SERVICE PROVIDERS AND ELECTRONIC EVIDENCE COLLECTION

Václav Stupka / Juraj Szabó

Václav Stupka, Ph.D., postdoc researcher; Masaryk University, Faculty of Informatics, CERIT and Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: vaclav.stupka@law.muni.cz; https://cyber.law.muni.cz/

Juraj Szabó, Ph.D., researcher and compliance specialist, Masaryk University, Faculty of Informatics, CERIT; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: 232758@mail.muni.cz; https://cyber.law.muni.cz/

Keywords: ***electronic evidence, criminal proceedings, evidence admissibility, evidentiary value, ISP compliance***

Abstract: *This paper deals with cooperation between information service providers and law enforcement authorities. LEAs increasingly demand electronic evidence from the ISPs for criminal investigations and the amount of these requests will likely increase with the implementation of the proposed European legislation on electronic evidence. This paper focuses on the analysis of current Czech and European legislation, practical implementation of procedural rules, and deals with problems that may negatively affect the quality of criminal investigation and cause unnecessary burdens on ISPs. The aim of this paper is to propose a set of compliance measures and procedures through which ISPs could prevent these problems.*

1. Introduction

With the development of the information society and the growing proliferation of information and communication technologies into all human activities the information services providers ("ISPs")[1] are increasingly being asked to assist law enforcement authorities in criminal investigations. This development is related to the growing importance of the information services they provide and the nature of ISPs, which are in the position of defining authorities and influence information interactions and effectively control computing and storage resources.

In general, law enforcement authorities may request a variety of assistance from ISPs. Depending on the nature of the provider concerned and the specific aim of the investigator, it may be, in particular:

- a request for non-content records (for example, various kinds of metadata billing records, transactional records etc.);
- a request to preserve certain records or information (usually to prevent their erasure or loss of their integrity);
- a request to collect communications metadata or implement trap and trace surveillance (of devices or electronic identifiers);
- a request for stored electronic communications (for example, e-mail messages); or
- a request to intercept a subscriber's communications (both analog and digital)
- a request to block access to content (i.e., to prevent the continuation of the crime and further damage)[2].

[1] See definition for the purposes of this paper below.

[2] This taxonomy was inspired by Electronic evidence compliance – a guide for internet service providers, prepared by the U.S. Internet Service Provider Association. Available online here: https://info.publicintelligence.net/USISPAelectronicevidence.pdf. (Accessed on 5 november 2021).

Requests for assistance by the LEA in criminal investigations are in individual countries governed by various laws. Most criminal laws in the EU member states have a long historical background and were drafted long before the digital age[3]. This is the case also in the Czech Republic where relevant procedures are regulated primarily in the Criminal Procedure Code[4], which dates from 1961 and, although it has undergone many amendments, it is still a relatively outdated procedural regulation. Although it specifically regulates certain procedures relating to some kinds of electronic evidence, the common trend among law enforcement authorities is to apply general principles and rules regarding traditional evidence (on collection, exchange and probative value) also to cases involving electronic evidence. This leads to significant problems – from a reduction in the protection of the rights of the persons concerned to inconsistencies in the procedures applied by individual investigators and LEAs. The case law, which is rather scarce and therefore fails to harmonize procedures, does not help in this regard either.

The ISPs must also deal with this complicated situation. They have a duty to provide a certain level of assistance to law enforcement authorities, but they also need to protect their users' rights and their own reputation and business models and prevent the risk of liability and possible damage. Some larger ISPs in Czechia decided to resolve this dilemma by setting up internal rules and procedures, that clarify by whom within the organisation, under what conditions and how should be the assistance to the law enforcement authorities provided, what internal processes should be implemented to when providing the assistance on the part of the ISP, or in what format should be the digital evidence provided. In addition, legal opinions and implemented procedures often differ significantly between individual ISPs. Which leads to a situation where, in some cases, the required assistance is limited or not provided with reference to the ISP's own legal assessment of the request presented by the LEA. This leads to further inconsistencies and delays in criminal proceedings.

To support efforts to find solutions to these issues and appropriate mechanisms for providing assistance, the authors in this article analyze current practice and legislation in the Czech Republic and suggest appropriate compliance measures that ISPs could implement to contribute to improving cooperation with LEAs in criminal proceedings.

2. ISPs and their role in the criminal investigation

Traditionally, the term ISP refers to Internet service providers[5], i.e., telecommunications network operators and providers of connections to these networks. For the purposes of this article, however, we use the abbreviation for the term information service provider, which in addition to the above entities also includes information society service providers, i.e., various information and Internet services – storage, marketplaces, social networks, database services, cloud services, etc.

Similar division applies in principle also in Czech criminal procedure. Due to the differences in applicable legislation, assistance mechanisms differ between providers of electronic communications services (operators of electronic communications infrastructure and providers of connection to these infrastructures) and providers of information society services (all kinds of online services from cloud storage, through electronic marketplaces to social networks).

This division is important for several reasons. The first fundamental reason is that the rules for mandatory data retention applies in the Czech Republic only to the first category of ISPs – network operators and connection

[3] See for instance comparative study in Mifsud Bonnici, J. P., Tudorica, M., & Cannataci, J. A. (2018). The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. In M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci, & F. Turchi (Eds.), Handling and Exchanging Electronic Evidence Across Europe (pp. 189–235). (Law, Governance and Technology Series; Vol. 39). Springer. https://doi.org/10.1007/978-3-319-74872-6_11.

[4] See Czech Act no. 141/1961 Coll. on criminal procedure (criminal procedure code).

[5] Cf. Internet Service Provider (ISP). Techopedia. https://www.techopedia.com/definition/2510/internet-service-provider-isp (accessed on 11. november 2021), 2020.

providers. They are obliged to keep historical metadata about the communication for up to six months. This of course helps with the tracing of perpetrators. The second category of ISP is not required to collect and retain such metadata, but they do so to a large extent for the purposes of their business model, security, accounting or for users.

The second reason is that liability of both categories of ISPs is constructed differently. Liability of the second category of ISPs is regulated only by the Act on some information society services[6], which implements the EU Directive on electronic commerce[7], which mostly deals only with liability in relation to the user content.[8] The second category of ISPs in the Czech Republic has its own legal regulation in the Electronic Communications Act[9], which imposes wider responsibilities and obligations on the protection of content, quality of service, documentation and cooperation with public authorities. This act and its amendments also require ISPs to retain traffic and localisation data, install wiretap devices, provides relatively detailed rules on cooperation with LEAs etc. On the other hand, to fulfill these obligations, in some cases these ISPs are entitled to reimbursement of related costs.

Another aspect that needs to be considered is that not every ISP uses the same technology or deals with the same kinds and amount of data; indeed, there can be radical differences in technology that have a substantial impact both on what the law requires and on what the ISP can do. Thus, both ISPs and law enforcement agencies should be wary of the notion that the capabilities and obligations of one ISP can be applied freely to other ISPs with different technical structures[10].

Thus, the level and extent of cooperation that LEAs can expect from different ISPs can vary significantly. For example, it is not possible to require assistance that is not technically or legally possible (for example, to obtain data encrypted by the user or data that the ISP is required to discard) or at which the ISP incurs disproportionate costs (for example, performing some analytical operations on large repositories to secure requested data).

3. Specifics of electronic evidence

Evidence comes in many different forms. In this paper, we focus on electronic evidence, which which we can define as "any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device".[11] This definition is relatively broad and includes a wide variety of evidence: both physical or traditional (non-electronic) evidence (such as fingerprints, drawing, murder weapon, etc.), which may be digitised for example by taking a digital photo; evidence which was originally obtained in an analogue format (videotape or vinyl) and later digitised; or evidence originally obtained in digital form outputted by a digital device (computer or other similar device). All of these kinds of evidence are, for the purpose of this paper, to be considered "electronic evidences".

In the criminal investigation, the law enforcement authorities require a variety of powers to collect, preserve and exchange (electronic) evidence. These powers might be traditional in nature (interview, surveillance, etc.) but also cyber-specific, such as search and seizure of devices or stored computer data, real-time collection of

6 See Czech Act no. 480/2004 Coll. on information society services.

7 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

8 The second category ISP would be in most cases considered providers of hosting services in relation to act on information society services and the e-commerce directive.

9 See Act no. 127/2005 Coll., on electronic communications.

10 For more on this see Electronic evidence compliance – a guide for internet service providers, prepared by the U.S. Internet Service Provider Association. Available online here: https://info.publicintelligence.net/USISPAelectronicevidence.pdf. (Accessed on 5. november 2021).

11 Definition used in the EVIDENCE Project – Deliverable 2.1 – EVIDENCE Semantic Structure, p. 18.

traffic data and interception and recording of contents of the electronic communication. Electronic evidence may also be collected in variety of forms, like computer files, logs, metadata, computer data, traffic, and location data etc.

Electronic evidence, like any other kinds of evidence, needs to be carefully preserved and handled, ideally by digital forensic experts, in accordance with applicable rules, to be admissible in Court. For example, in the Czech legal system, the (electronic) evidence needs to be legally obtained by the correct kind of Court order[12]. As electronic evidence is highly volatile, which means it can be easily modified, overwritten or deleted, the authenticity of the evidence may also be questioned in Court. Like physical evidence, electronic evidence needs to be authenticated and verified.[13] A clear chain of custody is therefore of the essence here.

The ISP and, subsequently, the investigator should be able to prove where the obtained evidence comes from, how and using what tools the evidence was obtained or extracted, who and how could have edited it, and what evidentiary value may the specific piece of evidence have. Thus, for example, if an ISP has mechanisms in place to ensure a specific workflow for the evidence provided, which ensures the integrity and confidentiality of the process and the evidence itself, the reliability and quality of the evidence will potentially be significantly greater.

It is also important to remember that for the evidence to be obtained legally and therefore admissible in court, it must be secured in accordance with due process, which is somewhat complicated in the Czech legal environment due to the obsolete nature of the Czech criminal procedure legislation, which often forces LEAs to follow procedural rules constructed for completely different purposes[14].

4. Types of assistance

The most common type of assistance provided in criminal proceedings by ISPs to LEAs is real time interception of contents of electronic communication, provision of user or subscriber content data, provision of metadata or operational and location data from information systems and data traffic, so-called freezing, disabling access to data or resources, or monitoring of devices, accounts, and electronic identifiers in real time.

Freezing is simply preserving user data to protect its integrity and availability for further processing in criminal investigation and/or preventing the access to the data or resources, primarily to prevent further criminal activities or their harmful consequences. These are rather specific tools, as their aim is not to directly obtain evidence, but rather to secure it against deterioration or prevent further harm. These tools have been implemented in the Czech Criminal Procedure Code relatively recently and are specifically regulated in § 7b. The reason for the implementation of this regulation was that the Czech Republic was bound to do so by the International Convention on Cybercrime, and so far, freezing has been carried out based on a request from the police for general assistance. In such a case, however, the rights of the entities concerned[15] by this procedural measure were not sufficiently protected.

Other types of assistance are more important in relation to electronic evidence. These can be divided according to whether they are aimed at securing content data (data that is created or processed by the user), or metadata produced by computer systems. Furthermore, the types of assistance can also be categorized according to whether they are data that has been created and is stored somewhere, or that is the subject of electronic communication. The table below classifies individual types of assistance in relation to the abovementioned categoties.

[12] If, for example, the investigator requests content data using court order for traffic data only, such content data would be rendered inadmissible at court.

[13] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 158.

[14] See below in the chapter 4.

[15] Mainly of the ISP and the user who the data or account belong to.

Table 1. Classification of types of assistance

	Historical data	Real time acquisition
Non-Content records (subscriber or transactional data)	**Subscriber data, traffic, and content related metadata** Requires Court order to provide data on telecommunications traffic according to § 88a of the Criminal procedure code.	**Realtime collection of traffic metadata, trap and trace of devices, accounts, and identifiers** Requires Court order to intercept and store electronic communication according to the § 88 of the Criminal procedure code.
Content data	**Stored records and communications data** Requires The court's consent to the monitoring of persons and things according to § 158d para. 3 of the Criminal procedure code.	**Interception of electronic communication** Requires Court order to intercept and store electronic communication according to the § 88 of the Criminal procedure code.

Securing the content of electronic communication is carried out in accordance with § 88 of the Criminal Procedure Code, which allows interception and recording of telecommunications traffic. Interception can only be carried out in the prosecution of the listed serious crimes, only if necessary, and only based on a court order. The interception is regulated in detail in the case of electronic communications network operators and connection providers. Under the Electronic Communications Act, they are obliged to enable the connection of interception devices into their infrastructures and to provide access and necessary assistance to the law enforcement authorities. They are also entitled to reimbursement of reasonable costs related to these duties. In the case of other information society service providers, the situation is a bit more complicated. These providers are also obliged to provide necessary assistance, but the scope of the assistance is not regulated, and they provide it without any reimbursement. Therefore, the LEAs cannot reasonably expect the same level and quality of assistance[16].

Basically, the same is the situation when requesting traffic and location data – such data also may be requested only based on court order, when necessary and in the investigation of listed serious crimes. As in the case of interception, there is specific legislation dealing with network operators and connection providers. They are obliged to retain the listed traffic and location data for a period of six months and, based on a court order, to provide such data to the law enforcement authorities. Here, too, these ISPs are entitled to reimbursement of costs. Other ISPs are not required to retain such data but are still required to provide available metadata to the LEAs on the basis of court order.

A bit more complicated situation applies to stored content data. Czech law enforcement authorities regularly request such data through the provisions of the Criminal Procedure Code regulating the investigative tool for tracing persons and objects. This provision allows LEAs to "[acquire] knowledge about persons and objects in a classified manner by technical or other means", they are also allowed to carry out related "video, audio or other recordings". If such monitoring interferes with "secrecy of the content of documents and records kept in private, it may be carried out only with the prior permission of a judge."[17] This provision clearly aims at completely different activities carried out in the investigation of crimes, but it is being used to obtain retained data solely because the Czech Criminal Procedure Code does not offer any more appropriate means. This

[16] For example, if law enforcement authorities required data from an e-commerce service provider that is not directly available but would have to be extracted through big data analysis. This ISP may refuse to provide such assistance on the grounds of disproportionate costs for such analysis, which are not covered by the requesting authorities.

[17] See § 158d of the Czech Criminal procedure code.

is also a problem in terms of protecting the rights of persons under investigation, as the collection of stored content data can lead to a more significant invasion of privacy than, for example, in case wiretapping, yet in this case the guarantees for the rights of the prosecuted are significantly weaker.

ISPs should, of course, be familiar with these rules and the specifics of each procedural measure and should take their responsibilities into account when setting up internal compliance processes. The following text deals with the identification of suitable tools and rules for setting up related compliance, to protect ISPs as well as rights of their customers and, at the same time, allow smooth cooperation with the LEA.

5. Compliance tools

In relation to the provision of assistance to law enforcement authorities, information service providers may use the following types of compliance measures: procedural, technical, legal, and documentation. However, the application of any of these tools and processes must be adapted to the specific nature of the services provided, the technical capabilities and capacities of the respective provider and the scope and nature of the data being processed. It is therefore appropriate to carry out the necessary procedural and legal analyses in this sense and, ideally, also a risk analysis.

The first and very important tool is setting up of appropriate processes on the part of the organization assisting in securing electronic evidence. The importance of this tool then grows significantly with the size of the organization and the scope and degree of sensitivity of the processed data. Within large transnational ISPs, there should be processes to ensure the whole related workflow including the collection of assistance requests, their evaluation, distribution to those competent to perform the necessary actions and subsequently process the required data into an appropriate format, transmission to the requesting authority as well as related control and documentation responsibilities. A useful tool is also a documented methodology that provides information to the law enforcement authorities – for example, information on where requests should be sent, what category of data is the ISP able to provide, how long the most common types of assistance can take, or in what format and structure is the ISP able to provide the data. These processes can be set up, for example, through an internal guideline or methodology.

It may also be appropriate to have appropriate technical tools for the provision of assistance and electronic evidence. These tools can be of various types – from a simple contact form for sending assistance requests, through various analytical and data mining tools for easy data acquisition and filtering to optional tools for digital forensics and standardization and signing of data outputs. These tools can not only streamline and speed up the entire process of securing data outputs, but also reduce financial and personnel requirements, or they can be dual-use tools that can be used for internal data analysis on the part of the ISP. To ensure a high level of privacy and security, the data that are being provided to the LEA should also be stored in a secure format, the access to such data should be limited strictly on a need-to-know basis and protected against any possible hindering.

As can be seen from in the previous chapters, the procedural rules for securing electronic evidence are problematic and do not provide clear guidelines on how to provide necessary assistance to LEA. Therefore, situations may arise where a law enforcement authority requests assistance illegally or through an inappropriate procedural provision. For this reason, ISPs should conduct an analysis of procedural tools to identify what kind of court or other decisions allow the provision of individual categories of data and establishes an obligation to provide appropriate types of assistance. Such an analysis will then provide the ISP with an argument supporting possible refusing to cooperate or release the data that were requested following legally flawed procedure. Other legal instruments that can be implemented on the part of ISPs are provisions on confidentiality in employment contracts of employees processing LEAs requests, appropriate privacy policies in which users will be informed about the possibility of providing their data to the public authorities, appropriate provisions in contracts with subcontractors allowing access to raw data, etc.

It is also very important to obtain appropriate documentation of all processes and actions performed on the basis of the requests for assistance from the law enforcement authorities. Such documentation may be required, for example, by administrative authorities for checks to ensure the protection of personal data, the integrity of electronic communications, etc. At the same time, they may serve to exclude liability in the event when someone defends themselves against the procedure implemented by the ISP. The documentation can also be used to evaluate and update the set processes, or to identify defects and possible illegal activities.

6. Conclusions

ISPs play an important role in securing electronic evidence in criminal proceedings. In addition, the importance of their role can be expected to grow with the development of the information society, as well as the number of requests for assistance. An increasing number of providers are therefore devoting themselves to setting up appropriate cooperation mechanisms with LEAs to make them more efficient, reduce costs, and eliminate the possibility of procedural liability.

This article therefore deals with the analysis of the Czech legislation on the procedures for obtaining electronic evidence from ISPs in criminal proceedings and describes the role that ISPs play in these processes. Following this analysis, the authors propose procedural, technical, legal and documentation tools that ISPs can implement to achieve their compliance with criminal law regulations and to streamline the assistance they provide.

Acknowledgments and funding

This article is a result of a research project no. VJ01010084 Electronic evidence in criminal proceedings, which was supported by the Ministry of interior of the Czech Republic in a project scheme Strategic support of the security research 2019–2025 (IMPAKT-1). This article expresses opinions of the authors and the project team, these are not the opinions of the institutions the authors represent nor the Ministry of interior.