CYBERCRIME AND COMPUTER-RELATED OFFENCES

JAN STAJNKO, OSKAR PEČE
University of Maribor, Faculty of Law, Maribor, Slovenia
jan.stajnko@um.si, oskar.pece@student-um.si

Abstract The chapter describes crimes that users of online learning platforms usually encounter: the crime of illegal access to an information system, illegal interception, computer forgery, computer fraud, computer insults, and copyright infringements via IT systems. Special attention is given to regulating the aforementioned criminal acts in the Council of Europe Convention on Cybercrime. Some important pieces of legislation with which the EU harmonises this field are also mentioned, primarily Directive 2013/40/EU on attacks on information systems and Framework Decision 2008/913/PNZ on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Keywords:
criminal law,
IT law,
cyberlaw,
cybercrime convention,
EU criminal law,
European criminal law

University of Maribor Press

DOI https://doi.org/10.18690/um.1.2023.7
ISBN 978-961-286-693-8

1 Introduction to Cybercrime

The term cybercrime covers crime connected to the globally connected space called cyberspace. Cybercrime can generally be defined as illegal conduct in which a computer or an information system is a tool or target of prohibited and harmful behaviour.[1] Here, it is important to divide such conduct into two types of cybercrime. Firstly, cybercrime is where the computer or information system is merely a tool (where the target is a person or organisationion). Secondly, in crime, the information system itself is the target. The difference is that the first form of crime requires a lower level of knowledge regarding the use and operation of information systems and often represents a digital form of traditional crime (fraud, extortion, etc.), with the consequences occurring in the material and not the digital domain. The second type of cybercrime, where the information system is the target of illegal conduct, requires, as a rule, a higher level of knowledge about the operation and use of information systems. Moreover, consequences mainly arise in the digital domain (unauthorised entry into the information system, interception of data, disruption of the operation of information systems, etc.).[2]

As cybercrime is on the rise[3], it is necessary to face these problems also in this manual. According to the authors, a list of crimes is discussed that users often encounter when using online learning platforms. These include illegal access to an information system, illegal interception, computer forgery, computer fraud, online defamation and hate speech, and copyright infringements via IT systems.

Users will typically encounter some of these crimes in the role of the victims, as the illegal attack will be directed against them or their information systems (and thus the legally protected goods, which they are the bearer of). In this sense, knowledge of the discussed offences makes sense so that users and professional staff at institutions are aware of them and know when it is appropriate to involve the police and the state prosecutor's office. On the other side, specific criminal acts are described, in which users typically find themselves in the role of the perpetrator (e.g., copyright infringement and online defamation and hate speech). The disclosure of these crimes

[1] M. Šepec, Kibernetski kriminal, 2018, pp. 7-8.
[2] K. Dashora., Cyber Crime in the Society, 2011, pp. 241-242.
[3] N. Y. Conteh and M. D. Royer, The rise in cybercrime and the dynamics of exploiting the human vulnerability factor, 2016, p. 4.

makes sense in the light of the general preventive effect, i.e., as a warning to users to better understand when their behaviour may result even in criminal sanctions.

Although users will be able to find these crimes in national legislation, cybercrime is predominantly an international phenomenon. For this reason, definitions of criminal acts in national criminal law are generally aligned with the corresponding international legal framework. Within the framework of relevant international legislation, the Council of Europe Convention on Cybercrime ("Budapest Convention"), adopted on 23 November 2001 and entered into force on 1 July 2004, will be highlighted. Most European countries ratified it, but also countries outside of Europe such as the USA, Canada and Japan.[4] The Convention contains a fundamental list of (cyber) crimes that should be criminalized by the signatory state.

Furthermore, based on paragraph 1 of Article 83 of the TFEU, the EU also has the competence to harmonize legislation in the field of computer crime. Therefore, the field of cybercrime and related crimes belongs to the so-called "Euro Crimes".[5] Within the EU, this field is, therefore, additionally harmonised. It is necessary to highlight Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks on information systems and to replace Council Framework Decision 2005/222/JHA.[6]

2 Illegal Access to an Information System

The crime of illegal access to an information system is considered a core cybercrime. It is defined already in Article 2 of the Convention, which reflects the interests of organisations and individuals in the management and control of their information systems:[7]

"Each Party shall adopt such legislative and other measures as necessary to establish as criminal offences under its domestic law when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require

[4] J. Clough, A world of difference, 2014, pp. 723-725.
[5] K. Ambos. European criminal law, 2018, p.
[6] For more on the Directive see L. Buono, Fighting cybercrime between legal challenges and practical difficulties, 2016, pp. 345-346.
[7] Council of Europe, Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, 2001, p. 53.

that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system connected to another computer system."

Illegal access to an information system is an act of deliberate, unjustified and illegal entry into an information system or part of it, whereby the crime in question does not concern access to hardware, but access to data content stored in the information system. Unauthorised access to the information system can be carried out via a public or local communication network.

Unauthorised entry into the information system is not given in cases of merely sending e-mails with unwanted or potentially dangerous content. An actual entry into the information system is required, which means access to the data content of the information system.

To understand the problem of unauthorised access to an information system, it is necessary to clarify when such access is considered justified. Access to the information system is justified when the person who accesses the system is the owner of the system or accesses it based on a contractual relationship, authorisation of the owner or (written or verbal) consent of the user. When determining legitimate access, two types of entitlement must be distinguished, namely entitlement for general access and entitlement for access with a specific purpose. In the case of entitlement to general access, the beneficiary can also access the system for a purpose for which the entitlement was not explicitly granted. However, when the beneficiary only has the entitlement to access for a specific, precisely defined purpose (e.g., entitlement to use a computer to search for professional resources in databases), he may not access the information system and use it for another purpose (e.g., login to social networks).

Finally, the difference between unauthorised access to an information system and infringing on an information system should also be clarified. Infringing means any unauthorised access to an information system, which the perpetrator performs when he bypasses the system's security mechanisms or accesses the information system using technical means or another information system. Infringing is a special form of unauthorised access to an information system. Because the criminalisation of any unauthorised access to the information system could be too strict and non-life-

threatening today, the Convention allows the signatory countries to criminalise only that unauthorised access that corresponds to the concept of infringing information systems.[8]

3 Illegal Interception

Communication privacy is based on a reasonable expectation of privacy, protected in Article 8 of the European Convention on Human Rights.[9] In order to protect the right to communication privacy, the Cybercrime Convention provides in Article 3:

»Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.«

Illegal interception (by technical means) refers to listening, monitoring or controlling the content of communications, obtaining the content of data, either directly, through access and use of a computer system, or indirectly, through the use of electronic eavesdropping or listening devices, where interception may also include recording. Technical means include technical devices attached to power lines, as well as devices for collecting and recording wireless communications. They include the use of software with direct access to the information system, as well as devices that read data indirectly, for example through the electromagnetic radiation of the devices (e.g. devices for catching and analysing the electromagnetic radiation of electric currents inside keyboards or keyloggers).[10] The requirement to use technical means is a restrictive qualification, the purpose of which is to prevent excessive expansion of the scope of incrimination.[11] The described interception of computer data is, therefore often carried out without access to the information system, covertly and

[8] M. Šepec, Kibrenetski kriminal, 2018, p. 61-70
[9] Ibid., p. 80
[10] A. Završnik, Napad na informacijski sistem, 2018, pp. 693-694.
[11] Council of Europe, Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, 2001, p. 53.

without the victim's knowledge.[12] However, if the victim becomes aware that his or her computer data has been unlawfully intercepted (e.g., e-mail interception), it is helpful to immediately notify the competent authorities of the suspected criminal offence.

4 Computer-related Forgery

For the crime of forgery, it is essential that the perpetrator wants to create the appearance that a document was issued by a certain person, even though the statement in the document was not really made by this person. Therefore, the creation of a document which contains false or misleading information ("fake news" and the like) does not count as falsification of a document. Instead, the crime of forgery is the production of a document, in which the perpetrator forges a signature (and a stamp) and thereby creates a false impression that the document was issued by a certain person. For example, it is a criminal act of forgery if a person creates a false certificate of the result of a covid-19 test and thereby creates a false impression of the authenticity (credibility) of the issuer of the document. Changes to an existing authentic document, such as changing examination dates or other information on a medical certificate, are treated similarly. If the falsification of the document is done using the information system or if the electronic document is changed, such crime can be considered computer-related forgery.

Article 7 of the Convention on Cybercrime stipulates: »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent before criminal liability attaches.«

[12] See M. Šepec, Kibernetski kriminal, 2018, p. 81

5 Computer-Related Fraud

In essence, fraud means taking advantage by causing harm or misleading another person.[13] Misleading a person is usually related to the perpetrator's false claims about some factual circumstances. The essential element of this criminal act is also the fraudulent intention of the perpetrator - i.e., the intention to obtain a financial benefit or cause property damage. When fraudsters use an information system to commit fraud, such a crime can be considered computer-related fraud. As examples of computer fraud, criminal law theory cites fraudulent sales over the Internet (e.g., through an online platform such as eBay), cash advance fraud or Nigerian frauds (the fraudster allegedly needs an advance to later transfer inherited property and similar), wire fraud (e. g., persuading victims to invest in fictitious funds), fraudulent investments (various forms of fraud with fake websites) and identity theft (the perpetrator obtains financial gain by revealing the victim's identity).[14] Computer fraud can be committed through the information system or against it (e. g., when the perpetrator deceives the information system so that it indirectly causes property damage to the injured party). A special form of cyberfraud is data manipulation, i.e., the change or deletion of data stored and published in the information system, with the aim of misleading another person.[15]

Article 8 of the Convention on Cybercrime stipulates: »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right, the causing of a loss of property to another person by a) any input, alteration, deletion or suppression of computer data, b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or another person.«

6 Computer-Related Defamation and Hate Speech

Information systems can also serve communication that the legislator defines as inadmissible due to interference with a person's reputation (honour and good name). These legal goods are typically offended by crimes such as (computer-related)

[13] Ibid., p. 163.
[14] Ibid., pp. 166-168.
[15] D. Shinder Littlejohn and M. Cross, Scene of the Cybercrime, 2008, p. 22.

defamation. Apart from crimes against reputation, cases of racist and xenophobic insults also ought to be tackled. The basis for criminalising such hate speech is not entirely left to national law. Instead, it can be found in international law, especially in the Additional Protocol to the Convention on Cybercrime, which deals with criminalising racist and xenophobic acts committed in computer systems and entered into force on 1 March 2006. Article 5 of the Additional Protocol stipulates:

»1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

2) A Party may either a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule, or b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.«

The criminalisation of certain forms of hate speech, which is not only related to behaviour within cyberspace, is also harmonised in the EU member states by Council Framework Decision 2008/913/JHA of November 28, 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. At the international level (mainly in the EU), there are also initiatives to include members of the LGBT+ community as one of vulnerable groups, which ought to be protected from hate speech by national legislators by means of criminal law.[16]

7 Copyright Infringement via IT Systems or Digital Piracy

Offences related to copyright infringement through information systems have become one of the most widespread cybercrimes with the development of the Internet and the increasing use of digital media for the distribution of copyrighted

[16] See European Commission, Union of Equality: LGBTIQ Equality Strategy 2020-2025, COM(2020) 698 final, 2020, p. 14.

works.[17] Copyright infringement through information systems, or digital piracy, is the intentional and unjustified exploitation of an author's content through information systems, including the unjustified acquisition, reproduction, use and distribution of protected works (literary, photographic, musical, audio-visual, and other works[18]) as well as other forms of conduct which constitutes copyright infringement.[19] The requirement to criminalise copyright infringement through information systems is set out in Article 10 of the Convention and establishes as a minimum standard of protection criminalisation of copyright infringements of commercial-scale (exploitation for commercial purposes[20]), but does not exclude stricter national criminal provisions, which may also prohibit the unjustified exploitation of author's works in the private sphere or for non-commercial purposes.

In the context of the online educational environment, it is necessary to emphasise two forms of the described criminal offence, namely the creation and submission or publication of plagiarism (seminar papers, diploma theses or other contributions that can be uploaded to the online platform) and the use of protected photographs or images and other works in presentations, without obtaining appropriate permissions from the author. Audio or audio-video recordings of lectures are also controversial. Recording of lecturers on online platforms and their distribution (especially the sale of material obtained in this way) can therefore constitute a criminal offence of copyright infringement.

8 Conclusion

The legislative framework concerning cybercrime is one of the most dynamic and rapidly developing fields of criminal law. The reason for such rapid development is, on the one hand, connected to advancements in information and communications technology and, on the other hand, to the resourcefulness of cyberfraudsters and other cybercriminals. Hence, it is increasingly difficult for national lawgivers as well as international organisations to react to the ever-changing digital environment. The legislative framework regarding cybercrime is, therefore still associated with being full of grey and deregulated areas which need to be tackled in the future. Regardless,

[17] M. Yar, K. F. Steinmetz, Cybercrime and society, 2019, p. 125.
[18] Council of Europe, Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, 2001, p. 9.
[19] See: M. Šepec, Kibrenetski kriminal, 2018, p. 246
[20] See ibid, p. 249.

knowledge of fundamental cybercrime legislation (such as the Budapest Convention and EU legislation on cybercrime) is nonetheless useful for users of online learning platforms. When end users are equipped with such knowledge, they are able to timely report to the competent authorities that they were a victim of a cybercrime. What is more, expanding their knowledge solidifies their understanding of when their online conduct may be treated as illegal or even subject to criminal law sanctions.

Acknowledgements

We would like to thank Assoc. Prof. Dr. Miha Šepec from the University of Maribor for the review and suggestions for improvement of this chapter.

References

Ambos, Kai, European Criminal Law. Cambridge University Press: Cambridge 2018.

Buono, Laviero, Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. ERA Forum, 17(3), 2016, pp. 343-353.

Clough, Jonathan, A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation, Monash University Law Review, 40(3), 2014, pp. 698-736.

Conteh, Nabie Y., and Malcolm D. Royer. "The rise in cybercrime and the dynamics of exploiting the human vulnerability factor." International Journal of Computer, 20 (1), 2016, pp. 1-12.

Council of Europe, Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, 2001.

European Commission, Union of Equality: LGBTIQ Equality Strategy 2020-2025, COM(2020) 698 final, 2020.

Šepec, Miha, Kibernetski kriminal: Kazniva dejanja in kazenskopravna analiza. Univerzitetna založba Univerze v Mariboru: Maribor 2018.

Dashora, Kamini. Cyber crime in the society: Problems and preventions. Journal of Alternative Perspectives in the social sciences, 3(1), 2011, pp. 240-259.

Shinder Littlejohn, Debra, and Cross, Michael, Scene of the Cybercrime, 2nd edition. Szngress Publishing: Burlington 2008.

Yar, Majid, and Steinmetz, Kevin F., Cybercrime and Society, 3rd edition. SAGE: London, 2019.

Završnik, Aleš, Napad na informacijski sistem: 221. člen, in: Veliki znanstveni komentar posebnega dela kazenskega zakonika (KZ-1), 2. knjiga, Korošec, Damjan, Filipčič, Katja, and Zdolšek, Stojan (eds), Zradni list Republike Slovenije: Ljubljana 2018, pp. 676-708.