with the Member States of the European Union Act (Article 77.k) regulates the situation of notification received by the other EU Member State in accordance with Art. 31 of the EIO Directive, when **monitoring of the electronic communication** of a person is ordered in another MS, and the person is currently in Slovenia, yet **no technical assistance** is required from Slovenia. Competent authority in Slovenia for receipt of such notification from another MS is District Court in Ljubljana. This court has obligation to inform the authority that sent the notification if it does not allow the monitoring on the territory of Slovenia or that monitoring should be terminated because such measure would not be allowed in a similar domestic case. The court has to inform the authority of another MS in 96 hours.

If the national court is asked to execute European investigation order on the monitoring of telecommunication it does so, if the conditions of the Slovene Criminal Procedure Act are respected (Article 77.j. of the Cooperation in Criminal Matters with the Member States of the European Union Act). The requesting state can monitor communications directly (if technically that is possible) or the nationally monitored communications can be later provided to it.

With non-EU states: in accordance with national legislation (Art. 516 of the Criminal Procedure Act) the authority competent to order the measure requested by a foreign authority decides about the permissibility of the measure and the manner of enforcement in accordance with national legislation and international agreements. In cases when requesting country asks for the measure to be ordered in a manner provided by the legislation of requesting country, the competent authority in Slovenia may order so if that is in accordance with the fundamental principles of the national criminal proceeding.

Channels of communication:

With EU Member States: the general rule is direct cooperation between competent judicial authorities, in accordance with EIO Directive, except for Denmark and Ireland (channel of communication is central authority);

With non-EU states: The Ministry of Justice of the Republic of Slovenia acts as the Central Authority. Provisions of relevant international instruments (e.g. European Convention on Mutual Assistance in Criminal Matters 1959 and Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 2001) providing for the possibility of direct communication apply in relation to the states that have ratified relevant instruments. Communication via police channels is used in cases provided for in the relevant international instrument that is used in a specific case. Direct communication between judicial authorities and communication through police channels is possible also when no international instrument applies under the condition of reciprocity (Article 515 of the Criminal Procedure Act).

4. International legal framework applicable for this measure in your Member State

International instruments that can be used for obtaining (e-) evidence:

- Convention on Cybercrime of 23 November, 2001, with additional protocol;

- European Convention on Mutual Assistance in Criminal Matters of 20 April, 1959, with additional protocols,
- EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May, 2000;
- European Investigation Order (EIO);
- UN conventions (UN Convention against Transnational Organized Crime of 15 November, 2000; UN Convention against Corruption of 13 October, 2003, UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988);
- Bilateral treaties;
- and in absence of the international or bilateral treaty the principle of reciprocity applies;

5. Competent authority to receive and execute your request

Territorially competent District Courts of Republic of Slovenia and/or in cases of EIO territorially competent District prosecution offices regarding measures that they are competent for.

6. Accepted languages

Are defined in relevant bilateral or international agreements, EIO related requests must be translated in Slovene or English language (preferably Slovene, because translations in English might take longer to process as translations are needed to issue the relevant order to the addressee in Slovene which is the official language in which court orders have to be issued).

7. Definition of data category and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations

Subscriber data are indirectly defined in Article 149.č of the Criminal Procedure Act (ZKP) as data regarding the owner or user of a certain communication device or of a service of information company or data about the existence and content of his contractual relationship with a service provider. The content of the contractual agreement between an individual and the operator is furtherly defined in Electronic Communications Act. The contract should for example include information on the offered service and time of its duration.

Traffic data are defined in Electronic Communications Act (point 45 of the Article 3) as any data processed for the purpose of transmission of communication through an electronic communication network or because of its billing. Typical traffic data are the time and duration of the telephone call among two mobile phones.

Traffic data can be acquired, if the threshold of reasons for suspicion that a criminal offence from the catalogue (which is identical to the one for secret surveillance – i.e. "following" of the suspect) was committed is fulfilled. The mentioned catalogue consists of all *ex officio* prosecuted criminal offences, for which prison sentence of five or more years is prescribed in Slovene criminal code (KZ-1) as well as other individually listed criminal offences, which were chosen on the basis of their nature or gravity of the prescribed sanction.

In narrowly defined cases, such as thefts of the mobile phones (i.e. criminal offences, which are prosecuted *ex officio* and for which at least one year of prison sentence is prescribed), the Criminal Procedure Act allows for gathering of traffic data in "real time", in case that the threshold of reasons for suspicion is shown in the request for the court order.

Content data are not specifically defined in the law. In general, the threshold of specifically grounded reasons for suspicion that a criminal offence, which is prosecuted *ex officio* and is included in the catalogue must be fulfilled (this covers also all such criminal offences for which the prison sentence of at least eight years is prescribed in the Slovene Criminal Code (KZ-1)).

8. Voluntary-disclosure:

According to the national law, the search of the electronic device can be performed on the basis of the written consent of the possessor of such device. Similarly, real time tracking of traffic data in case of stolen mobile phones can be performed on the basis of the consent of the legal user of the phone.

a. As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure.

There are no specific legal provisions, except the general rules on exclusion of evidence in Art. 18 and 84 of Criminal procedure Act (ZKP) pursuant to which the evidence would be excluded from the case file, if the consent was achieved with the violation of the right of the accused or violation of human rights. If such data obtained in a foreign country is to be used in criminal proceedings in Slovenia the court would decide regarding the (in)admissibility of such evidence upon the motion (probably of defence attorney) or ex officio in each individual case based on specific circumstances at the pre-trial hearing at the latest, if not sooner.

b. As executing state: Procedures/legislation in your Member State with regards to the possibility for the OSPs in your Member State to provide data directly to other Member States

Our legislation does not include provisions by which the court could order that data be provided directly to other Member States by OSPs operating in Slovene territory. This is not done in practice either.

9. Data retention periods (including procedures for extensions)

The Constitutional Court declared the previous regulation of data retention as unconstitutional. Consequently, there is currently no legally prescribed retention period. Yet, traffic data are retained for the business (billing etc.) purposes, which is in most cases up to three months and during this period police or state prosecutor can demand data freeze or acquire a court order.

10. Procedure for data preservation/execution deadline

Data freezing can be requested directly by the state prosecutor or police, in case that reasons for suspicion exist that criminal offence, which is prosecuted *ex officio*, was committed or is being committed or is being prepared or organized and that it is probable that the data, which are being stored in electronic form and which can otherwise be acquired by the court order, would already be erased until the court order is issued. Such data freeze request can last until the court order for obtaining the data is actually issued, but no longer than 30 days (state prosecutor or police can prolong the time period with additional request, but for no longer than another 30 days). In exceptional cases data freeze can be ordered orally and then a written request has to be sent in the next 12 hours.

11. Procedure for data production/ execution deadline

Subscriber data

A written request of police or state prosecutor is sufficient. In case that the operator estimates that the request actually covers traffic data, for which the court order should be acquired, he has the possibility of the so-called "motion to quash" - he can send the request to the competent investigative judge, who then destroys the received data (in case that legal requirements are not met and the police/prosecution requests more than it is allowed by law) or in the opposite case sends the requested data to the state prosecutor or the police.

Traffic data

State prosecutor or police must request a court order for the traffic data, which exist at the time when the court order is issued. Both request and court order must be in written form, exceptionally an oral court order can be issued on the oral request of the state prosecutor. In this case a written court order must be issued at latest in 12 hours.

For the so-called real time traffic data tracking, the court order can cover the maximum period of up to three months and this period can be extended for three months with a new order.

Monitoring of electronic communications, control of the computer systems of banks or other legal entities which perform financial or other commercial activities and listening to and recording of conversations with the permission of at least one person participating in the conversation can be performed on the basis of the court order. Both request and court order must be in written form, exceptionally an oral court order can be issued on the oral request of the state prosecutor. In this case a written court order must be issued at latest in 12 hours.

The listed measures can last for a month and they can be prolonged each time for one more month, all together not more than 6 months. If the wiretapping device has been installed in the room (Article 151 of the Criminal Procedure Act), the measures may be prolonged each month for not more than 3 months. The duration of the measures is regulated in Article 152 of the Criminal Procedure Act.

Search of electronic devices

The legal framework is quite detailed and includes also so-called forensic rules. Electronic device is protected, then a copy is made, and the search is performed only on the copy. The search is made on the basis of the written consent of the user of the electronic device or on the basis of the written court order (exceptionally oral court order is issued on the basis of the oral request from the state prosecutor and in 12 hours a written order must be issued or the preserved data must be destroyed).

12. Concise legal practical information

Amendments to the Criminal procedure Act from 2019 (ZKP-N) have not been translated yet. Fiches Belges regarding electronic evidence will be updated with an updated consolidated translation of the relevant articles of the Slovene Criminal Procedure Act (ZKP) once it is translated and made available for publication in English.

Until that time in case more detailed practical information regarding electronic evidence is required please turn to the relevant European judicial network contact (EJN) point in your country and establish direct contact with the relevant Slovene EJN contact point for more concise legal practical information.