Contemporary Approaches to Combat Cybercrimes in Ireland

Viktor Shestak[1][a] and Nadezhda Slivinskaya[1][b]
[1]*Moscow State University of International Relations (MGIMO University), Moscow, Russia*

Keywords: Criminal law, cybercrime, cybersecurity, digital technologies, phishing, fraud, cyberspace.

Abstract: The relevance of researching the problem in the field of cybercrime in Ireland lies in the fact that Ireland is a leading EU state in the dissemination and usage of digital technologies, therefore, like in the rest of the developed world, these technologies have begun to play an important role in supporting and facilitating the economic and social life of the country. Information has become a valuable commodity, so the collection and use of digital data is a promising area for international cooperation in the terms of legislation and enforcement. However, the progressive development of digital technologies in Ireland has generated a complex and constantly evolving set of risks, some of which have a coherent and interconnected set of consequences for the state, ranging from the protection of citizens to the protection of central infrastructure and services. The aim of the research is to study the theoretical component of the nature of the concept of "cybercrime", the types of cybercrimes and the differences between them. The main object is to analyze the current legislation of Ireland and the EU in the field of regulation of liability for cybercrimes, as well as non-legislative national instruments and mechanisms designed to combat cybercrime in general. In this regard, the benefit of the scientific article lies in the synthesis and study of the problems and gaps existing in the national legislation of Ireland and the current legal doctrine in the field of cybersecurity, as well as in the search for possible methods and means to improve the mechanism for combating cybercrime.

1 INTRODUCTION

The dynamics of the cybercrime has been recognized as a real threat since long time ago. Sieber suggests that reports of the first attacks on computer systems appeared in the late 1960s. Since then state governments have realized the urgent necessity to adopt special legislation to combat these types of crimes (Cindy J. Smith, 2004).

Clough suggests that the level of cybercrime reflects the real factors necessary for any criminal activity, in particular: the desire to break the law, impunity and benefit, the lack of adequate measures to prevent this type of crime. Global interaction at the speed available on the network entails inherent difficulties in preventing and detecting criminal activity on the net. Consequently, the more time it takes to complete a crime report, the more possibility it gives to the criminals to commit illegal acts, distribute proceeds, and destroy evidence of data. This is the nature of computer networks and the criminal activity that they generate (Clough J., 2012).

The anonymous nature of Internet use and privacy practices that only increase the growth of cybercrime are equally important. The ability to hide behind an artificially created person in the network provides additional security for a person to act with relative impunity (Gura, D. et al, 2020).

Over the past decades, the computer industry has undergone significant changes: data is transferred faster, in large amount and over long distances than ever. Online technology has transcended national and international boundaries. This improvement has led to significant advantages for the economic and financial spheres, since with the opening of the global market, it became possible to communicate directly between clients and legal entities.

The general public has also taken advantages from these developments as social awareness, product availability and simpler means of communication have emerged due to the removal of national barriers.

However, not all of these changes have benefited potential users of information technology. Despite the fact that the Internet is one of the most significant discoveries of the last decades, it can also be called

[a] https://orcid.org/0000-0003-0903-8577
[b] https://orcid.org/0000-0002-9918-5003

Shestak, V. and Slivinskaya, N.
Contemporary Approaches to Combat Cybercrimes in Ireland.
DOI: 10.5220/0010628100003152
In *Proceedings of the VII International Scientific-Practical Conference "Criminal Law and Operative Search Activities: Problems of Legislation, Science and Practice" (CLOSA 2021)*, pages 44-49
ISBN: 978-989-758-532-6; ISSN: 2184-9854

one of the most complex and contradictory both in its structure and in the alternative reality that it creates.

Cybercrime is an area that requires a paradigm shift in approach from both the industry and legislators to protect the public from cybercrimes.

2 MATERIALS AND METHODS

The methodological basis of the existing need to study the theoretical nature of the phenomenon of "cybercrime", types of cybercrime, as well as legislative regulation and methods of combating them, includes various research methods. In particular, while studying the legal nature of the concept of cybercrime, comparative and functional research methods were used. The systematic approach that was used in the analysis of cybercrime in Ireland made it possible to identify four approaches to distinguish cybercrime groups, as well as to study the issue of legislative regulation of the institution of cybercrime in Ireland and strategies to combat it.

3 RESULTS AND DISCUSSION

3.1 Approaches to the Definition of "cybercrime"

Nowadays, there's no generally accepted definition of the term "cybercrime" and no consensus on what cybercrime really is (LNICST, Vol. 53). This term is often used to refer to a number of criminal acts using information and communication technologies (hereinafter refer to as – ICT). The essence of "cybercrime" is periodically characterized by other terms, such as: "virtual crime", "network crime", "high-tech crime", "computer crime". The lack of clarity in understanding the different nature of the above terms has led to the tendency that any crime associated with the use of computer system software, the computer itself or a part of it, is classified as a cybercrime.

It should be noted that two of the six strategies (one of which is Ireland's National Cybersecurity Strategy 2019-2024) don't define and describe this term, but address the problem of cybercrime in common. Thus, in relation to Ireland, the general definition of cybercrime is given on the official website of the Department of Justice and Equality and it's as follows: "Cybercrime comprises traditional offences (e.g. fraud, forgery and identity theft); content related offences (e.g. online distribution of child sexual abuse material, hate speech or incitement to commit acts of terrorism); and offences unique to computers and information systems (e.g. attacks against such systems, spread of malware, hacking to steal sensitive, personal or industry data and denial of service attacks to cause financial and/or reputational damage). Electronic devices are also used to sell and transfer all sorts of illicit goods and services, from illicit drugs to online child sexual abuse and exploitation materials to lists of stolen credit card numbers" (The Department of Justice of Ireland).

3.2 Types of Cybercrimes under Irish Law

Assessing the current state of cybercrime, it should be taken into account what exactly constitutes the object of cybercrime. Consequently, Ireland in its approach to the classification of cybercrimes is guided by widespread, large-scale and automated types of data leak, when such data (personal or any other kind) have become the subject of unauthorized access, collection and use for the purpose of obtaining monetary gain.

Cybercrimes can be divided into several main types. The first type is identity theft. Cybercriminals collect personal information from individuals (e.g. address, date of birth, or bank account details) and use this information online to open fraudulent accounts (such as bank accounts or mortgage-backed security). The second type is cyber extortion. Therefore, it's the type in which an attack or threat is carried out against a legal entity and followed by the requirement to pay a sum of money to prevent or stop a cyberattack. The third type is corporate espionage. It takes many forms: for example, competitors gaining authorized access to confidential data for competitive advantage, or individuals gaining insider knowledge for financial gain. Such actions may include finding out the bid price of a competitor or information about a possible merger or acquisition of the company. The fourth type is intellectual property theft on the Internet (Liu, Z. et al, 2020). Cybercriminals, often sponsored by competing businesses, steal samples, technical drawings, trade secret, and other confidential information that undermine a competitive advantage.

3.3 Cybercrime Law and Approaches to Combat Cybercrimes in Ireland

Ireland's first National Cybersecurity Strategy (2015-2017) (National Cyber Security Strategy, 2015-2017), published in 2015, sets out how the Irish Government will secure the country's computer

networks and associated infrastructure. Key legislative measures under the first strategy (2015–2017) included the introduction of core legislation to formalize agreements and comply with EU requirements for cooperation and reporting opportunities. In this context, a key piece of legislation related to cybercrime in Ireland is the Criminal Justice (Offences relating to information system) Act of 2017 (hereinafter the 2017 Act) (Criminal Justice (offences relating to information system) Act, 2017). The 2017 Act amended the Criminal Damage Act of 1991 (hereinafter the 1991 Act) (Criminal Damage Act, 1991), the Bail Act of 1997 (hereinafter the 1997 Act) (Bail Act, 1997) and the Criminal Justice Act of 2011 (hereinafter the 2011 Act) (Criminal Justice Act, 2011). The Act also includes some of the provisions of EU Directive 2013/40 / EU on attacks against information systems. The EU Directive of 2013 sets out the minimum rules for the definition of criminal offences. The purpose of this Directive is to approximate the criminal legislation of the EU States in the field of attacks on information systems by establishing minimum rules regarding the definition of criminal offences (Directive 2013/40/EU, 2013). Moreover, in accordance with the Criminal Justice (Theft and Fraud) Act of 2001 (hereinafter the 2001 Act) (Criminal Justice (theft and fraud) Act, 2001), the 2017 Act introduces a new crime of "illegal use of a computer", since the Act wasn't originally intended to combat crimes on the Internet (Slevin S., O'Reilly S., 2017). Prior to the entry into force of the 2017 Act, computer crimes were considered in accordance with the 1991 Act and section 9 of the 2001 Act. Consequently, with the advent of the relevant act, some ambiguity of previous legislative acts is eliminated and the concept of "digital" crime is introduced. An interesting aspect of the 2017 Act is that its provisions have extraterritorial application. It means that they may apply not only to a person engaging in such illegal activity in Ireland, but also to a person outside Ireland who gains access to data or damages digital property in Ireland, provided that such action is a crime in this jurisdiction, i.e. the principal of the dual criminality is to be observed.

Thus, it's a comprehensive Act that provides for required legislative updates in this area, it shouldn't be viewed exclusively. The 2011 Act is also relevant as it expands the authority of An Garda Síochána (National Police of Ireland) to investigate white collar crimes, which includes cybercrime. As the representative of An Garda Síochána motioned in his speech, despite the fact that the 2017 Act is complex, cybercrime bodies are still scattered across the acts (Garda National Cyber Crime Bureau). For example, Offences against the State (amendment) Act of 1998 (Offences against the State (amendment) Act,1998) also deals with cybercrime. Section 15 of the 2011 Act states that "for the purpose of investigating a related offence, a member of An Garda Síochána may file a motion with a District Court judge to issue an order under this section regarding: 1) the person has provided any specific documents or documents with a specific description; 2) the provision of certain information with respect to a person by answering questions or statements". These additional powers are vital to investigate cybercrimes, as cybercrime is considered to be a complex crime and generally falls within the scope of this Act.

Moreover, recently in 2018, the provisions of the EU Enforcement Directive (hereinafter - LED) (Directive (EU) 2016/680, 2016) and the General Data Protection Regulation (hereinafter - GDPR) (GDPR, 2018) were implemented into the Ireland legislation. LED establishes the personal data processing for law enforcement purposes, which is outside the realm of the GDPR. The LED provisions are incorporated in Part 5 (personal data processing for law enforcement purposes) of the Data Protection Act 2018 (Data Protection Act, 2018). Also, Ireland has implemented into national legislation the provisions of the following directives in three categories. The first category is data protection. The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") and the Data Protection Acts from 1988 to 2018 ("DPA") govern the collection and processing of personal data in Ireland. Data collection units must take "appropriate security measures" against unauthorized access, alteration, disclosure or destruction of data, in particular when the processing involves transmission of data over a network, and comply with strict reporting obligations (Stepenko V. et al, 2021). The second category is electronic privacy. The Electronic Privacy Regulation of 2011 (S.I. No. 336 of 2011), which implemented the Electronic Privacy Directive 2002/58/EU (as amended by Directives 2006/24/ EU and 2009/136/EU) ("Privacy Policy"), regulate the order in which the providers of public telecommunication networks or services process personal data, and require providers to take appropriate technical and organizational measures to ensure the security of their services. It also prohibits interception or surveillance of messages and related traffic data through public electronic communication services without the consent of users. The third category is payment services. The Payment Services Directive II (Directive 2015/2366/EU or "PSD2") was

implemented and came into force on the basis of the European Union (Payment Services) Regulation 2018 (S.I. 6 of 2018) (“Payment Services Regulation”). Regulatory technical standards (which have been published by the European Banking Authority) will provide “strong customer authentication” and payment service providers will have to inform the national competent authority in the event of serious incidents regarding transactions or their safe operation. Providers should also notify customers if any incident affects the financial interests of payment service users. The Network and Information Systems Security Directive 2016/1148/EU (“NISD”) has been implemented into Irish legislation in accordance with S.I. 360/2018 European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (“NISD Regulation”) (Cybersecurity laws and regulations, 2021). Statute (S.I.) No. 360 of 2018 transposed the EU Directive on the Security of Networks and Information Systems (NIS Directive, 2016) into Irish legislation. Such a move represents “a significant change in the EU countries' approach to cybersecurity and includes a shift in approach to a more formal type of regulatory relationship in certain key sectors (NCSC, official website).

As part of a tendency to combat cybercrime, Ireland has introduced a new National Cybersecurity Strategy. Over the period 2019-2024, the Government of Ireland will implement the following systematic measures to protect the country, develop the cybersecurity sector and deepen international cooperation in combating cybercrime in the future: 1)the National Cyber Security Centre will be further developed, particularly with regard to expand its ability to monitor and respond to cyber security incidents; 2) threat intelligence and analysis prepared by the National Cybersecurity Center will be integrated into the work of the National Security Analysis Center; 3)the existing Critical National Infrastructure Protection system flowing from the NIS Directive will continue to be deployed and developed, with particular focus on the ongoing compliance and audit programs to mitigate risks to key services; 4) the NCSC, with the assistance of the Defense Forces and An Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber-attack; 5) the existing Critical National Infrastructure protection system will be expanded and deepened over the life of the Strategy to cover a broader range of Critical National Infrastructure, including aspects of the electoral system; 6) Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the state; 7) The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies; 8) a Government IT Security Forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard; 9) The National Cybersecurity Center will issue recommendations on the use of special software and hardware in government IT and telecommunications infrastructure; 10) enterprise Ireland will develop a cyber security program to facilitate collaborative links between enterprise and the research community that leads to the practical application of research in business; 11) Government will develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision. A detailed implementation plan of action related to these measures, including timelines and responsible organizations, are set out in the Appendix to the National Strategy (National Cyber Security Strategy, 2019-2024).

Among other measures to combat cybercrime, the following three methods can be distinguished: 1) "beacons" (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content); 2) "honeypots" (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organization to detect and counteract attempts to attack its network without causing any damage to the organization’s real network or data); 3) "sinkholes" (i.e. measures to re-direct malicious traffic away from an organization’s own IP addresses and servers, commonly used to prevent DDoS attacks).

With regard to penalties, in relation to offences under the 2017 Act, the penalties range from a maximum imprisonment of one year and a maximum fine of € 5,000 for charges brought “on a summary basis” (for less serious offences) to a maximum five years’ imprisonment (10 years in case of DDoS attacks) and a unlimited fine for more serious crimes. Crimes under the 2001 Act are only tried in the Circuit Court, with ”making a gain or causing a loss by deception” carrying a maximum penalty of 5 years’ imprisonment and an unlimited fine, and forgery and “unlawful use of a computer” offences

carrying a maximum of 10 years and an unlimited fine.

Despite such a complex legal regulation, one important aspect that negatively affects the functioning of the entire mechanism of combating cybercrime is reporting. Manning (Manning C., 2016) pinpoints that cybercrime cases are often not reported. Accordingly, if such cases aren’t reported, then prosecution is doubtfully possible. As a result, there is no complete picture of the degree or scale of the problem, which means that the effectiveness and feasibility of the developed system is called into a question.

4 RESULTS

Ireland is one of the leading countries in the European Union in the dissemination and use of digital technologies. As in the rest of the world, these technologies have begun to play a key role in the support and development of all spheres of the state. However, the dynamic development of cyberspace has led to an increase in organised crime. Several fundamental challenges arise in the process of developing a cybersecurity strategy in Ireland.

First of all, it’s worth mentioning that the legal nature of such a criminal act as "cybercrime" hasn’t been enshrined at the Irish legislation yet, it means that the acts and statutes of Ireland don’t contain a provision that would clearly describe the objective side of the act being committed. Such a problem leads to an incorrect classification of criminal acts in the field of digital technologies, and therefore to the lack of adequate methods of combating them.

Secondly, it’s necessary to introduce and enforce a new act that would consolidate the whole classification of types of cybercrime. In fact, all cybercrimes in Ireland can be divided into four groups and each of them provide for separate elements of criminal body. The problem lies in the variety of existing legislative acts, the provisions of which provide for responsibility in the field of information technology.

The last problem is the lack of clear statistics on the recording of cybercrimes. According to the latest data, the information indicated in the statistics reflects the number of appeals to An Garda Síochána by individuals rather than legal entities. The reluctance of legal entities to provide a report on the security status of their information system, as well as on the cyberattacks, is explained by the motivation to preserve their business reputation. However, this approach leads to the fact that the legislator doesn’t have real data on the number of cybercrimes committed, which means that he won’t be able to provide preventive measures and improve the mechanism for combating cybercrime in Ireland.

5 CONCLUSION

Ireland is one of those countries where the increase in cybercrime poses a real threat to both the public and private sectors. The abundance of theoretical literature suggests that there are significant gaps in the current mechanism for combating cybercrime.

Despite such a complex legislative regulation, the corpus delicti is enshrined in a large number of legislative acts, the content and legal nature of which are significantly different from the original concept of "cybercrime". Thus, it’s necessary, first of all, to introduce into the legislative base a definition of the concept of "cybercrime", which would include a comprehensive description of the objective side of the criminal acts committed in this area.

Secondly, a new legal act should be introduced, which would contain all the elements of cybercrime with reference norms to the current legislation. Such a solution will simplify the qualification of digital crimes and help to improve the mechanism for combating cybercrime.

Thirdly, the National Cybersecurity Center of Ireland should establish a system of constant monitoring and control of legal entities for cyber-attacks, the availability of information system security software and qualified personnel, as well as compliance with the rules established by National Cybersecurity Strategy 2019-2024. Such a scheme will allow to recreate real statistics of cybercrime, which means that the National Cybersecurity Center will be able to take all the necessary measures to combat it.

Given the global nature of cyberspace and the need for international law enforcement cooperation to effectively combat cybercrime, Irish legislation should continue to take into account global legislative initiatives and best practices.

REFERENCES

Bail Act. 1997, http://www.irishstatutebook.ie/.

Cindy, J. S., 2004. Crime and Technology, New Frontiers for Regulations. Law Enforcement and Research. pp. 105-110.

Clough, J., 2015. Principles of Cybercrime, *In Cambridge University Press*, p.4.

Criminal Justice (Offences relating to information system) Act, 2017, http://www.irishstatutebook.ie/.

Criminal Justice (theft and fraud) Act, 2001.

Criminal Damage Act, 1991, http://www.irishstatutebook.ie/.
Criminal Justice Act, 2011, http://www.irishstatutebook.ie/.
Cybersecurity Laws and Regulations, 2021,https://iclg.com/practice-areas/.
Data protection Act, 2018, http://www.irishstatutebook.ie/.
Dealing with the problem of Cybercrime. *In LNICST*. 53.
Directive (EU), 2016/680, 2016. *In Official Journal of the European Union.*
Directive 2013/40/EU, 2013. *In Official Journal of the European Union.*
Garda National Cyber Crime Bureau (GNCCB), organized and serious crime, https://www.ncsc.gov.ie/.
General Data Protection Regulation (GDPR), 2018, https://gdpr-info.eu.
Gura, D., Khudyakova, N., et al., 2020. Chatbot design issues: building intelligence with the Cartesian paradigm. *In Evol. Intel*.
Liu, Z., et al. *Issues of crowdsourcing and mobile app development through the intellectual property protection of third parties. Peer-to-Peer Netw*., 2020.
Manning, C., 2016. Old Laws, New crimes: Challenges of Prosecuting cybercrime in Ireland. *In Cork Institute of Technology*.
National Cyber security Strategy 2019-2024 (Government of Ireland), https://www.gov.ie/.
National Cyber security Strategy 2015-2017, https://www.gov.ie/.
NCSC Ireland official website, https://www.ncsc.gov.ie.
Offences against the State (amendment) Act, 1998.
Official Website of The Department of Justice of Ireland, cybercrime, http://www.justice.ie/.
Slevin, S., O'Reilly, S., 2017. Dedicated cybercrime legislation in Ireland: Worth the wait? Cyber and Data Protection.
Stepenko, V., Dreval, L., et al., 2021. EU Personal Data Protection Standards and Regulatory Framework. *In Journal of Applied Security Research*.