The History of Cybercrime Legislation and Major Achievements

PhD Fabian Peter*

Abstract

The concept of information technology has changed and evolved in line with the independent development of the now interdisciplinary science. Although it is important to note that it is not to be confused with either computer science or cybernetics, even if, with regard to the types of offences covered by this thesis, it is not possible and not necessary to distract from the fact that a computer or computing devices are involved. Technical progress has taken us from the Abacus, through the Turing machine, to today's modern computer. Almost 30 years ago, IT tools and equipment began a process that has made them as ubiquitous in our lives as the invention of the wheel was in the history of mankind. It is imperative that such devices, the data stored in them or used by them, or their accessibility, become a socially protected asset and that certain forms of behaviour are criminalised by the legislator in order to protect them.

This is how information technology – along with other disciplines – has developed a permanent and close link with criminal law. The Hungarian legislation has developed in several stages a separate criminal law regime for information technology. In this thesis, I would like to describe this process, evaluate it through the results of my research and present the specific regulatory system, from the perspective of the expectations of the EU directives.

Two main categories of offences can be identified: the narrower category of information technology offences, where the information system is the object of the offence, i.e., the attack is directed against the computer, and the other category of offences, where the IT system is used as a tool to commit a "regular" crime (fraud, harassment etc.).

Keywords: *cybercrime, computer crime, internet, information system*

I. Introduction

We spend a significant part of our daily lives in the world of the internet, smart devices, we store our valuables in the cyberspace, and our human relationships are also focused on this special dimension. It is through such systems that the State keeps records of our data. It is undeniable that data has become one of the most valuable commodities, and therefore the most defensible and at very high risk. And the crimes once seen in science fiction stories are now not only a part of science fiction but have become a threat to us all.

What do we mean by information technology crime? There is no single definition, nor even a single name, but there is broad consensus that there are two main categories: one category includes offences where the object of the offence is the information system, i.e. the attack is directed against the computer ("cyber-dependent" offences), and the other category includes offences where the information system is the instrument of the offence, or, if you like, the information system is the medium in which the otherwise traditional offence (fraud, harassment, sexual assault etc.) is committed (so-called "cyber-enabled" crimes)[1]. The Hungarian Criminal Code in force – the 2012 Criminal Code[2] – uses the terminology of information technology offence, information system offence, referring to the fact that there is more than just a computer, as the instrument or object of the offence cannot be only the computer, but any information technology device (smartphone, tablet, printer, router etc.), equipment and interconnected system of such devices capable of communication and data transmission[3].

II. International institutional history overview

The first important milestone in the international fight against cybercrime was the initiative of the Organisation for Economic Co-operation and Development (OECD), when an ad hoc committee was set up by the organisation between 1983 and 1985[4], which analysed the experience of European countries with computer-related crime and called for comprehensive legislation in its report "Computer related Crime: Analysis of legal Policy"[5]. In 1996, Belgium and France drafted a multilateral agreement on the Internet, setting out the principles that could guarantee the protection of users' data. This effort is another indication that cybercrime was becoming a growing problem during this period. In 1998, Germany was one of the first countries to set up an independent internet police force (Zentralstelle zur Bekampfung der Internetkriminalitat) within the Federal Criminal Police Office (Bundeskriminalamt)[6].

The next major step in the international legislation was the Council of Europe's expert report[7] published in 1989 and the Recommendation (R89/9) adopted on the basis of it. The latter has defined a catalogue of computer-related offences, with a minimum list of offences that Member States must punish and an optional list of offences that they can penalize at their discretion. The minimum list includes: (1) computer fraud; (2) computer forgery; (3) damage to computer data and programs; (4) illegal

[1] J. Clough, *Principles of cybercrime*, Cambridge University Press, 2015, pp. 10-11.

[2] Act C of 2012 on the Criminal Code (hereinafter referred to as the "Criminal Code").

[3] K. Sorbán, *Viruses and zombies in criminal law. Criminal substantive and procedural issues of information system and data breaches*, in Medias Res 2/2018, issue 8, pp. 369-386.

[4] The 1980s was a defining period for IT. While in 1980 there were less than 1 million personal computers in the world, by 1985 there were more than 30 million computers with the Ms-DOS operating system installed. According to estimates, this means that the total number of computers was over 40 million.

[5] A. Bequai, *Computer-related crime*, European Committee on Crime Problems, Strasbourg, 1990. Available at: http://www.oas.org/juridico/english/89-9&final%20report.pdf.

[6] A permanent internet connection between Germany and China was established back in the 1980s! In the early 1990s, more than 40 million personal computers were sold worldwide every year. The White House and the Vatican has been connected to the Internet and a US court ruling declared that domain names had real property value.

[7] The Select Committee of Experts on Computer-related crime of the Committee on Crime Problems.

entry; (5) unlawful obtaining of secrets; (6) unlawful copying of proprietary computer programs; (7) unlawful copying of semiconductor topographies. The elements of the optional list are: (1) unauthorised alteration of computer data or computer programs; (2) computer espionage; (3) unauthorised use of a computer with intent to cause damage; (4) unauthorised copying and use of proprietary programs[8].

One of the important venues for international action against cybercrime is Budapest, where the Council of Europe adopted the Convention on Cybercrime (Budapest Convention) on 23 November 2001[9], the first multilateral convention to define the relevant concepts (service provider, computer system, computer data etc.) and to make criminal substantive and procedural recommendations to the State Parties.

In 2005, the Council of the European Union adopted Framework Decision 2005/222/JHA on attacks against information systems, with the aim of establishing a "common approach" to the constituent elements of the offences and the applicable sanctions[10]. The Framework Decision was replaced by Directive 2013/40/EU, which established the minimum standards for the constituent elements of computer-related offences and sanctions, and Member States undertook to criminalise – "at least in the most serious cases" – the following offences: unlawful access to information systems, unlawful interference with a system, unlawful interference with data and unlawful acquisition of data, as well as conduct that aims to produce, distribute or otherwise make it available for use the means necessary to commit these offences (computer programs, passwords and access codes etc.)[11].

In 2019, Directive 2019/713/EU on combating fraud and counterfeiting of cash-substitute payment instruments was adopted. While the Directive aims to harmonise the criminal law offences relating to cash substitutes, the EU legislator intends that the provisions of the Directive should also apply to virtual payment instruments (cryptocurrencies), provided that they can be used for payment[12]. Under the Directive, Member States will criminalise the fraudulent use of cash substitutes, offences relating to the fraudulent use of tangible and intangible cash substitutes, information systems fraud (which can be committed with regard to cash, monetary value and virtual payment instruments), the preparatory and ancillary conduct related to these offences, and attempted offences of all of the above offences.

III. Information technology offences under the current criminal code

The Hungarian legislator has placed information technology offences in the stricter sense in two separate chapters with the Criminal Code: in Chapter XLIII we find the unlawful acquisition of data (Section 422 of the Criminal Code), the unauthorised use

[8] N. Mezey, *Cybercrime* (jogiforum.hu), 2007, available at https://www.jogiforum.hu/files/publikaciok/mezey_nandor-szamitogepes_bunozes%5bjogi_forum%5d.pdf.

[9] Act LXXIX of 2004 on the proclamation of the Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001.

[10] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[11] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[12] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 combating fraud and counterfeiting of cash-substitute payment instruments and replacing Council Framework Decision 2001/413/JHA. PE/89/2018/REV/3. OJ L 123, 10.5.2019, pp. 18-29.

of unmanned aircraft (Section 422/A of the Criminal Code), and two offences against information systems, the violation of information systems or data (Section 423 of the Criminal Code) and the circumvention of technical measures ensuring the protection of information systems (Section 424 of the Criminal Code). One additional offence is covered by Chapter XXXVI on offences against property, namely fraud committed by using an information system (Article 375 of the Criminal Code)[13].

1. Fraud using an information system

Fraud committed using an information system – as the name and its place in the system suggests – is essentially a crime against property, a fraudulent offence against property interests. However, there is an important difference compared to normal fraud: while misleading or deceit is a necessary element of normal fraud, in case of fraud using an information system regulated under Section 375 of the Criminal Code, the fraud is committed without deceiving a natural person.

The offence has two forms, malicious misuse of data and misuse of an electronic cash substitute payment instrument. In the first case, the object of the offence is the information system itself or any of its components, or the data relevant to the information system.

The law punishes any conduct that may be capable of influencing the information system and that may cause damage: it is punishable if the offender enters data into the system, changes the data managed in the system, deletes or makes it inaccessible, or influences the operation of the information system by any other action.

Data entry can be the uploading of facts, information or programs, and can be done both online (for example, through electronic intrusion, known as hacking) and offline (for example, by manual data entry, typing or copying from a storage medium). Changing the data practically means modifying, adding, overwriting, or possibly partially deleting the data, while deleting the data means permanently and completely destroying the data. Disabling means that the perpetrator – temporarily or permanently – prevents the authorised person from accessing the data stored on the system (e.g., password protection, but also the installation of malicious software).

The offence is intentional and purposeful, and the offender seeks to obtain unlawful gain. However, this also means that although the offence can only be committed with a direct intent, for the harm to occur, probable intent is also sufficient. Unjust enrichment is not an element of the offence. It is a result linked crime; the result is the damage caused by the unlawful interference with the information system. It is common for the perpetrator to access a financial system and manipulate the bank account balances of customers, for example by transferring funds from one account to another without authorisation: the balance in the victim's account is then reduced and the damage is the loss of value in the customer's funds.

However, according to some authors (e.g., Miklós Hollán), in certain cases the loss of profit may also be relevant, so it would be more appropriate to consider the material loss as a result rather than the loss – as the legislator has already done in the case of "normal" fraud, indicating in the interpretative provisions that the unpaid consideration for the service provided should also be considered as loss. Accordingly,

[13] The chapter (in addition to the footnotes) is based on the following sources: Krisztina Karsai (2021): Major Commentary to Act C of 2012 on the Criminal Code; Explanatory Memorandum to Act C of 2012 on the Criminal Code.

currently the Criminal Code provides different protection depending on whether the offender commits the offence by deceiving a natural person or by making any operation on an information system. It would be appropriate to apply the interpretative provision extending the concept of damage (Section 373(7) of the Criminal Code) also to fraud committed using an information system[14].

As regards the different stages of the offence under Section 375 of the Criminal Code, the offence is completed when the damage has occurred. If the perpetrator has started to interfere with the information system but the damage has not yet occurred, he/she will be liable for attempted interference. The offender can be anyone, the law does not set any special criteria.

The offence has two forms, malicious misuse of data and misuse of an electronic cash substitute payment instrument. The main difference between the two forms is the object of the offence, which in this case is the counterfeit, falsified or unauthorised acquisition of an electronic cash substitute, whether issued domestically or abroad. The Criminal Code defines what constitutes an electronic cash substitute payment instrument in its interpretative provisions, partly by reference to the Credit Institutions Act: the offence can be committed – among others – on a bank card, credit card, electronic voucher, electronic money, such as Erzsébet vouchers or Széchenyi holiday cards[15]. As opposed to this, fraudulent conduct committed on paper (not electronic) cash substitutes is not covered by Section 375 of the Criminal Code, but is listed under normal fraud.

The forms of the criminal offence are the use of a counterfeit, falsified or unauthorised electronic cash substitute payment instrument or the acceptance of payment by such an instrument. Use can mean withdrawing money from the ATM; making a bank transfer; making a purchase at a POS terminal; making an online purchase.

If the perpetrator is in lawful possession of the payment instrument in question (for example, because the victim entrusted it to him), he/she is committing embezzlement by using it without authorisation. Unlike under the previous rules, it is no longer a criminal offence if the cash substitute is used by the holder without authorisation (for example, the cardholder tried to pay after the expiry date of the card).

2. Prohibited data mining

The legal offence of unlawful data mining is intended to protect the right to privacy and the rights derived from it (such as the right to private secrets, the right to personal data, the right to economic and business secrets, the right to privacy in the private home, the right to privacy of correspondence) as established in the Constitution. There are three basic offences: the first is the actual illicit acquisition of data, the second is the covert acquisition of data by an undercover investigator, and the third is the illicit use of data. It is a matter of interpretation whether the offence of using a drone is to be regarded as the fourth type of offence, but the legislator has regulated in a separate section the case where the offender uses an unmanned aircraft to observe the home or other premises of another person, or the fenced area belonging to them, and at the same time records what happens there.

---

[14] M. Hollán, T*he use of services without an intention to pay and criminal law – A dogmatic and legal policy analysis at the dawn of empirical research*, Magyar Jog, 4/2019, pp. 207-208.

[15] Section 6(1)(55) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings.

The legislator basically penalizes the use of secret methods and means which law enforcement authorities are only authorised to use by the authorisation of a judge or a minister: secretly searching another person's home, recording what happens in another person's home using a technical device etc. Strictly speaking, only Section 422(1)(e) of the Criminal Code is related to information systems: the offender "secretly intercepts data handled in an information system and records the intercepted data by means of a technical device". Illegal access to the information system is not an element of the offence: for example, if the offender takes a photograph or screenshot of a computer screen of the right holder, taking advantage of the rightsholder's temporary absence.

3. Information system or data breach

The breach of an information system or data is already a purely information technology crime[16], which the law defines in three forms: unauthorised access, obstruction of operation and misuse of data. In all three cases, the object of the offence is the information system.

In the first form (Section 423(1) of the Criminal Code) the offender unauthorisedly (1) enters the information system, or (2) remains in the information system exceeding the limits of his/her access rights or violating them and does this by violating or circumventing the technical measures intended to ensure the protection of the information system. In the first case, the offender does not have access rights, but in the second case he/she does (e.g. as an employee). It is essential that the information system (network, computer, computer system) is protected by password, code or any other suitable means and that the protection is active. How the unauthorised perpetrator obtains the necessary access data is irrelevant: by social engineering, by hacking, by exploiting the negligence of the authorised person (who, for example, stores the username and password in a prominent place next to the monitor), by using a code recognition program[17].

The offence is intentional but not purposeful, neither profit nor harm is a prerequisite, i.e., the law only punishes mere hacking. If the perpetrator carries out further – now intentional – operations (deleting data etc.) after the unauthorised access, a more serious form of the same offence is committed[18].

The offence may be committed by exceeding the limits of the right of access or by remaining in the system in breach of it. The Criminal Code does not define what is meant by "exceeding the limits of the authorisation" and under what conditions this is punishable. However, in a specific case, the Supreme Court pointed out that exceeding the limits of the authorisation only constitutes a criminal offence if the perpetrator did so by violating or circumventing the technical measures protecting the system. In itself, therefore, "going beyond the limits of the authorisation does not rise to the level of danger required by the first terminology"[19].

In case of the second form (Section 423(2)(a) of the Criminal Code), the offender obstructs the operation of the information system without authorisation or in

---

[16] K. Mezei, *The regulatory challenges of cybercrime in criminal law*, Ügyészek Lapja 4-5/2019. Available at: http://ugyeszeklapja.hu/?p=2592.

[17] K. Mezei, *cited.*

[18] *Idem.*

[19] BH2017. 392. (Kúria Bhar. I. 537/2017.)

violation of the limits of his/her authorisation, while the offender of the third form (Section 423(2)(b) of the Criminal Code), the perpetrator changes, deletes or makes inaccessible the data in the same way. What is meant by data is defined in the Criminal Code. Changing the data can mean either changing the content or the format, or partially deleting it. Erasure is achieved by destroying even a single piece of data. As a result of making the system inaccessible, the data remains hidden from the right holder for a shorter or longer period of time or even permanently.

While it is possible to perform these behaviours individually and manually (by typing in the command), automated operations are now commonplace, and can cause significant harm to a large number of users in a short period of time. Malware is self-replicating, capable of reaching and infecting millions of systems simultaneously (e.g., the *WannaCry* ransomware). A botnet network can be used to launch targeted attacks against multiple systems simultaneously, causing them to shut down completely, but it may also be that it is not a disabling attack, as the botnet controller can gain access to the device and its connections. Botnets can be used for phishing, distributed denial of service (DDoS) attacks, sending spam. They can change the content of a website or overwrite it with their own content[20].

Website corruption, program or data manipulation can be cost-effectively resolved, and data can be copied or modified without loss of quality and without being detected. Malware attacks (spyware, ransomware, computer viruses etc.) target outdated/ inadequately protected systems, exploiting the users' unsuspecting nature (for example, opening an e-mail with a malicious attachment is enough)[21]. Some malware families (such as *WannaCryptor)* infect all systems in their path, others launch targeted attacks, for example against a specific country or its financial, administrative etc. systems (such as *Petya* or *Industroyer*, the latter attacking unprotected industrial control systems used in the electrical grid, including in Ukraine)[22].

It also applies to the offence under Section 423(2) of the Criminal Code that it can only be committed intentionally and purposefully. This is relevant in the case of botnet attacks, in that the owners of remotely controlled, zombie-like systems are not actually aware that their machines are infected, so their perpetrator status is not even an issue. The perpetrator is the botherder, the owner of the master machine, who not only interferes with the operation of the information system targeted by the attack, but also with all the information systems that are infected and ordered to perform the overload attack[23].

The second and third forms of the offence (obstruction and misuse of data) are more serious if the offence involves a significant number of information systems. The Criminal Code does not provide guidance on what is meant by "significant number" in this respect, leaving the interpretation to the courts. An example of a qualified case is a DDoS attack, where the perpetrator launches a DDoS attack from a network of hundreds

---

[20] P. Sabanal, *Thingbots: The Future of Botnets in the Internet of Things*, Security Intelligence, 20 February 2016, https://securityintelligence.com/thingbots-the-future-of-botnets-in-the-internet-of-things/.

[21] B.-J. Koops, *The Internet and its Opportunities for Cybercrime*, Tilburg School Legal Studies Paper, Series No. 9/2011, pp. 740-741.

[22] A. Cherepanov, *Industroyer: Biggest threat to industrial control systems since Stuxnet,* www.welivesecurity.com. ESET. 12 June 2017 Available at: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[23] K. Sorbán, *cited*, p. 378.

of thousands of computers infected with a virus against the attacked website and the infrastructure behind it[24]. However, it is a qualifying case in all cases if the act is directed against the information system or data of a public interest enterprise (Section 423(4) of the Criminal Code).

Concerning this aspect, the Hungarian legislation does not fully comply with the EU rules, as Directive 2013/40/EU states that in the case of attacks against critical infrastructure of the European Union or of a Member State, it is justified to establish more severe legal consequences. The EU concept of critical infrastructure is broader than that of a public interest undertaking under the Criminal Code, which does not cover health and social welfare institutions[25].

IV. Circumvention of a technical measure meant to protect an information system

The offence detailed in Section 424 of the Criminal Code is a sui generis preparatory and auxiliary offence, which is related to fraud committed using an information system (Section 375 of the Criminal Code) and to illicit acquisition of data by means of an electronic communications network or device (Section 422(1)(d) of the Criminal Code), and thirdly, the infringement of an information system or data (Section 423 of the Criminal Code).

Directive 2013/40/EU also provides for the penalisation of preparatory or facilitating offences related to information technology offences. This is based on the realisation that cybercrime has become an industry in its own right, with the software, tools and even the skills needed to launch attacks available on the online black markets of the dark web, and even complete botnet infrastructures.

The offence is committed by anyone who, "for the purpose of committing the offences referred to above, creates, transfers, makes available, obtains or places on the market a) a password or computer program, or makes available to another person b) the economic, technical or organisational knowledge of the creation of a password or computer program".

---

[24] S. Gyányi, *Ddos attacks and how to defend against them*, Hadmérnök Special Issue. Robot wars 7. A scientific conference. 27 November 2007. Available at: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html.

[25] Section 459 of the Criminal Code: "21. Public interest undertaking:

a) public utilities,

b) public transport,

c) electronic communications networks,

d) logistics, payment and IT centres and facilities operated by the universal postal service provider in order to fulfil its public interest tasks,

e) a plant producing war material, military equipment, or the energy or raw materials for plant use".

Critical infrastructure is defined by Council Directive 2008/114/EC as "assets, systems or parts thereof located in a Member State which are essential for the performance of vital social functions, health, safety, security, economic and social well-being of its people, and the disruption or destruction of which would have significant consequences in a Member State if it were to fail to continue to perform those functions". Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). OJ L 345, 23.12.2008, pp. 75-82. Available at: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32008L0114.

Accordingly, the offence has two elements, the first being the creation, transfer, acquisition, distribution or making available to others of a program (code, password etc.). Acquisition means that the offender obtains possession of the program, transfer means giving it to a third party. Placing on the market has a broader meaning than sale, sale for consideration, most commonly understood as transfer to several persons. Making the program (code, password etc.) available to others, which is possible even through passive behaviour (the perpetrator leaves a password in an office used by others, in a place visible to all, such as a piece of paper pinned to a monitor).

In this case the offender is actively involved in the creation of the program (code, password etc.), while in the second case the offender is not actively involved, but only provides the knowledge needed to create the program (code, password etc.). The knowledge transferred can be theoretical or practical, and in terms of its content it can be technical, economic, organisational, or knowledge needed to crack code, write programs etc. The provision of knowledge that does not relate to the creation of the program, which is not factual (e.g., the name of the program, a description of how it works). The provision itself can be realised by active or passive conduct, and whether it is free of charge or for consideration is irrelevant to the offence.

The offence can only be committed intentionally and with a specific purpose, i.e., to commit the offences listed above. The Criminal Code, however, defines a ground for decriminalisation, but only for the perpetrator under Section 424(1)(a) of the Criminal Code: if the person discloses his/her activity to the authority – before the creation of the program (code, password etc.) is notified to the authority in charge of the criminal case – he/she will not be punished. However, it is essential that the perpetrator cooperates with the authorities after his/her report, and hands over what he/she has made and provide assistance to establish the identity of the other persons involved in the making.

V. Conclusion

There is no single, universally accepted definition of offences involving information systems, and even the name is uncertain. The literature distinguishes between two types of offences in this area, in addition to the narrower information technology offences, there are also offences where the information technology system is the instrument of a “normal" crime. The Criminal Code regulates the latter category of offences, fraud committed using an information system, under the heading of offences against property, and dedicates a separate chapter to "real" information technology offences. The Hungarian legislation is basically in line with the relevant EU directive, but – as I have pointed out – some provisions need to be amended (or at least clarified).

References

1. Bequai, A. (1990), *Computer-related crime*, European Committee on Crime Problems, Strasbourg. Available at: http://www.oas.org/juridico/english/89-9&final%20 report.pdf

2. Cherepanov, A. (2017), *Industroyer: Biggest threat to industrial control systems since Stuxnet*, www.welivesecurity.com. ESET. 12 June 2017 Available at: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

3. Clough, J., *Principles of cybercrime*, Cambridge University Press, 2015, pp. 10–11.

4. Gyányi, S. (2007), *Ddos attacks and how to defend against them*, Hadmérnök Special Issue. Robot wars 7. A scientific conference, 27 November 2007. Available at: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html

5. Hollán, M. (2019), T*he use of services without an intention to pay and criminal law – A dogmatic and legal policy analysis at the dawn of empirical research*, Magyar Jog, 4/2019, pp. 207–208

6. Karsai, K. (2021), *Major Commentary to Act C of 2012 on the Criminal Code; Explanatory Memorandum to Act C of 2012 on the Criminal Code*. Available: Complex Legal Directory.

7. Koops, B.-J., *The Internet and its Opportunities for Cybercrime*, Tilburg School Legal Studies Paper, Series No. 9/2011, pp. 740–741.

8. Mezei, K. (2019), *The regulatory challenges of cybercrime in criminal law*, Ügyészek Lapja 4-5/2019. Available at: http://ugyeszeklapja.hu/?p=2592

9. Mezey, N. (2007), *Cybercrime* (jogiforum.hu). https://www.jogiforum.hu/files/publikaciok/mezey_nandor-szamitogepes_bunozes%5bjogi_forum%5d.pdf

10. Sabanal, P. (2016), *Thingbots: The Future of Botnets in the Internet of Things*, Security Intelligence, 20 February 2016. https://securityintelligence.com/thingbots-the-future-of-botnets-in-the-internet-of-things/

11. Sorbán, K. (2018), *Viruses and zombies in criminal law. Criminal substantive and procedural issues of information system and data breaches*, in Medias Res 2/2018, issue 8, pp. 369–386.

12. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

13. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance) OJ L 345, 23 December 2008, pp. 75–82. Available at: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex% 3A32008L0114

14. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

15. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 combating fraud and counterfeiting of cash-substitute payment instruments and replacing Council Framework Decision 2001/413/JHA. PE/89/2018/REV/3.OJL 123, 10.5.2019, p. 18–29.

16. Act LXXIX of 2004 on the proclamation of the Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001.

17. Act C of 2012 on the Criminal Code (hereinafter referred to as the "Criminal Code") and the Explanatory Memorandum to Act C of 2012 on the Criminal Code.

18. Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings.