UDK 343:004.056(437.6)
https://doi.org/10.18485/fb_ic4hs.2018.10

TECHNOLOGIES AND DEVELOPMENT IN VIEW OF TAX CRIMINAL OFFENCES[1][2]

Tomáš STRÉMY[*], Natália HANGÁČOVÁ [**]

Abstract: Nowadays, technologies are developing rapidly and legal systems are not able to react to changes in the society and economy as fast as the perpetrators of individual criminal offences. This fact is particularly notable in the area of economic criminality. Due to the European Union's evolution, European Union's internal market, the digitalisation of economy and the development of new technologies, it is necessary to adapt the legal systems of states to new challenges, in order for them to be able to react to changes in society in an appropriate manner.

Tax criminal offences are committed across a number of states, making cooperation among states necessary as well. Cooperation and mutual assistance should be strengthened, in order to prevent states from losing revenues from taxes, which will be used to finance public services.

These days many companies use clouds as a medium to store data, e.g. data concerning companies' bookkeeping records. In the legislation of the Slovak Republic, there is a special procedural institute for securing data stored in clouds. This is why the data stored in clouds are secured in a different way for the purpose of criminal proceedings than other data/evidence saved or downloaded on personal computers. Using clouds as a place for storing accounting records is a new trend. However, the Slovak Republic has legislation enabling the state to secure data stored in clouds. On the other hand, many problems arise in practice.

It is clear that legislation has to be in compliance with the development of new technologies. Therefore, the following question arises: *"Are technologies a tool of empowerment or vulnerability?"*

---

[1] Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-15 0740.

[2] This paper was supported by the Agency for Research and Development under contract no. APVV-15-0740.

[*] Prof. JUDr., PhD, Faculty of Law, Comenius University in Bratislava, tomasstremy@gmail.com

[**] JUDr, Faculty of Law, Comenius University in Bratislava, natalia.hangacova@flaw.uniba.sk

Keywords: tax criminal offences, mutual assistance in criminal matters, clouds, evidence in criminal law

1. INTRODUCTION

Technologies are our future. In recent years, the European Union has launched several exchange programs (for the exchange of information among the Member States) which use technologies with the aim of preventing tax criminal offences. Council Directive 2008/117/EC also emphasises the fact that the exchange of information between the Member States needs to be strengthened. The basic framework for exchange of information is Council Directive 2006/112/EC. Council Directive 2008/117/EC amends Council Directive 2006/112/EC. The latter was introduced due to the losses that the Member States were suffering as a consequence of value added tax frauds (hereinafter referred to as "VAT frauds"). VAT frauds distort competition in the single market: Member States are losing tax revenues and goods are placed on the market at abnormally low prices as a consequence of companies' fraudulent behaviour.

Technologies themselves are helping in the exchange of information between the Member States of the European Union to facilitate a quick response to required information. Eurojust has its coordination centres and Europol deploys a mobile office which enables real-time information exchange on e.g. VAT frauds.[3] A close cooperation between Eurojust and Europol helps to reveal VAT frauds.

The use of technologies is also helping in the area of situation prevention, where camera systems are installed and used in public places and private premises to protect property against criminality. Property criminality is the most common type of criminality committed in the Slovak Republic.

On the other hand, modernisation and technologies help to facilitate money laundering, where money moves quickly through a number of bank accounts in order to cover its real origin. Money usually comes from illegal activities such as drug trafficking or illicit arms trafficking. Technologies promote a rapid flow of money; however, when businesses use bank transfers, these transactions can be traced. The problem with tracing the transactions arises due to bank secrecy, alternatively known as bank-client confidentiality or financial privacy. Money is moved across a number of Member States or third countries. At this stage, exchange of information is crucial.

Technologies, the Internet and modernisation are lending a hand to cybercrimes as well e.g. hacking, phishing and other forms of frauds committed in cyberspace. This is why technologies should be used to support the fight against tax criminality. In the article, the authors focus on the issues of securing evidence for criminal proceedings stored in clouds and on the videotaking of evidence in criminal proceedings. In the course of securing evidence, a search warrant has to be issued, yet its execution interferes with human rights.

---

[3] A major Europe-wide VAT fraud network busted with the support of Eurojust and Europol. (2018, July 16). Retrieved from http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-03-03.aspx, 15.8.2018.

2. SECURING EVIDENCE IN CLOUDS

In the Slovak Republic, there is a difference between securing evidence downloaded and/or saved on personal computers and evidence which is located in mailboxes or in clouds. This is relevant mainly in connection with tax criminal offences. The issues of cloud storage are not applicable in connection with e.g. the criminal offence of abuse of competition, because cartel agreements are usually not made in writing and non-existent agreements can therefore not be stored in clouds.

Cloud storage is a new phenomenon for businesses. It is a place where companies store data. By virtue of digitalization, companies are increasingly using information technologies for their business activities. Companies claim that they are going green (because e.g. purchase orders, invoices, and bookkeeping records are not kept at the seat of the company physically but are stored electronically in clouds). Cloud storage means that data are stored in an immaterial cloud. Cloud storage providers provide a service and they make the stored data available to their "owners" anytime and anywhere. The owner simply needs to have Internet access. The documents located in mailboxes or in the cloud are accessible on the Internet.

For most people, it seems that clouds are a new phenomenon. However, the first clouds were invented in the 1960s and the first widely used cloud was Amazon's cloud, which was introduced in 2006.

Purchase orders, invoices and bookkeeping records are crucial evidence in criminal proceedings related to tax criminal offences, because they refer to business which was made. However, in carousel frauds the transactions are made only "on paper" most of the time. It is therefore important to confront the transactions declared with witness statements.

When law enforcement agencies need to secure evidence stored in the cloud in criminal proceedings related to tax criminal offences, they need an Order according to § 115 (Interception and recording of telecommunication operation) or § 116 (Notification of telecommunication data) of the Criminal Procedure Act of the Slovak Republic. However, cloud providers cannot grant them access to the content saved in the cloud; under the Order, they are obliged/allowed to give only log-in data such as name/e-mail and password to law enforcement authorities.[4] This is justified by the fact that cloud or e-mail providers are not allowed to store the content of e-mails or content of cloud data.

According to § 130 subparagraph 2 of the Criminal Code Act of the Slovak Republic, *the thing* for the purpose of criminal proceedings is also immaterial information and data from computing technology. Immaterial information and data from computing technology can be secured for the purpose of criminal proceedings using the institute of house search, personal search or search of other premises and land set in § 99 and following the Criminal Procedure Act of the Slovak Republic. The institute of house search is applicable only in cases when the information which will be secured as evidence in criminal proceedings has been saved or downloaded on a computer which was found on the inspected premises. The

[4] Article 116 subparagraph 2 of the Criminal Procedure Act of the Slovak Republic.

institute of house search is not applicable for securing data stored in clouds or in e-mails. In accordance with § 100 subparagraph 1 of the Slovak Criminal Procedure Act, a search warrant is required. The requirement of the search warrant rests on the fact that its execution interferes with human rights such as the right to home liberty as well as the right to privacy. A house search may be executed if there is reasonable suspicion that there is a thing of importance for criminal proceedings (i) in a flat or (ii) on other premises used for housing or (iii) on the premises belonging to them as well as (iv) premises not used for housing and (v) land which is not publicly accessible.[5] Data which are saved on a computer are considered to be a *thing* in terms of § 130 subparagraph 2 of the Criminal Code Act of the Slovak Republic and may be secured and analysed legally if they were secured during a house search when a search warrant was issued.

On the other hand, e-mail communication as well as information in clouds has the character of a telecommunication operation. This information is accessible on the Internet and the Internet is not a *thing* in accordance with the definition enshrined in § 130 of the Criminal Code Act.

The institute of notification of telecommunication data enshrined in § 116 of the Slovak Criminal Procedure Act is applicable in situations where e-mail communication (any communication available on the Internet) needs to be secured for the purpose of criminal proceedings. The notification of telecommunication data refers to electronic communication that has already taken place (not communication running in real time, e.g. having WhatsApp communication where § 115 of the Slovak Criminal Procedure Act is applicable). Communication and information accessible on the Internet (not saved or downloaded on a computer) cannot be secured using the institute of house search.

The conditions for issuing an Order for the notification of telecommunication data are set in § 116 subparagraph 1 and 6 of the Slovak Criminal Procedure Act. Provision § 116 subparagraph 6 refers to the fact that paragraphs 1 to 5 of § 116 also apply to data transmitted via a computer system, i.e. data stored in clouds. An Order for the notification of telecommunication data may be issued in relation to an exhaustive number of criminal offences, but only if the intended purpose cannot be achieved otherwise, if achieving the intended purpose would otherwise be substantially more difficult and if the information is necessary to clarify facts important for criminal proceedings.[6]

In practice, problems arise when the cloud provider has its seat in another Member State or in a third country or when the provider is unknown. In the worst-case scenario, law enforcement agencies will not be granted log-in data and they are prevented from inspecting documents e.g. bookkeeping records stored in the cloud. From this point of view, it seems that technologies may facilitate the commitment of criminal offences, predominantly tax criminal offences, where documentary evidence is crucial.

5 Article 99 subparagraph 1 and 2 of the Criminal Procedure Act of the Slovak Republic.

6 The restrictions for issue of Order for notification of telecommunication data are imposed in order to protect telecommunication secrecy and personal data of individuals.

3. VIDEOTAKING OF EVIDENCE

Another modern type of evidence in criminal law apart from evidence stored in clouds is evidence obtained by videotaking. In the second part of the article, we focus on the issue of videotaking of evidence.

The classification of evidence defines the differences between various types of evidence and determines their relevance for the evidentiary process during criminal proceedings.

Evidence in criminal proceedings is classified according to the subject matter of the accusation, according to the relationship between the evidence and the source of information, according to the relationship between the evidence and the facts to be proven, according to the source of evidence and according to the possibility of its use in criminal proceedings.

According to the possibility of their use in criminal proceedings, two types of evidence are distinguished:

- absolutely void evidence – evidence obtained illegally, which may not be used in the evidentiary process, e.g. a coerced confession of the accused,
- relatively void evidence – evidence with lesser defects that can be used in the criminal proceedings provided that the defects are eliminated, e.g. if the accused signs the pages of the minutes that he did not sign during his examination,
- absolutely valid evidence – evidence obtained legally, by using the means of evidence in accordance with the Criminal Procedure Act.

According to § 119 subparagraph 2 of the Criminal Procedure Act of the Slovak Republic, evidence can be not only what is mentioned as the evidence in this article but everything that can contribute to the clarification of the case and that has been obtained from evidences according to the Criminal Procedure Act of the Slovak Republic or another act. In conclusion, we believe that we could add videotaking of evidence to absolutely valid evidence.

Videoconferencing is a useful tool, which has great potential not only at the national level but also in cross-border situations involving different Member States and even third countries. In cross-border cases, smooth communication between the judicial authorities of the Member States is crucial. Videoconferencing is a possible way of simplifying and encouraging such communication. The advantages of videoconferencing are acknowledged by Union Law, which encourages its use, inter alia, in cross-border taking of evidence, in civil and commercial matters, in the European Small Claims Procedure, or in regulated procedures for its use in criminal proceedings.[7]

It is essential to understand the main purposes of Regulation 1206[8] in order to improve and facilitate judicial cooperation between the Member States. The central theme of Regulation 1206 is that the taking of evidence needs to be efficient and swift. Courts are

---

[7] Torres M. (2018). Cross-border litigation: Videotaking of Evidence within EU Member States. Dispute Resolution International, 12(1), 71.

[8] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

expected to execute a request from other Member States expeditiously.[9] Regulation 1206 provides a certain number of forms to allow reliable communication among courts in the interest of swiftness and limits the cases in which cooperation requests may be refused. Finally, Regulation 1206 tries to minimise the issue of costs as an obstacle to the execution of requests. The EU promulgated the Strategy on European e-Justice (2014–2018), adopted by the Council (Justice and Home Affairs) on 6 December 2013. An e-Justice Action Plan 2014–2018 (the "Action Plan") was also adopted by the Council. This was followed by guidelines on the implementation of the Multiannual European e-Justice Action Plan (2014–2018), which were endorsed by the Council (Justice and Home Affairs) on 4 December 2014, and set out concrete steps to implement the Action Plan by the Working Party on e-Law (e-Justice).[10]

According to Council Act (2000/C 197/01) article 10 paragraph 1, if a person is in one Member State's territory and has to be heard as a witness or expert by the judicial authorities of another Member State, the latter may, where it is not desirable or possible for the person to be heard to appear in its territory in person, request that the hearing take place by videoconference, as provided for in paragraphs 2 to 8 of article 10.

The requested Member State must agree to the hearing by videoconference provided that the use of the videoconference is not contrary to the fundamental principles of its law and on condition that it has the technical means to carry out the hearing. If the requested Member State has no access to the technical means for videoconferencing, such means may be made available to it by the requesting Member State by mutual agreement (article 10 paragraph 2 of 2000/C 197/01).

The paragraph 8 of article 10 of 2000/C 197/01 states that each Member State shall take the necessary measures to ensure that, where witnesses or experts are being heard within its territory in accordance with this Article and refuse to testify when under an obligation to testify or do not testify according to the truth, its national law applies in the same way as if the hearing took place in a national procedure.[11]

If we ask ourselves under what conditions a witness can be heard via videoconferencing or other technical means, the answer would be that before examining the witnesses the court must establish their identity and their relationships to the parties. Furthermore, witnesses must be informed of the significance of the testimony, their rights and obligations, the criminal consequences of giving false testimony, and of their entitlement to witness fees. The court invites the witnesses to describe, in a coherent manner, everything that they know about the subject matter of the examination. The court then asks the witnesses questions that are necessary for supplementing and clarifying their testimony. Witnesses

---

[9] Recital 10 of the Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

[10] Torres M. (2018). Cross-border litigation: Videotaking of Evidence within EU Member States. Dispute Resolution International, 12(1), 72-73.

[11] Council Act (2000/C 197/01) establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

may not be asked tendentious or leading questions. If the parties to the proceedings or expert witnesses are asked any such questions or any questions relating to the legal assessment of the case, the presiding judge will deem the questions inadmissible. The presiding judge decides on the inadmissibility of the questions in an order that is not served and against which no appeal may be lodged. The order only forms part of the transcript of the hearing. Subject to the consent of the parties to the proceedings, the court can organise an oral hearing via videoconferencing or other communication technology facilities.[12]

4. CONCLUSION

The article has dealt with technology as a tool of empowerment or vulnerability. The authors have highlighted the securing of evidence in clouds because cloud storage is a new phenomenon for businesses – it is a place where companies store data. Cloud computing has been one of the most important topics in the field of Information Technology in recent years, and its popularity is rising very fast. According to Forbes contributor Louis Columbus, a key point from an IBM study was that "Cloud computing has rapidly accelerated from 30% of Chief Information Officers (CIOs) mentioning it as a crucial technology for customer engagement in 2009 to 64% in 2014". Every day, many organizations and companies are migrating their services over the cloud, and a great number of companies are considering adopting this technology. But companies' primary obstacle to moving their systems to the cloud concerns security and the constantly increasing number of digital crimes occurring in cloud environments. The authors have also dealt with the videotaking of evidence because the possibility of taking evidence by videoconference has been enthusiastically promoted by the European Union Member States, and it is now legally permissible not only for civil and commercial matters but also for criminal matters. Subject to the consent of the parties to the proceedings, the court can organise an oral hearing via videoconferencing or other communication technology facilities.

5. REFERENCES:

Act no. 301/2005 Coll. Criminal Procedure Act of the Slovak Republic.

Act no. 300/2005 Coll. Criminal Code Act of the Slovak Republic.

BLAŽEK R. (2018) *Trestnoprávne aspekty držania strelných zbraní v Slovenskej republiky*. Bratislava, Slovak Republic: Heureka.

ČENTÉŠ J. a kol. (2017) *Trestný poriadok Veľký komentár.* Bratislava: Bratislava, Slovak Republic: Eurokódex.

Council Act (2000/C 197/01) establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

[12] Taking of evidence – Slovakia. (2018, July 16). Retrieved from https://e-justice.europa.eu/content_taking_of_evidence-76-sk-en.do?member=1#toc_2_12, 15.8.2018.

Council Directive 2008/117/EC of 16 December 2008 amending Directive 2006/112/EC on the common system of value added tax to combat tax evasion connected with intra-Community transactions.

Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC.

Major Europe-wide VAT fraud network busted with the support of Eurojust and Europol. (2018, July 16). Retrieved from http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-03-03.aspx. 15.8.2018.

STRÉMY T., HANGÁČOVÁ N. (2017) *Value Added Tax Frauds (Carousel Frauds)*. Praha, Czech Republic: Leges.

ŠAMKO P. (2017) *Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestnom konaní*. Zo súdnej praxe, 6, 248-252.

Taking of evidence – Slovakia. (2018, July 16). Retrieved from https://e-justice.europa.eu/content_taking_of_evidence-76-sk-en.do?member=1#toc_2_12

Torres M. (2018). *Cross-border litigation: Videotaking of Evidence within EU Member States*. Dispute Resolution International, 12(1), 71-95.