CYBER CRIME

Cybercrime

Cybercrime

edited by Agnieszka Gryszczyńska

Wydawnictwo Instytutu Wymiaru Sprawiedliwości **Warszawa 2024**

The publication was written within the framework of the international scientific project "Polish-Hungarian Research Platform" conducted by the Institute of Justice in Warsaw in 2023

REVIEWERS *dr hab. Piotr Sowiński, prof. UR*
dr Krzysztof Mucha, UO

PROOFREADING *Lingua Lab*

TYPESETTING *Wiaczesław Krysztal* AT ONCE

COVER DESIGN *Alicja Paradzińska* AT ONCE

ISBN 978-83-67149-76-1

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI
ul. Krakowskie Przedmieście 25, 00-071 Warszawa
SEKRETARIAT tel.: (22) 630 94 53, e-mail: wydawnictwo@iws.gov.pl

BOUND AND PRINTED BY *"Elpil", ul. Artyleryjska 11, 08-110 Siedlce*

Table of Contents

DR HAB. AGNIESZKA GRYSZCZYŃSKA, PROF. UKSW
Cardinal Stefan Wyszyński University in Warsaw | DOI: 10.32041/9788367149761/0

Preface

We present a monograph summarising the research conducted in 2023 by an international Polish-Hungarian research team on the new trends, challenges and solutions in combating cybercrime. The team was established as part of the Polish-Hungarian Research Platform project organised by the Institute of Justice in Warsaw. The team was composed of Piotr Burczaniuk, Judit Jacsò, Agnieszka Gryszczyńska, Erika Róth, Ferenc Sántha and Rafał Wielki.

The rapid development of digital technology has caused an evolution in criminal behaviour, as it creates opportunities for previously unknown forms of crime. The term "cybercrime" is nowadays widely used, especially in the Council of Europe's Cybercrime Convention, international and national literature, incident reports, scientific publications and the mass media. However, it remains unclear what exactly the terminology means and difficulties in understanding cybercrime also arise from the diversity of terminology and the inconsistency of legislation on cybercrime in different countries.

Meanwhile, analysis of reports on the security of networks and information systems indicates an increasing number of incidents. Certain incidents described in the reports also constitute offences – cybercrimes. Additionally added to the problems associated with defining cybercrime, it is also necessary to overlay the terminology

associated with incidents and particular types of attacks in order to better understand the phenomenon of cybercrime.

The modus operandi of perpetrators of cybercrimes is characterised by a high degree of adaptability to the current economic, geopolitical, and social situation. Perpetrators exploit loopholes in the law, adapting the modus operandi to regulatory changes on an ongoing basis. They make use of modern technological solutions (ICT, AI/ML) that allow them to remain anonymous, communicate efficiently and transfer the proceeds of cybercrime.

In order to conceal their own identity, they create a new identity or use the data of other individuals, use services and technical tools that make it difficult or impossible to analyse network traffic (TOR), determine the IP address assigned to them by the telecommunication network providers (VPN, PROXY), encrypt data and their carriers and use anti-forensics techniques. Crimes are committed by them individually as well as within highly specialised and organised criminal syndicates. The attribution of the attack and the identification of the perpetrators is hampered by the cross-border nature of cybercrime – manifested, among other things, by the need to collect evidence in different jurisdictions.

Considering the increasing number of incidents and cybercrimes and their consequences, research is required to identify solutions that would facilitate the detection of offenders and increase the effectiveness of criminal proceedings.

In view of these identified problems, the main research hypothesis that is being tested in this monograph is the hypothesis that the effectiveness of countering of cybercrime is determined not only by the scope of criminalisation and substantive criminal and procedural law, but additionally there is a need for an ecosystem of criminal, administrative and civil regulations, both at the national and international levels.

To verify this hypothesis, the individual chapters of the monograph address the verification of the following researched questions:

- Is there a generally accepted definition of cybercrime, and is it possible to develop a new classification of cybercrimes that takes into account the latest trends of this form of criminality?

- Does the scope of criminalisation of cybercrime need to be expanded due to the continuous development of tactics, techniques and procedures used by cybercriminals?
- Is there a need to define new forms or methods of money laundering?
- Are current measures in the European Union adequate to combat money laundering?
- Are traditional jurisdictional principles in national and international criminal law able to meet the challenges of cybercrime, in particular positive jurisdictional conflicts?
- Are the responsibilities and international cooperation of cyber security actors and law enforcement agencies carrying out reconnaissance activities sufficient, given the nature of the current types of cybercrime, and what are the most significant challenges in this area that require legislative activity?
- What are the effective coercive measures in cybercrime cases?
- What are the specificities of electronic evidence and how should the rules for their preservation be regulated?
- Should new cybersecurity responsibilities be imposed on digital service providers, and should efforts be made to enhance end-user cyber awareness?
- Is the key to effectively countering cybercrime to correlate the scope of the services' operational and investigative powers with the level of technological development of ICT systems, software and services?

In order to verify main research hypothesis, the first step was to examine the definitions and systematisation of cybercrime. The research conducted by Ferenc Sántha in Chapter 1 indicates that the definition of cybercrime and the categorisation of criminal offences are of great importance for a number of reasons. From a legal perspective, a unified definition of cybercrimes can facilitate the harmonisation of national cybercrime legislation. Presently, there are notable discrepancies between European countries with regard to the categorisation of illicit acts perpetrated in cyberspace as criminal offences. Moreover, international cooperation in criminal matters and efforts to combat cybercrime may be more effective if national legislation governing cybercrime is based on

the same principles and if the designation and statutory definition of the crimes can be aligned and harmonised to the greatest extent possible. In conclusion, a unified definition of cybercrimes and the associated statistical methods and metrics will facilitate a more comprehensive understanding of the true scope of cyber-criminality and enable a more precise measurement of the crimes.

The main conclusion of the review of international, Hungarian (Ferenc Sántha) and Polish (Agnieszka Gryszczyńska) literature, is that there is no universally accepted definition of cybercrime. This fact has led to various definitions put forward by researchers and international organisations. The two-factor approach (dividing cybercrime into "cyber-dependent" and "cyber-enabled") is dominant in the academic literature. This may be because that this definition makes a simple but clear distinction between types of cybercrime. As Ferenc Sántha pointed out, the most popular definitions of cybercrime are those that refer to broader categorisations of cybercrime, namely typologies and taxonomies. Considering the scope, a taxonomy of cybercrimes based on the Budapest Convention and its First Additional Protocol is presented more broadly. The classification system of the Budapest Convention (and its First Additional Protocol) contains 13 different cybercrimes in five categories. The first category is *offences against the confidentiality, integrity and availability of computer data and systems*, including illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5) and misuse of devices (Article 6). The second group is *computer-related offences*, which include computer-related forgery (Article 7) and computer-related fraud (Article 8); the third is *content-related offences* which in the Convention are offences related to child pornography (Article 9); the fourth is *offences related to infringements of copyright and related rights* (Article 10). Finally, under the Additional Protocol, the fifth category covers *acts of a racist and xenophobic nature committed through computer systems*, which include the dissemination of racist and xenophobic material through computer systems (Article 3), racism- and xenophobia-motivated threat (Article 4), racism- and xenophobia-motivated insult (Article 5), denial, gross minimisation, approval or justification of genocide

or crimes against humanity (Article 6). The Budapest Convention was also the basis for an analysis of the scope of criminalisation of cybercrime in Poland (Agnieszka Gryszczyńska) and Hungary (Ferenc Sántha).

The research presented in Chapter 2 on the scope of criminalisation of cybercrime in Poland indicates that in Poland, there is no legal definition of cybercrime or a statutory catalogue of acts deemed to be cybercrimes, while the criminal conducts that may be deemed cybercrimes is dispersed and, in addition to the Criminal Code, also includes administrative law regulations containing articles introducing criminal liability and defining the elements of the offences. With regard to the scope of criminalisation of cybercrime in Poland, Agnieszka Gryszczyńska points out that the work of the Council of Europe (Budapest Convention) and the EU (Directive 2013/40/EU) has had the greatest influence on the shape of criminal regulations in Poland. The criticised slowness of changes to criminal code provisions relating to cybercrime is in stark contrast to the speed of extra-code provisions resulting from ad hoc measures related to the increase in specific attacks or the exploration of gaps and vulnerabilities (e.g., CLI spoofing and smishing). In order to ensure regulatory consistency, it is advisable to limit the placement of criminal law provisions outside the Criminal Code.

The empirical research on the number of incidents and cybercrimes analysed in Chapter 2 shows a significant increase in the number of incidents and a growing number of cybercrime cases. A problem with the empirical research and the mapping of incidents onto a cybercrime taxonomy is the lack of a uniform classification for CSIRT teams and law enforcement agencies. The lack of a uniform and acceptable classification also hinders the cross-border exchange of information between CSIRT teams and law enforcement authorities as well as the research and analysis of the most serious threats. In order to increase knowledge on current threats, reliable data from multiple entities is necessary. Quantitative studies show that prosecutors are most likely to pursue cases involving fraud committed online. The grounds for criminalisation included in cyber-dependent crimes are not common grounds for registering cases at the prosecutor's office.

Apart from the critical remarks concerning the correct and consistent with the Convention on Cybercrime characterisation of the elements of individual cybercrimes in Poland, after the introduction of criminal liability for abuse of electronic communication, currently the scope of criminalisation of cybercrime in Poland does not need to be expanded. Definitely greater deficiencies are diagnosed in the procedural provisions. However, it should be mentioned that the scope of criminalisation of cybercrime in Poland may be influenced by the ongoing work of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes.

Finally, Agnieszka Gryszczyńska points out that the development of cybercrime leads to the need for constant evaluation and improvement of existing legal regulations, as changes in the threat landscape must be followed by changes in substantive and procedural law. Undoubtedly, another trigger for change will be the need to include criminal liability related to the use or abuse of disruptive technologies.

Research conducted in the area of money laundering by Judit Jacsó (Chapters 3 and 4) indicates that the development of the digital technologies had opened the door to new types and methods of criminal activity, which is true for the laundering of money as well. It is the reason that cybercrime and money laundering is one of the biggest challenges of our time. It should be stressed that money laundering is a constantly changing phenomenon. Hence, the combat against money laundering is a continuously developing area, which can be seen in the international, the EU and the domestic regulation as well. Cyber-laundering is a term that combines cybercrime and money laundering, representing the convergence of these two illicit activities, that is why the combat against it is a special challenge. However, the purpose of cyber-laundering is no different from the traditional form of money laundering, i.e., it aims to make it impossible to identify the origin of illegally acquired money derived from a crime.

New technologies create new methods for the commission of money laundering, which requires the legislators and the law

enforcement bodies to create and use new measures. Offenders increasingly use innovative technologies to launder criminal assets. The COVID-19 epidemic, the expansion of the new payment technologies and innovative payment system has given new power to the spread of cybercrime in parallel of money laundering. It is difficult to estimate the scale of money laundering, given the high latency rate for legalised amounts. The same can be established with regard to cyber-laundering.

One of the most important questions in connection with money laundering is the scope of the predicate offence. The fight against money laundering was initially similar to the fight against organised crime (including drug trafficking). But today the so-called all-crime approach became significant, which means that all criminal activity could be a predicate offence of money laundering. It means that the crimes in the field of cybercrime can also be a predicate offence of money laundering, if it results in financial advantage or assets.

Crypto assets should be given special attention as an object of money laundering. Crypto (currency) assets have expanded into practically every country and sector in the last decades. Cryptocurrency is being abused to commit new forms of crime and to launder the proceeds of crimes, however, the unique characteristics of blockchain-based technologies offer an unprecedented opportunity to investigate organised crime and money laundering networks and to recover the illicit asset. It is essential that crypto assets be treated as any other asset for the purposes of AML/CFT supervision and enforcement; likewise, it is important to bring the crypto assets (and service providers) into existing AML/CFT frameworks, and such laws should be broad enough to cover crypto assets and have the capacity to anticipate future evolutions in the crypto industry. In addition, the need for training, adequate communication and increased cooperation between public and private actors in the AML regime was also stated.

The cross-border nature of money laundering and of the cyber-laundering cases is also a significant factor that makes it difficult to combat these crimes and to identify perpetrators. In the fight against money laundering, the cooperation of several institutions is very important, both at the national and at the international

level. The dynamic change in money laundering methods requires regulatory authorities, including those in the European Union (EU), to constantly modify their regulations to effectively combat these illicit activities. It must be highlighted that the majority of cases in money laundering involve cross-border money-mule operations, where both the predicate offence and the transfer of proceeds occur in distant jurisdictions. International cooperation is crucial for these cases, but finding a legal basis for reaching countries on the other side of the globe can be challenging. This is where the multilateral conventions of the United Nations and the Council of Europe play a very important role by providing a legal framework for dialogue and mutual assistance in global money laundering cases.

Since 1991, the European Union has tried to create an effective and coherent framework against money laundering, which include five anti-money laundering directives that require Member States to prescribe the service providers many obligations, the most important of which are the identification of their customers (Know Your Customer, (KYC) and the Suspicious Transaction Reports (STRs)). It is important to emphasise that from the beginning, when formulating the obligations, the European Union regulation has been taking international standards into account, especially the Forty Recommendation of the Financial Action Task Force (FATF) and international conventions of United Nation and the Council of Europe. Several reports of international organisations and scientific studies pointed to the danger that the anti-money laundering (AML) regime, which was created to fight the traditional forms of money laundering, was not adequate against money laundering using virtual methods, thus it became necessary to modify them and extend their scope to virtual assets (VAs) and virtual assets providers (VASPs). An important and necessary first step in the necessary action against cyber-laundering was the creation of a regulatory framework in connection with crypto assets.

Research carried out by Judit Jacsó in the area of money laundering leads to the conclusion that it is essential for the national legislator, also for the Polish legislator, to continuously align domestic legislation with international and EU legislation, which is one of the keys for the effective action against money laundering.

Furthermore, another essential component of Poland's AML/CFT system is international co-operation, which is even more essential in cyber laundering cases. The inclusion of crypto-asset service providers in the system of preventive tools against money laundering helps to fight against money laundering (cyber-laundering). The legal framework for this must also be created by the Polish legislator by amending the relevant national regulation. With the new EU legal framework, every cryptocurrency-related business will adhere to the same AML/KYC rules as other financial service providers. In the digital age, the traditional strategy of "follow the money" could be supplemented by "follow the virtual asset" or "follow the crypto asset", which could contribute to the effective fight against the new form of money laundering: cyber-laundering.

Determining jurisdiction in cybercrime cases and instruments of international cooperation are essential for law enforcement and the judiciary. As Ferenc Sántha points out, until the mid-20th century, crime was largely a local matter, and the principles governing the exercise of criminal jurisdiction were based on the axiom that a crime was a phenomenon tied to a specific geographic area. Cybercrime has fundamentally changed the nature of crime, making it transnational and borderless. As Ferenc Sántha outlines in Chapter 5, traditional jurisdictional principles in domestic and international criminal law are unable to respond to the challenges posed by cybercrime, in particular positive jurisdictional conflicts. One potential solution to the aforementioned challenges is the creation of a global international treaty that would regulate jurisdictional issues and establish a framework for addressing conflicts of jurisdiction. In addition, it should be emphasised that the successful determination of the state that has de facto jurisdiction over the case is only the first step towards holding the offender accountable, as jurisdiction can only be effectively exercised and proceedings conducted if the offender is accessible to the authorities of the state that has jurisdiction. Otherwise, the institution of international or European mutual legal assistance in criminal matters should be used.

In Chapter 6, Piotr Burczaniuk examines the pre-trial activities directed at acquiring information, relevant from the perspective of criminal law enforcement agencies, to carry out activities

in identifying and detecting cybercrimes and prosecuting their perpetrators. These considerations focus on two key types of these activities: first, security activities related to the functioning of the European and national cybersecurity system, and second, operational and reconnaissance activities authorised by national services in the context of the possibility and scope of their use to combat cybercrime. A complementary element of these considerations was the analysis of international cooperation in the two areas indicated. The main objective of the research presented in Chapter 6 was to answer the question of whether the scope of action and international cooperation of entities responsible for cyber-security and law enforcement agencies conducting reconnaissance activities is sufficient, given the nature of current types of cyber-crimes, and to identify the most significant challenges in this area requiring legislative activity.

Referring to the first of the analysed areas, Piotr Burczaniuk pointed out that the cybersecurity system, based on prevention, detection and response to various types of cyber threats, plays a key role in the combat against cybercrime. This role is outlined in two key aspects: first, when the cybersecurity system supports the process of identifying and prosecuting cyber criminals and second, when it neutralises opportunities for perpetrators by eliminating system vulnerabilities previously identified in specific criminal activities. The directions of cyber security policy changes indicated in the chapter, focusing on the role and importance of the user of an ITC system, and thus also on the potential victim or perpetrator of a crime, lead to the conclusion of an even greater need for rapprochement between cybersecurity and countering cybercrime. However, it should be kept in mind that this rapprochement may face significant legal and practical problems. The most significant of these seem to be related to the different outlook of both regulators and the main participants in both aspects on privacy and data protection issues. The second aspect is the concern about the use of various modern technologies, such as facial recognition systems, the monitoring of online behaviour, and artificial intelligence algorithms, among others, which, on the one hand, may have a high level of effectiveness in the fight against cybercriminals, but on the other hand, the mechanism of their operation is based on the collection

and aggregation of large amounts of personal data. Also worth noting is the challenge of the lack of consistency and harmonisation between different countries and regions in the regulation of both cybersecurity and fighting cybercrime. Many companies operate globally, in multiple markets, and face the need to comply with different standards and regulations, which can lead to complex and costly compliance processes and often, in situations of apparent contradiction, lack of implementation.

Summarising the second of the analysed areas in Chapter 6, it should be pointed out that undoubtedly the most important and effective tool in the hands of law enforcement agencies remains operational control, particularly in the scope involving the so-called electronic surveillance. This is because the detection and prosecution of many types of cybercrimes is only possible thanks to the ability of authorised services to conduct monitoring of the means of electronic communication, of content delivered electronically or, finally, electronic data itself. These activities may include various levels of "depth" of interference in civil rights and freedoms, including in particular the secrecy of correspondence, ranging from the analysis of instant messaging, messages transmitted by e-mail, or in Internet chats, to the study of user activity on social media platforms or information on websites visited by the user. However, it should be added that the effective application of this activity, mainly due to technological developments, faces numerous difficulties. It should be noted, however, that a fundamental political and legal debate is currently underway around this activity, specifically the scope of telecommunications data collected by providers, at both the European Union and national levels. Moreover, retention obligations are at this date not imposed on electronic services providers (e.g., providers of e-mail and instant messaging services), which creates a significant information gap in this regard. Changes in this regard were proposed by the Polish legislator in the draft Law on Electronic Communications, which met with a negative opinion from both public administration bodies and publicists and representatives of social organisations.

Research on international cooperation between services indicates an overabundance of organisations responsible for cyber-security

and countering cybercrime. This leads to both information chaos and coordination deficiencies, both at the level of the organisations themselves and at the level of individual member states. In addition, these organisations are still equipped only with soft tools, both in terms of information acquisition and threat response, which ultimately translates into their often insufficient effectiveness. Research presented in Chapter 6 leads to the conclusion of the need for consolidation at both the legislative and operational level. At the level of European and national legislation, a kind of demarcation is noticeable, separating prevention activities (the domain of cybersecurity) from activities directed at combating threats, and from procedural activities strictly related to the combat against cybercrime. This boundary translates directly into the tasks and powers granted in each area to the services and entities responsible for them. In turn, with respect to them, there is a distinct lack of clearly defined coordination rules and cooperation mechanisms. The comprehensive outlook should be adopted by both European and national legislators, in the numerous currently underway normative acts aimed at raising the level of cybersecurity.

In Chapter 7, Erika Róth undertakes an analysis of the application of coercive measures in cybercrime cases. She points out that a delicate balance need prevail in criminal proceedings. On one side of the scale is the interest in the effectiveness of criminal proceedings, while on the other side are the rights of the participants in the proceedings. And while the principles of coercive measures in Hungarian law do not differ depending on whether they are applied in cybercrime cases or in other criminal cases, several features specific to cybercrime can be identified in the case of coercive measures affecting property, in particular with regard to the search, seizure and rendering of electronic data temporarily inaccessible. An interesting legislative solution in Hungary, analysed by Erika Róth, is the rendering of electronic data temporarily inaccessible which may be ordered where a proceeding is conducted regarding a criminal offence subject to public prosecution, and in connection with which the rendering of electronic data permanently inaccessible may be ordered when so doing is necessary to interrupt the criminal offence. Rendering electronic data temporarily inaccessible restricts

the right to dispose of data published via an electronic communications network. It may be ordered in the form of temporarily removing the electronic data concerned, or temporarily preventing access to the electronic data concerned. The enforcement of this coercive measure is organised and controlled by the National Media and Communications Authority. In addition, the Hungarian legislator also created the possibility for the prosecutor or the investigating authority to call on the service provider capable of preventing access to electronic data to voluntarily remove electronic data, provided that this doesn't harm the interests of the criminal proceeding. The purpose of this provision is to ensure that the content that violates criminal law is only available for the shortest possible time. The Hungarian regulation also regulates searches (including of the information system) and seizures of electronic data more broadly and in greater detail. It indicates in particular the methods by which electronic data, including electronic data used for payments, may be seized. The seizure of electronic data used for payment can also be carried out by performing an operation on the electronic data that prevents the person concerned from disposing of material (property) value expressed by the electronic data. According to the current rules of criminal procedure in Hungary, the Bitcoin to be seized is transferred from the owners address to the address of the authority.

In conclusion, Erika Róth pointed out that although certain coercive measures affecting assets (e.g., search, seizure) are of paramount importance in the case of cybercrimes, it should not be forgotten that other coercive measures can also play a role in ensuring the effectiveness of evidence or preventing re-offending (e.g., pre-trial detention, criminal supervision or restraining order).

In Chapter 8, Erika Róth analyses the principles of electronic evidence preservation. The rules resulting from the Hungarian Code of Criminal Procedure seem to be more detailed and comprehensive. In Poland, there are no special rules governing the preservation of electronic evidence, and the application to it by analogy of the rules relating to physical evidence is sometimes questionable. The HCCP provides a list of the means of evidence and evidentiary acts. Electronic data was also recognised as one of the means of evidence

in Hungary. As Erika Róth points out in her summary of the research, lack of regulation or insufficient regulation of the preservation of electronic evidence may even result in inadmissibility of evidence. In order to avoid such law enforcement actions that result in inadmissibility of evidence and consequently render prosecution ineffective, the legislator must monitor law enforcement practice and respond to problems that can be solved by legislation. The legislature should also be sensitive to amendment proposals formulated by the scientific community that recognise regulatory deficiencies or loopholes. Moreover, the legislator should pay attention to international expectations, which means more than compliance with EU requirements only.

In Chapter 9, "Data Retention and Legal Problems of Investigating Cybercrime", Rafał Wielki draws attention to the problem of storing and processing data held by operators of ICT services. While there used to be EU regulations that facilitated a uniform understanding of the problems (Directive 2006/24/EC of the European Parliament and the Council), their legality has been challenged by the Court of Justice of the European Union, with the result that today there is no legal act that defines what type of data can be processed by ISPs, how long it can be stored, and on what basis law enforcement agencies can use it. By failing to cooperate with law enforcement agencies in sharing traffic data on suspected users, online platforms are essentially making it easier for cybercriminals to go unpunished. Despite the introduction of a number of laws that indirectly address the retention of telecommunications data, email data, etc., there is still a lack of legislation that regulates this issue directly. The regulations in force in individual EU countries are not uniform, which does not serve to promote the exchange of information crucial in the fight against cross-border cybercrime. It seems high time to raise the need for renewed discussions among member states on creating a piece of legislation that would frame and address civil liberties on the one hand, and the needs of investigators who need access to data on the other.

An analysis of the perpetrators' modus operandi carried out by Rafał Wielki allows conclusions to be drawn regarding effective methods of fighting cybercrime that use information analysis tools (Chapter 10). By understanding the characteristics of cybercrimes, it is possible to understand the motivations of the perpetrators, their

modus operandi, and the tools used to commit criminal acts. Among the *de lege ferenda* proposals, it is suggested that international cooperation in the prosecution of cybercrimes be tightened in general, and that as many procedures as possible be regulated in a similar manner, so that laws are not mutually exclusive in different countries. Nowadays, criminals are turning more often to instant messaging to communicate with each other, while at the same time the tools of classic communication via telephone network (SMS, voice calls) are gradually being consigned to oblivion. This fact poses a very serious challenge in the form of the lack of access to network traffic data of suspected users, as currently the retention of data collected by social media and instant messaging is regulated neither by national law nor by international law. This demonstrates the need for uniform regulations to facilitate cooperation with social media operators as processors of personal data and user activity information. Among the legal and technical challenges, attention should also be paid to the impact of disruptive technologies, i.e., the impact of quantum computing on encryption methods and the use of artificial intelligence by perpetrators of crime. Given the increasing technical advancement of the perpetrators using encryption tools, anonymisation of network traffic and sophisticated money laundering methods, it is of fundamental importance that law enforcement agencies are also equipped with tools allowing them to effectively conduct criminal proceedings. As indicated in many chapters of the monograph, the rapid acquisition and analysis of electronic data and the preservation of evidence are important for the effectiveness of criminal proceedings in cybercrime cases. This process is significantly influenced by the availability of modern technology and work-supporting IT systems in the police and in the prosecutor's office.

We believe that the monograph will have a positive impact on setting the direction of legislative work aimed at countering cybercrime and protecting users of digital services from cybercriminals. Since cybercrime issues are a very popular research topic, the introduction to the Polish and Hungarian legal background and law enforcement practice will provide an essential source for researchers as well.

Agnieszka Gryszczyńska

DR. FERENC SÁNTHA, EGYETEMI DOCENS
University of Miskolc | DOI: 10.32041/9788367149761/1

Chapter 1. Definition and Systematisation of Cybercrimes

1.1. Introduction

The first step of any scientific research is to define the subject the research. For us, as members of the cybercrime research team, it is therefore fundamental to answer the question of what we mean by the term *cybercrimes*. The term is widely used nowadays both in international and national literature, as well as in various international legal sources. My task is to review and analyse the international academic literature and international legal instruments on the definition and categorisation of cybercrimes but my first question is: Why is it necessary to address the problem of definition and categorisation?

A clear definition of cybercrimes and an appropriate classification of the criminal offences covered is essential for several reasons. On the one hand, it can help harmonise national cybercrime laws, as there are currently significant differences among European countries as to which illegal acts committed in cyberspace constitute a criminal offence. On the other hand, international cooperation in criminal matters and efforts to combat cybercrimes in general may be more effective if national rules governing relevant offences are based on the same principles and if the designation and statutory definition of the crimes can be aligned and harmonised to the greatest extent possible. Finally, a common definition of cybercrimes and associated statistical methods and metrics will allow

for a better understanding of the true scope of cyber-criminality[1] and a more accurate measurement of relevant crimes. With more accurate data, legal and non-legal responses to combat cybercrimes can be developed more effectively. However, clearly defining and classifying cybercrimes is no easy task, as the types of behaviour covered by this term are extremely diverse and constantly expanding, making it nearly impossible to capture. In this paper, I use the terminology of cybercrime, but point out that both domestic and foreign literature use several terms to describe the phenomenon, which is a direct consequence of the fact that "problems in defining cybercrime begin with the terminology itself".[2] Indeed, the terminology is almost endless: "cyberspace crimes"; "computer crimes"; "computer-related crimes"; "electronic crimes"; "e-crimes"; "technology-enabled crimes"; "high-tech crimes", etc. Until the early 2000s, computer crime or crime by computer was the most popular in international literature but today the term "cybercrimes" is the most accepted and most commonly used.

In Hungary, the first cybercrime in today's meaning was codified by the Hungarian legislature in 1994; it was computer fraud. Therefore, the term "computer crime"[3] was initially used in Hungarian literature, while other authors preferred the definition "computer-related crimes". In the early 2000s, the terms "crimes in the computer environment"[4] and "information technology crimes"[5] also became popular, and after the adoption of the current Hungarian Criminal Code, two terms prevailed:

[1] B. Grund, *A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról*, "MTA Law Working Papers" 2021, No. 21, p. 2.

[2] K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, "Forensic Sciences" 2022, Vol. 2, Issue 2, p. 379.

[3] J. Pergel, *A számítógépes csalás és egyéb számítógépes bűncselekmények*, "Statisztikai Szemle" 2001, No. 9.

[4] Z.A. Nagy, *Bűncselekmények számítógépes környezetben*, Budapest 2009.

[5] K. Mezei, *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, Pécs 2019, p. 10; K. Sorbán, *Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói*, "Themis" 2015, No. 6.

- the first one is "crimes against the information system"[6], as this is the title of the corresponding chapter of the Criminal Code,
- the second is a simple translation of the English word cybercrimes, which sounds like this in Hungarian: *kiberbűncselekmények*.[7]

International and domestic literature on the concept of cybercrime could fill libraries. In this paper, I will briefly analyse the different conceptual and classificatory approaches and outline the one I have chosen. Finally, as an overview, the paper provides an insight into the Hungarian system of cyber-dependent crimes.

1.2. Single Definitions of Cybercrimes

A single definition means that the author tries to describe the phenomenon in a longer or shorter sentence. Thus, according to Wall, cybercrime is "the occurrence of a harmful behaviour that is somehow related to a computer".[8] As interpreted by Gordon and Ford, "any crime that is facilitated or committed using a computer, network, or hardware device".[9] From the Hungarian literature, it is worth mentioning Imre Kunos' definition, according to which computer criminality is the totality of crimes in which information technology tools and systems are used as a means of committing crimes.[10]

Although their truth content is generally undisputed, single definitions formulated in one sentence are necessarily simplistic, their usefulness is questionable, and they cannot provide a comprehensive

[6] M. Gellért, *IOT és a kiberbűncselekmények szabályozása*, "Biztonságtudományi szemle" 2021, No. 1.

[7] R. Gyaraki, *A kiberbűncselekmények megjelenése és helyzete napainkban*, [in:] *A bűnügyi tudományok és az informatika*, K. Mezei (ed.), Pécs 2019; Z.A. Nagy, *Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország!*, "Magyar Jog" 2016, No. 1.

[8] D.S. Wall, *Introduction: Cybercrime and the Internet*, [in:] *Crime and the Internet*, D. Wall (ed.), New York 2001, p. 3.

[9] S. Gordon, R. Ford, *On the Definition and Classification of Cybercrime*, "Journal of Computer Virology" 2006, Vol. 2, No. 1, p. 14.

[10] I. Kunos, *A számítógépes bűnözés*, "Belügyi Szemle" 1999, No. 11, p. 28.

picture of the phenomenon.[11] Moreover, the question arises as to whether we can actually speak of new crimes that have emerged as a result of technological development, or whether we are merely witnessing the spread of traditional crimes into cyberspace?[12] Grabosky denies that the Internet represents anything new beyond its technological background. All that has happened is that existing crimes have been given a new space and new tools ("old wine, new bottles").[13] More recently, however, it has been argued that the Internet is a new medium that enables new forms of crime or deviance, such as hacking into computer systems or spamming ("new wine, new bottles").[14] The literature therefore tends to use definitions that refer to different categories of relevant crimes.

1.3. The Definitions Refer to Different Categories of Relevant Crimes

These definitions are characterised by using of the term "cybercrimes" as a working definition, focusing on grouping the characteristics of each group, and classifying the few relevant crimes. The literature distinguishes between a two-fold (dichotom) and a three-fold (trichotom) classification of cybercrime.

---

[11] See K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing…*, *op. cit.*, p. 383.

[12] A. Varga, *Az informatikai bűnözés fogalmi meghatározása, csoportosítása*, "In medias res" 2019, No. 6, p. 150.

[13] K. Parti, *Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze*, Pécs 2008, p. 33; P. Grabosky, *Virtual criminality: Old wine in new bottles?*, "Social and Legal Studies" 2001, Vol. 10, Issue 2.

[14] See K. Parti, *Az eladók…*, *op. cit.*, p. 33; Á. Varga, *Az informatikai…*, *op. cit.*, p. 151. According to Parti, there is a third new form of crime that has emerged as a result of the Internet, but which would have developed even without cyberspace (*new wine, no bottles*). She indicates, based on Wall's study, that such a crime as the production and distribution of obscene or child pornography content depicting fictional characters. See also: D.S. Wall, *Cybercrimes: New wine, no bottles?*, [in:] *Invisible Crimes: Their Victims and their Regulation*, P. Davies, P. Francis, V. Jupp (ed.), London 1999.

1.3.1. DICHOTOMIES OF CYBERCRIMES

The system that distinguishes between crimes that exist exclusively in cyberspace (*cyber-dependent crimes*) and traditional crimes that can also be committed in cyberspace (*cyber-enabled crime*) is most commonly used and adopted by international and Hungarian researchers. The first group of crimes – "cybercrimes in a narrower sense" – or so-called "real cybercrimes" – emerged with the advent of information communications technology and do not exist outside the digital world.[15] Examples include hacking, ransomware attacks and various forms of phishing. The second category – "cybercrimes in a broader sense" – includes traditional crimes that have migrated[16] into cyberspace, but can also be committed in the real world. In this context, the information system may be the tool or place where the offence is committed or may facilitate the commission of the offence. Crimes that can also be committed in cyberspace include fraud, money laundering, drug trafficking, harassment, various verbal crimes, etc.[17]

1.3.2. TRICHOTOMIES OF CYBERCRIMES

The first type of the three-fold division is a definition that adds a third group to the widely used two-class categorisation mentioned above. In this system, there are:

- computer-centred crime: criminal activity targeting computer systems, networks, storage media, or other computer

[15] These crimes – the subject of which is the information system – can only be committed with the help of computers, their networks or other ICT devices.

[16] S.W. Brenner, *Re-thinking crime control strategies*, [in:] *Crime Online*, J. Yvonne (ed.), Cullompton 2007, pp. 12–28.

[17] Based on the above distinction, Ambrus also makes a double division in the domestic literature when he distinguishes between digital crimes in the narrower and broader sense. I. Ambrus, *Digitalizáció és büntetőjog*, Budapest 2021, p. 290. I note that crimes that can be committed in cyberspace can also be categorised according to the protected legal value, so that a distinction can be made between crimes against property and crimes against the person.

devices which can be considered as "new tools facilitating a new class of crime";
- computer-assisted crime: use of computer systems as tools to assist in a criminal activity that can be undertaken with or without the use of a computer, which can be seen as "new ways to commit conventional crimes";
- incidental computer crime: criminal activity in which the use of a computer system is incidental to the activity itself, which can be described as "new tools to replace conventional tools".[18]

Another similar example is the trichotomy system, which uses the terminology of the previously mentioned popular two-fold classification to distinguish:

- cyber-dependent crimes or true cybercrimes, where the computer is the target and the crime could not happen without a computer, e.g., hacking;
- cyber-enabled crimes or hybrid crimes, where the computer plays a significant role, but the crime could still be committed without the involvement of the computer, e.g., fraud;
- cyber-assisted crimes or the use of computers in traditional crime, where the computer's involvement is incidental to a real-world crime and simply increases the opportunity for traditional crimes, e.g., criminal communications.[19]

There is no denying that there are differences between the second and third categories, but I am not sure that a separate third category is necessary.

The second type of the trichotomy is a definition that proposes a new three-factor classification of cybercrimes based on the role of technology. One of the best known is the divisions devised by Wall, who distinguishes between:

1. "Crimes against the machine", also known as *computer integrity crimes*, e.g., hacking, cracking, or DoS attack,

[18] E. Huebner, D. Bem, O. Bem, *Computer Forensics – Past, Present and Future*, "Journal of Information Science and Technology" 2008, Vol. 5, Issue 3, p. 45.

[19] About Wall's threefold system see K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing…*, *op. cit.*, p. 385.

2. "Crimes using the machine", also known as *computer-assisted crimes*, e.g., piracy, robberies and scams,
3. "Crimes in the machine", also known as *computer content crimes*, e.g., online hate, harassment, child-pornography.[20]

Finally, I mentioned a third, very constructive classification proposed by Sarre, Lau, and Chang. Since "artificial intelligence and developments in robotics are quickly changing the technological landscape", they also use a three-factor spectrum system in which:

1. Type I cybercrimes denotes crimes that are technical in nature (e.g., hacking),
2. Type II cybercrimes denotes crimes that involve human contact (e.g., cyberbullying),
3. Type III cybercrimes denotes crimes that are committed by Artificial Intelligence, robots or self-learning technology.[21]

In my view, a three-fold categorisation of cybercrimes based on the role of advanced technologies[22] is more forward-looking than dichotomies because it better reflects the likely future of cybercriminality: In the future, most of these crimes will be facilitated by particular technologies whose role in the commission of crimes will certainly increase.

---

[20] D.S. Wall, *The Transformation of Crime in the Information Age*, Cambridge 2007.

[21] R. Sarre, Y-C. Lau, L.Y.C. Chang, *Responding to cybercrime: Current trends*, "Police Practice and Research" 2018, Vol. 19, Issue 6, p. 517. The authors' position is also quoted in K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing…*, *op. cit.*, p. 385.

[22] From the domestic literature, it is worth highlighting Grund's threefold division, according to which cybercrime includes the following:

1) crimes in which the security of the computer or computer network is threatened by criminal acts and which have developed in parallel with the emergence of ICT (cybercrimes in the narrow sense),
2) traditional crimes in which the computer is used as a tool of the commission. These crimes existed before the introduction of ICT, but they have been revived by the integration of cyberspace (computer-assisted crimes),
3) computer content-related crimes where the contents of the device can be used as evidence of the crime (computer content-related crimes).

See B. Grund, *A kibertér…*, *op. cit.*, p. 4.

1.4. Definitions Based on the Systematisation of Cybercrimes (Taxonomies of Cybercrimes)

Taxonomy is the process of identifying, grouping, and categorising cybercrimes into a complex system based on the similarities and differences of the crimes. It is an intricate and, in many cases, complicated system that attempts to comprehensively classify cybercrimes. Taxonomies of cybercrime have been developed by both international legal institutions and representatives of the academic literature.

An example of the first is the classification system of the Budapest Convention[23] (and its First Additional Protocol[24]) which contains 13 different cybercrimes in five categories. The first category is *offences against the confidentiality, integrity and availability of computer data and systems*, including illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5) and misuse of devices (Article 6). The second group is *computer-related offences*, which include computer-related forgery (Article 7) and computer-related fraud (Article 8); the third is *content-related offences* which in the Convention are offences related to child pornography (Article 9); the fourth is *offences related to infringements of copyright and related rights* (Article 10). Finally, under the Additional Protocol, the fifth category covers *acts of a racist and xenophobic nature committed through computer systems*, which include the dissemination of racist and xenophobic material through computer systems (Article 3), racist and xenophobic motivated threat (Article 4), racist and xenophobic motivated insult (Article 5), denial, gross minimisation, approval or justification of genocide or crimes against humanity (Article 6).

An example of the second is the systematisation devised by Wall, who proposed a system based on the distinction between

[23] The Council of Europe's Convention on Cybercrime, Budapest, 23. XI. 2001.

[24] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 I 2003.

person-target and computer-target crimes, instead of an offence--based framework. Wall's four-category taxonomy is as follows:

1. cyber-trespass, which is defined as the unauthorised crossing of the boundaries of computer systems, e.g., hacking and cracking,
2. cyber-deception/theft, which is defined as the use of ICT to steal either information or valuable items. This is typically achieved by cyber-trespass, and the applicable crimes are digital piracy, credit card frauds and spam,
3. cyber-pornography and obscenity is the publication or trading sexually expressive materials within cyberspace. This category includes paedophilia, child sexual abuse material, child sexual exploitation, sex trade and sex trafficking,
4. cyber-violence means the violent impact of the cyber-activities of another upon an individual or a social or political grouping. The relevant crimes are cyberstalking, hate-speech, bomb-talk, online harassment, politically motivated hacking and terrorism.[25]

There are developed taxonomies of cybercrimes that attempt to provide an exhaustive list of crimes in each category and take into account the latest developments in ICT and the newest forms of cybercrime. In this paper, for reasons of novelty and originality, the system of Philips and his co-authors[26] is only outlined in a slightly simplified table. The novelty of the approach is that it focuses not only on cybercrimes, but also on unlawful or deviant acts that can (also) be committed in cyberspace, but which are not or not yet criminalised.

[25] D.S. Wall, *Introduction…*, *op. cit.*, pp. 5–11. For an explanation and completion of the system of Wall see: K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing…*, *op. cit.*, p. 388, and E.C. Viano, *Cybercrime: Definition, Typology, and Criminalization*, [in:] *Cybercrime, Organized Crime, and Social Responses*, E.C. Viano (ed.), Switzerland 2017, pp. 5–6.

[26] K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing…*, *op. cit.*, p. 390.

Table. *A new system of cybercrime and cyber-deviancy*

I. Crimes against the machine (1. Attacks against Data and Systems)	**II. Crimes using the machine (2. Attacks against Property or Theft)**	**III. Crimes in the cybersphere**	**IV. Cyber-assisted crimes**	**V. Cross-category A**	**VI. Cross-category B (8. Information and Behaviour Manipulation)**
1/a. against individuals and organizations	computer-related forgery	*3. interpersonal violence*	*7. incidental technology use*	organised crime	*8/a. using advanced technology*
illegal access	computer-related fraud	harrassment, cyberbullying	illegal gambling and illegal gaming	deep web markets, illegal virtual marketplaces	AI, ML
illegal data acquisition	copyright infringements, trademark-related offences	trolling, coercion	money laundering, money muling	cybercrime as a service	algorithmic profiling
illegal interception	digital piracy	extortion	drug trade		deep fakes
data interference, system interference	spam	*4. sexual violence*	criminal communications		bots and botnets
misuse of devices	identity theft	pornographic material			*8/b. using false information*
extortion, ransomware heist	phishing	child sexual abuse material			cyber troops

1/b. against states and nations	cyberfraud	grooming, stalking			fake news
political interference		image-based abuse			misinformation, disinformation
cyberwarfare		sextortion			
espionage		sex trade, sex trafficking, sex tourism, sexting			
		5. violence against groups			
		hate speech, religious offences			
		xenophobia			
		terrorism, radicalisation			
		6. violence (general)			
		inciting violence			

Source: K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, "Forensic Sciences" 2022, Vol. 2, Issue 2.

My comments on this system are the following: I fully agree with the title and the elements of Category I, and I propose to rename Category II "crimes against property rights and intellectual property committed using a computer", taking into account the protected legal values of the offences. As regards Category III, I prefer the term "crimes against the person committed using a computer", as the information system is also the tool or place of the offences in this category. I would avoid the reference to "violence", as in Hungarian criminal law it means physical force, but it is not an element of the offences covered by this category. The title of subcategory 5 is proposed to be "verbal offences", which would also include offences in the second subcategory (8/b.) of Category VI. I agree with the name and elements of Category IV, in which I would also include organised crimes.

In my view, from a criminal substantive law perspective, Category V needs to be ignored, as the acts in this group are deviant rather than necessarily criminal. The creation of Category VI is the most important innovation of the system and should be strongly supported.

1.5. Overview: Cyber-Dependent Crimes in Hungarian Criminal Law

First, I note that the main influence on the current regulation of cyber-dependent crimes has been the relevant international legal instruments. As I mentioned earlier, the first cybercrime in Hungary was computer fraud, but in 2001 – after Hungary signed the Council of Europe's Cybercrime Convention (the so-called Budapest Convention) – the Hungarian legislator introduced two new offences into the chapter of economic crimes of the old Criminal Code: crime against computer systems and data, and crime of circumvention of technical measures for the protection of computer systems.

This solution has been criticised because the protected value of these offences is not the order of the economic management, but the social interest of the proper functioning of information systems. Taking this into account and in order to harmonise with the provisions of the EU Framework Decision on attacks against information systems (2005) and the draft EU Directive (later the European

Union's Directive 2013/40/EU), the Hungarian legislator inserted the cyber-dependent crimes into a separate chapter (XLIII) of the new Hungarian Criminal Code (HCC), titled "Illegal Access to Data and Crimes Against the Information System". In this chapter, there are two criminal offences which can be classified as cyber-dependent crimes, and one is closely related to them:

- breach of an information system or data,
- circumvention of technical measures for the protection of the information system,
- illegal access to data.

And there is one more cyber-dependent crime among the crimes against property:

- fraud committed by means of using an information system.

1.5.1. ARTICLE 423 OF THE HCC – BREACH OF AN INFORMATION SYSTEM OR DATA

This first Hungarian[27] cybercrime can be described as unauthorised use of an information system. It can be committed in two ways: by unauthorised entry to the information system or by remaining inside the system while exceeding or violating the access rights.

An example of the first type is the perpetrator not having access to the system (this is called "hacking"). There are different types of unauthorised intrusion, e.g., by obtaining and using the password of another person who has access to the system, by exploiting security weaknesses of the computer or the network, by using a code-cracking programme, etc. The offence requires a specific method of commission, namely it must be committed by breaching or circumventing a technical measure that provides protection. This means that the information system must be actively protected, e.g., by a password, firewalls or other protective measures, in order

[27] See Art. 423(1) of the HCC: "Any person who enters an information system without authorization by violating or circumventing a technical measure designed to protect the information system, or stays in the system in excess of or in violation of his or her access authorization."

for there to be the commission of a crime.[28] The other illegal act, staying in the system, can only be committed by a person authorised to enter the system. The entry is legal, but later the perpetrator performs operations that exceed his or her user authorisation.

This offence does not constitute a purpose, and therefore it is not a condition of the crime that it be committed for gain, damage or similar purposes. It is also not required that the perpetrator subsequently perform an operation on the data stored in the information system or even interferes with the functioning of the system. Therefore, unauthorised intrusion into the system is a criminal offence in itself, it is the mere act of hacking.

The second category[29] of the offence is the disruption of the functioning of the information system. Examples of this category are the so-called "malware attacks".

The effects of malware can be various. They can disrupt the operation of the IT system by slowing down or stopping the computer, overwriting stored or transmitted data, and modifying programs; Denial of Service (DoS) attack, where the perpetrator aims to make a computer or other device unavailable to the intended users. DoS attacks typically work by flooding a target computer with requests until normal traffic can no longer be processed, resulting in denial of service to additional users. In addition, defacement[30] (or web defacement), i.e., an attack on a website in which the appearance or content of the information is altered, also constitutes this category.

The third category[31] of the crime is the various manipulations of data in the information system. Data entry alone is not punishable, but deletion or modification of even a single piece of data already

[28] K. Mezei, *A kiberbűncselekmények hazai szabályozásának aktuális kérdései*, "Magyar Jogászegyleti Értekezések" Budapest 2018, p. 160.

[29] See Art. 423(2) a) of the HCC: "Any person who interferes with the operation of the information system without authorisation or in violation of his or her access authorization."

[30] See in detail, e.g., Z.A. Nagy, *A kiberbűncselekmények fogalma és csoportosítása*, [in:] *Kibervédelem a bűnügyi tudományokban*, T. Kiss (ed.), Budapest 2020, p. 41.

[31] See Art. 423 (2) b) of the HCC: "Any person who alters, deletes or makes inaccessible data in the information system without authorization or in violation of the limits of his authorization."

constitutes a criminal offence.[32] By way of example, I can mention the IT specialist perpetrator who was an employee of a university and altered data in the IT system about a student who failed an exam. As a result of his act, the modified data indicates that the student passed the exam.[33]

There are two aggravated sub-categories of the offence. The first can be established if the above criminal acts involve a significant number of information systems. The law does not define what is meant by a significant number, but an example of this aggravated sub-category is the so-called DDoS (distributed denial of service), a type of DoS attack that originates from many distributed sources.[34] In the second aggravated sub-category, the crime is directed against a facility of public interest, such as public transport facilities, electronic communication networks, logistics, financial and IT hubs, facilities for the production of war material, military goods or energy.

1.5.2. ARTICLE 424 OF THE HCC – CIRCUMVENTION OF TECHNICAL MEASURES FOR THE PROTECTION OF THE INFORMATION SYSTEM

Nowadays, cybercrime has become a service-based business model, where tools and programs for carrying out various attacks are offered as a service, or we can purchase these tools through the so-called darknet online black markets. Cyberattacks have become easier due to easy access to the knowledge and software needed to commit crimes. Therefore, it is important to define and punish preparatory acts linked to cybercrimes as a separate criminal offence,[35] which is not considered a true cyber-dependent crime. However,

[32] See M. Gellért, *IOT és…*, *op. cit.*, pp. 19–20.

[33] J. Gula, *Tiltott adatszerzés és az információs rendszer elleni bűncselekmények*, [in:] *Magyar büntetőjog különös rész*, I. Görgényi *et al.*, Budapest 2020, p. 896.

[34] See K. Mezei, *A kiberbűncselekmények…*, *op. cit.*, pp. 166–167.

[35] See Art. 424 of the HCC: "Any person who, with intent to commit a cybercrime:

(a) creates, transmits, provides, receives, or disseminates a password or computer program; or

to effectively prevent cyber-criminality, it is necessary to punish these behaviours.

1.5.3. ARTICLE 422 OF THE HCC – ILLEGAL ACCESS TO DATA

Illegal access to data is a category of crime[36] that can be considered as cyber-dependent crime, since it can only be committed by using an information system. This crime may occur, for example, by the deployment of spyware. Spyware is one of the most common threats to Internet users. Once installed, it monitors Internet activity, tracks login credentials and spies on sensitive information.[37] The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.

1.5.4. ARTICLE 375 OF THE HCC – FRAUD COMMITTED BY MEANS OF AN INFORMATION SYSTEM

The Hungarian legislator has included this offence in the crimes against property, since the protected values are the property rights. This type of fraud can be considered as a cyber-dependent crime, as it covers fraudulent acts that result in property damage through the direct use of an information system. Another important difference is that this crime does not involve deception of a natural person, which is the essential element of traditional fraud.

(b) provides his or her economic, technical, or organizational knowledge in connection with the creation of a password or computer program to another person."

[36] See Art. 422 of the HCC: "Any person who, with intent to obtain without authorization personal data, private secrets, trade secrets or business secrets (…): e) secretly monitors the data handled in the information system and records them by technical means."

[37] See: https://www.techtarget.com/searchsecurity/definition/spyware (accessed on: 25.07.2023).

This first type[38] of the crime can be committed – like the first previously mentioned cybercrime – by manipulating data, but with the difference that the purpose and the result are also elements of the crime. The purpose is unlawful gain, and the result is financial loss.

Examples of this case:

- bank fraud, when the perpetrator obtains Internet banking login data and uses them to cause damage through a transaction in the information system (e.g., making a bank transfer),
- card not present fraud (CNP), where the crime is committed without the card being present, i.e., the card is not in the hands of the perpetrator. The fraudsters obtain bank cards details and purchase products on online shopping websites.

The second case[39] of the crime is the so-called "card present fraud" where a bank card is physically present and is used by the perpetrators. This crime includes the various forms of ATM fraud, where the perpetrator steals the victim's bank card and then takes money from the ATM,[40] or uses "skinners" to obtain credit card details and create a clone card.

1.6. Closing Remarks

The main finding of the international and Hungarian literature review is that there is no universally accepted definition of cybercrime. This fact has resulted in various definitions being put forth by academics and international organisations. As noted above, single

[38] See Art. 375(1) of the HCC: "Any person who, for unlawful financial gain, enters data into an information system, alters, deletes or makes inaccessible the data handled in the information system, or interferes with the operation of the information system by performing any other operation, and thereby causing financial loss."

[39] See Art. 375(5) of the HCC: "Any person who causes damage by using a counterfeit or forged, or unlawfully obtained electronic payment instrument, or by accepting payment with such payment instrument."

[40] F. Sántha, *A vagyon elleni bűncselekmények*, [in:] *Magyar büntetőjog különös rész*, I. Görgényi *et al.*, Budapest 2020, p. 708.

definitions of cybercrimes are necessarily simplistic; their usefulness is questionable, and they cannot provide a comprehensive picture of the phenomenon. Consequently, it appears that the more popular of the definitions of cybercrime are those that refer to broader categorisations of cybercrime, namely typologies and taxonomies.

The two-factor approach (which using the terms "cyber-dependent" and "cyber-enabled") is dominant in the academic literature. This may be because this definition makes a simple but clear distinction between types of cybercrime.[41] The three-category classification of cybercrimes, which is based on the role of technology, are even more progressive because they reflect the likely future of cyber-criminality: Most crimes in the future will be facilitated by some form of technology, and the role of complex technologies in the commission of crimes will increase. However, in my view, the most advanced and progressive definitions of cybercrimes are the taxonomies, namely definitions that attempt to classify and categorise, and provide the most comprehensive list of the relevant offences. I concede that there is no universal definition of cybercrimes. However, this does not mean that it would be a useless task to create a system of relevant criminal offences which takes into account technological developments and recent trends in cybercrime, is compatible with international legal instruments, and which keeps pace with technological changes and challenges.

REFERENCES

Ambrus, I., *Digitalizáció és büntetőjog*, Budapest 2021.

Brenner, S.W., *Re-thinking crime control strategies*, [in:] *Crime Online*, Yvonne, J. (ed.), Cullompton 2007.

Gellért, M., *IOT és a kiberbűncselekmények szabályozása*, "Biztonságtudományi Szemle" 2021, No. 1.

Gordon, S., Ford, R., *On the Definition and Classification of Cybercrime*, "Journal of Computer Virology" 2006, Vol. 2, No. 1.

[41] See K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing…*, *op. cit.*, p. 391.

Grabosky, P., *Virtual criminality: Old wine in new bottles?*, "Social and Legal Studies" 2001, Vol. 10, Issue 2.

Grund, B., *A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról*, "MTA Law Working Papers" 2021, No. 21.

Gula, J., *Tiltott adatszerzés és az információs rendszer elleni bűncselekmények*, [in:] *Magyar büntetőjog különös rész*, Görgényi, I. *et al.*, Budapest 2020.

Gyaraki, R., *A kiberbűncselekmények megjelenése és helyzete napainkban*, [in:] *A bűnügyi tudományok és az informatika*, Mezei, K. (ed.), Pécs 2019.

Huebner, E., Bem, D., Bem, O., *Computer Forensics – Past, Present and Future*, "Journal of Information Science and Technology" 2008, Vol. 5, Issue 3.

Kunos, I., *A számítógépes bűnözés*, "Belügyi Szemle" 1999, No. 11.

Mezei, K., *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, Pécs 2019.

Mezei, K., *A kiberbűncselekmények hazai szabályozásának aktuális kérdései*, "Magyar Jogászegyleti Értekezések", Budapest 2018.

Nagy, Z.A., *A kiberbűncselekmények fogalma és csoportosítása*, [in:] *Kibervédelem a bűnügyi tudományokban*, Kiss, T. (ed.), Budapest 2020.

Nagy, Z.A., *Bűncselekmények számítógépes környezetben*, Budapest 2009.

Nagy, Z.A., *Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország!*, "Magyar Jog" 2016, No. 1.

Parti, K., *Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze*, Pécs 2008.

Pergel, J., *A számítógépes csalás és egyéb számítógépes bűncselekmények*, "Statisztikai Szemle" 2001, No. 9.

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., Aiken, M.P., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, "Forensic Sciences" 2022, Vol. 2, Issue 2.

Sántha, F., *A vagyon elleni bűncselekmények*, [in:] *Magyar büntetőjog különös rész*, Budapest 2020.

Sarre, R., Lau, Y-C., Chang, L.Y.C., *Responding to cybercrime: Current trends*, "Police Practice and Research" 2018, Vol. 19, Issue 6.

Sorbán, K., *Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói*, "Themis" 2015, No. 6.

Varga, Á., *Az informatikai bűnözés fogalmi meghatározása, csoportosítása*, "In medias res" 2019, No. 6.

Viano, E.C., *Cybercrime: Definition, Typology, and Criminalization*, [in:] *Cybercrime, Organized Crime, and Social Responses*, Viano, E.C. (ed.), Switzerland 2017.

Wall, D.S., *Cybercrimes: New Wine, No Bottles?*, [in:] *Invisible Crimes: Their Victims and Their Regulation*, Davies, P., Francis, P., Jupp, V. (ed.), London 1999.

Wall, D.S., *Introduction: Cybercrime and the Internet*, [in:] *Crime and the Internet*, Wall, D. (ed.), New York 2001.

Wall, D.S., *The Transformation of Crime in the Information Age*, Cambridge 2007.

DR HAB. AGNIESZKA GRYSZCZYŃSKA, PROF. UKSW
Cardinal Stefan Wyszyński University in Warsaw[1] | DOI: 10.32041/9788367149761/2

Chapter 2. The Scope of Criminalisation of Cybercrime in Poland

2.1. Introduction

Cybercrime is one of the most dynamic forms of crime, which prompts a review of the scope of criminalisation of acts considered to be cybercrimes in Poland. The perpetrators of cybercrimes are characterised by a high level of adaptability – in order to achieve their objective, they swiftly adjust both their methods, the tools used and the socio-techniques associated with their attacks. They use modern technological solutions to maintain anonymity and create new identities or use other people's data to conceal their identities. Crimes are committed by them individually as well as within highly specialised and organised criminal groups. The entry threshold for more, less-technical criminals has been lowered by the use of the Cybercrime-as-a-Service model.[2] Attacks on critical infrastructure and the kinetic effects of cyber-crime attacks are becoming an increasing concern, causing threats to the lives and health

[1] Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Department of Informatics Law, ORCID: 0000-0003-3004-5253, a.gryszczynska@uksw.edu.pl.

[2] K. Huang, M. Siegel, S. Madnick, *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*, "Cambridge Institute for Sustainability Leadership" 2017, Vol. 1, No. 1.

of many in the real world.[3] Another breakthrough that is starting to pose new challenges for law enforcement agencies is the use of artificial intelligence and more broadly disruptive technologies in attacks.[4]

The aim of the chapter is to analyse the scope of criminalisation of cybercrime in Poland and to verify the hypothesis that the scope of criminalisation needs to be extended in view of the continuous development of tactics, techniques and procedures used by cybercriminals.

In Poland, there is no legal definition of cybercrime or a statutory catalogue of acts deemed to be cybercrimes,[5] while the criminal conduct that may be deemed cybercrimes is dispersed and, in addition to the Criminal Code, also includes public law acts. The analysis to be carried out will therefore go beyond the regulation of the Criminal Code[6] and will also take into account criminal liability for selected behaviours, as defined in selected acts of administrative law. Due to the lack of a definition of cybercrime, the scope of regulations will be examined with reference to Directive 2013/40/EU on attacks against information systems,[7] the Council of Europe Convention on

[3] S.D. Applegate, *"The dawn of Kinetic Cyber"*, 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn 2013, pp. 1–15.

[4] *Malicious Uses and Abuses of Artificial Intelligence*, Europol, 2022, p. 52, https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf (accessed on: 1.06.2024); A. Gryszczyńska, *The impact of AI on cybercrime. Will it facilitate the actions of perpetrators or enhance the effectiveness of law enforcement?*, [in:] *Hominum causa omne ius constitutum sit. Collection of scientific papers of the Polish-Hungarian Research Platform. Volume I*, M. Wielec, P. Sobczyk, B. Oręziak (eds.), Warszawa 2024, pp. 69–96.

[5] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, p. 32 et seq.; J. Kosiński, *Cyberprzestępczość AD 2020 – stan aktualny i prognozy*, [in:] *Internet. Cyberpandemia*, G. Szpor, A. Gryszczyńska (red.), Warszawa 2020, pp. 101–104.

[6] Act of 6 June 1997 – Criminal Code (consolidated text Journal of Laws of 2024, item 17, as amended), hereinafter referred to as CC.

[7] 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, OJ EU L 218, 14.8.2013, pp. 8–14.

Cybercrime[8] and in light of the work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.[9]

2.2. The Most Common Cyber Security Incidents Occurring in Poland

Globally, there has been an increase in the number of internet users, with internet users accounting for approximately 64.4% of the population in January 2023, mobile phone users accounting for 68% of the population, and social media users accounting for 59.4%. In 2023, after a large increase during the pandemic, the amount of time spent online fell slightly, which among internet users aged 16 to 64 years at the beginning of 2022 was 6 h 58 m per day[10] and in January 2023 was 6 h 37 minutes per day.[11] Global trends also point to an increasing number of people shopping online, so it should come as no surprise that criminals are also becoming more active online. Analysis of cyber-security reports indicates a steady increase in the number of incidents both in Poland and globally, as a result of the global increase in the number of Internet users, time spent online and changes in the modus operandi of perpetrators committing crimes against property. Remote working, education or carrying out public tasks online enforced during the pandemic, have become an opportunity for cybercriminals to increase the effectiveness of attacks. In 2020 and 2021, scenarios linked to the pandemic dominated, which in 2022 were replaced by scenarios linked to an attack by the Russian Federation on the Republic of Ukraine.

[8] The Budapest Convention (ETS No. 185) and its Protocols, in Poland ratified pursuant to Dz. U. 2015, item 728.

[9] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed on: 1.06.2024).

[10] DataReportal, *Digital 2022*, https://datareportal.com/reports/digital-2022-global-overview-report (accessed on: 1.06.2024).

[11] DataReportal, *Digital 2023*, https://datareportal.com/reports/digital-2023-global-overview-report (accessed on: 1.06.2024).

In 2022, CERT Polska[12] observed an increase of more than 34% in the number of recorded incidents compared to the previous year. The significant increase in the number of incidents handled continues (Figure 1). In 2023, CERT Polska recorded a total of 80,267 unique incidents, an increase of 100% compared to 2022. At this point, however, it is necessary to note that the UKSC[13] has introduced the obligation to report certain incidents to the relevant CSIRT, and has also led to the popularisation of the incident reporting procedure where it is optional.[14]

However, the categories of main threats do not change significantly. In the light of reports by CERT Polska (CSIRT NASK),[15] computer fraud, and among them phishing, is definitely dominant. In 2021, there were 22,575 incidents classified as phishing, which accounted for as much as 76.6% of all incidents handled,[16] its share

[12] CERT Polska is historically the first incident response team in Poland. The CERT Polska team operates within the structures of NASK – Państwowy Instytut Badawczy (NASK National Research Institute) and performs part of the tasks of the CSIRT NASK team in accordance with the Act on the National Cyber Security System. Incidents in Poland are also handled by CSIRT GOV and CSIRT MON teams. Due to the broad scope of CSIRT NASK's responsibilities, only quantitative data on incidents from CERT Polska reports were analysed.

[13] Act of 5 July 2018 on the National Cyber Security System (i.e., Journal of Laws 2022, item 1863, as amended), hereinafter referred to as UKSC.

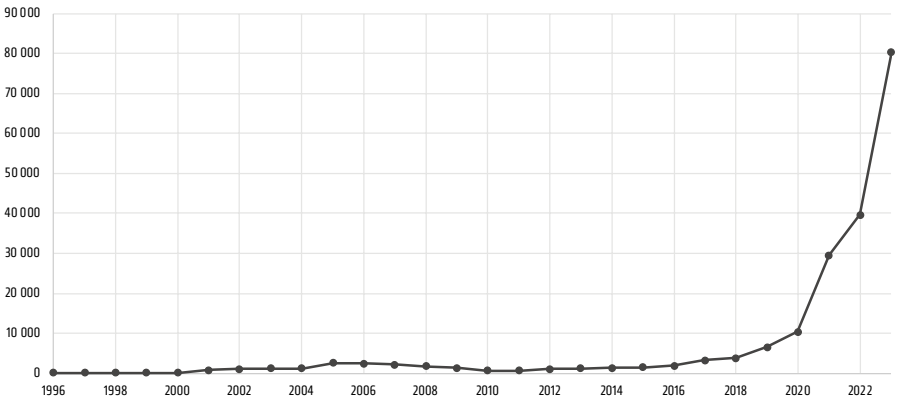
[14] Read more: *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2018,* https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2019*, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2020*, https://www.nask.pl/pl/raporty/raporty/4289,RAPORT-CERT-2020.html (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2021*, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2022*, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (accessed on: 1.06.2024).

[15] CSIRT NASK – Computer Security Incident Response Team operating at the national level, run by the Research and Academic Computer Network – National Research Institute.

[16] *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2021,* pp. 20–24, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (accessed on: 1.06.2024).

in 2022 dropping to 64.6% (25,625 incidents) and 51.61% (41,423) of all incidents in 2023 registered by CERT Polska were classified as phishing.

Figure 1. *Number of incidents handled by CERT Polska in 1996–2023*



Source: Own compilation based on CERT Polska reports.

In 2021, the most popular phishing attack according to CERT Polska reports was impersonation of a Facebook login page. In 2022, the most common perpetrators impersonated InPost (5,119 incidents), Facebook (4,370 incidents) and Vinted (2,926 incidents). In 2023 the attackers most frequently impersonated Allegro (11,161 incidents), Facebook (5,308 incidents) and OLX (4,753 incidents).

Phishing was most often carried out through a page imitating a login panel to a trusted service (email, social networking or e-banking). Links to phishing sites for log-in credentials to various services were sent both by email and in SMS messages (smishing). In recent years, it has become increasingly common for phishing to take place during a telephone call (vishing), during which perpetrators impersonate the phone number of a trusted entity (Calling Line Identification spoofing). The main purpose of impersonation is to increase the effectiveness of the attack. Messages are designed to appear authentic, so the perpetrators most often use spoofing

of e-mail addresses or telephone numbers or send messages from e-mail addresses that are confusingly similar to those of the impersonated entities. In order to effectively counter the new threats posed by the growth of phishing, smishing, and CLI spoofing, the Law on Combating Abuse in Electronic Communications was adopted in Poland in 2023.

Another common type of incident was malware. In 2022, the incidents recorded in this category numbered 3,409, of which as many as 2,607 were related to a malware called "Flubot". In 2023, incidents in the malware category numbered 1,650, half as many as in 2022. Classified incidents included both ransomware infections and campaigns distributing malware known as "Remcos" and "Agent Tesla".

By comparison, in 2021, CSIRT GOV recorded 26,899 incidents out of more than 760,000 notifications, an increase of approximately 15% compared to the previous year.[17] The largest number incidents – 24,171 – were classified under the *VIRUS* category, which is related to alerts from the ARAKIS GOV web-based threat early warning system.[18] In 2022, a total of 21,563 events were classified as security incidents by CSIRT GOV. The majority of these were incidents recognised by ARAKIS.[19]

Some reports point to a noticeable increase in the Distributed Denial of Service attacks (hereinafter DDoS), which experts indicate are geopolitically motivated and are one of the instruments used in the war in Ukraine. They target not only the parties to the conflict, but also countries providing support to Ukraine, including Poland in particular. DDoS attacks are facilitated not only by

[17] *Report on the state of Poland's cybersecurity in 2021*, CSIRT GOV, 2022, p. 9, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/977,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2021-roku.html (accessed on: 1.06.2024).

[18] ARAKIS GOV distributed early warning system for ICT threats occurring at the interface between the internal network and the Internet.

[19] *Report on the state of Poland's cybersecurity in 2022*, CSIRT GOV, 2023, p. 120, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/979,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2022-roku.html (accessed on: 1.6.2024).

the development of botnets, but also by the availability of services in the DDoS-as-a-Service model.[20]

Before moving on to the analysis of the elements of offences classified as cybercrime and the scope of criminalisation, attention should be drawn to the problems of mapping incidents classified by CSIRT/CERT teams to specific articles of the Criminal Code. Table 1 presents the types of incidents handled by CERT Polska in 2018–2023.

Table 1. *Types of incidents handled by CERT Polska in 2018–2023*

Incident Classification	Number of incidents 2018	% 2018	Number of incidents 2019	% 2019	Number of incidents 2020	% 2020	Number of incidents 2021	% 2021	Number of incidents 2022	% 2022	Number of incidents 2023	% 2023
Abusive Content	431	11,53	812	12,52	371	3,56	311	1,05	308	0,78	584	0,73
Malicious Code	862	23,05	969	14,9444787	746	7,16	2847	9,66	3409	8,59	1650	2,06
Information Gathering	101	2,70	95	1,47	60	0,58	27	0,09	31	0,08	29	0,04
Intrusion Attempts	153	4,09	77	1,18753856	174	1,67	127	0,43	121	0,3	205	0,26
Intrusious	125	3,34	160	2,47	317	3,04	247	0,84	354	0,89	418	0,52
Availability	49	1,31	57	0,87908698	121	1,16	148	0,5	175	0,44	385	0,48
Information Content Security	46	1,23	41	0,63	68	0,65	55	0,19	39	0,1	59	0,07
Fraud	**1878**	**50,23**	**4086**	**63,016656**	**8310**	**79,75**	**25472**	**86,40**	**35009**	**88,22**	**75917**	**94,58**
Vulnerable	69	1,85	102	1,57310302	211	2,02	216	0,73	188	0,47	964	1,2
Other	25	0,67	85	1,31091919	42	0,4	33	0,11	49	0,12	56	0,07
Total	**3739**	**100**	**6484**	**100**	**10420**	**100**	**29483**	**100**	**39683**	**100**	**80267**	**100**

Source: Own compilation based on CERT Polska reports[21].

[20] *C.H. Beck Publishers Report – LegalTech 2023*, https://legalis.pl/legaltech-raport-2023/ (accessed on: 1.06.2024).

[21] *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2018,* https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2019*, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2020*, https://www.nask.pl/pl/raporty/raporty/4289,RAPORT-CERT-2020.html (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2021*, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (accessed on: 1.06.2024); *The security*

The largest number of incidents in each of the surveyed reports were classified as "computer fraud". However, according to eCSIRT.net 2012's Incident Classification/Incident Taxonomy which is the basis for categorisation in CERT Polska reports, there is no category (class)[22] "computer fraud". The classification includes the category "fraud", which should be understood as "deception". This category includes the following subcategories (types of incidents):

- "unauthorised use of resources", including for financial gain,[23]
- "copyright", i.e., infringement of copyright,[24]
- "masquerade", i.e., impersonation of another entity[25] and
- "phishing", i.e., impersonation of another entity in order to induce the user to disclose private credentials (e.g., login and password).[26]

The category of "fraud" will therefore include both classic fraud within the meaning of Article 286 § 1 CC (e.g., running a fake online shop, BEC, "Nigerian fraud"), as well as computer fraud within the meaning of Article 287 § 1 CC, identity theft (Article 190a

landscape of the Polish Internet. Annual report on the activities of CERT Polska 2022, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities 2023*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf (accessed on: 1.06.2024); Incident Classification/Incident Taxonomy according to eCSIRT.net, International Version Don Stikvoort, 11 January–19 December 2012 (version mkVI of 31 March 2015), https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (accessed on: 1.06.2024).

[22] The Incident Classification/Incident Taxonomy according to eCSIRT.net uses the concepts of category and subcategory, in the Common Taxonomy for Law Enforcement and The National Network of CSIRTs they correspond to the concepts of class and type of incident (Common Taxonomy for Law Enforcement and The National Network of CSIRTs, v. 1.3, Europol, 2017, https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts (accessed on: 1.06.2024).

[23] *Unauthorised use of resources* – using resources for unauthorised purposes including profit-making ventures (e.g., the use of e-mail to participate in illegal profit chain letters or pyramid schemes).

[24] *Copyright* – offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).

[25] *Masquerade* – type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.

[26] *Phishing* – masquerading as another entity in order to persuade the user to reveal a private credential.

§ 2 CC), unauthorised acquisition of computer passwords or other access data (Article 269b § 1 CC), hacking (Article 267 § 1 CC), copyright infringement as defined in the Act on Copyright and Related Rights.[27]

Lack of consistency in incident classification between CSIRTs renders quantitative research and categorisation of the most serious threats in Poland. The lack of a uniform and acceptable classification also hinders the cross-border exchange of information between CSIRT teams and law enforcement authorities, as well as the research and analysis of the most serious threats. CSIRT reports' incident categories also do not correspond to normative descriptions of criminal acts. In order to increase knowledge on current threats, reliable data from multiple entities is necessary.[28]

2.3. The Substantive Basis for the Criminalisation of Cybercrime in Poland

2.3.1. INTRODUCTORY REMARKS

The vast majority of incidents reported to CSIRT/CERT teams constitute criminal acts that can be considered cybercrimes. The Polish Criminal Code lacks a legal definition of such concepts as: "cybercrime", "computer crime" or "internet crime". In Poland, cybercrime is discussed from the perspective of both substantive and procedural criminal law provisions. Cybercrimes from the perspective of substantive criminal law provisions may be understood narrowly, as crimes encompassing any illegal behaviour aimed at the security of computer systems and the data processed therein, or broadly, as crimes encompassing any illegal behaviour committed by means

[27] Act of 4 February 1994 on Copyright and Related Rights (consolidated text Journal of Laws 2022, item 2509).

[28] Criticisms relating to the lack of consistency in incident classification between the NASK CSIRT teams, the GOV CSIRT and the law enforcement agencies are made in: A. Gryszczyńska, *Fraud and computer scams-global and local players*, [in:] *Internet. Global Games*, G. Szpor, A. Gryszczyńska, W.R. Wiewiórowski (red.), Warszawa 2021, pp. 194–213.

of or in relation to a computer system or network. Vertical and horizontal depictions of cybercrime are proposed.[29] There are also "cyber-dependent crimes" (corresponding to a narrow or vertical view of cybercrime), "cyber-enabled crimes" and "cyber-related crimes" (corresponding to a broader, horizontal view), and sometimes as a special category, "online child sexual exploitation and abuse".[30] From the perspective of criminal procedural law, cybercrimes include all acts prohibited by criminal law, the prosecution of which requires the judicial authorities to gain access to information processed in computer or information systems.[31] An extensive analysis of the definition and systematisation of cybercrimes is contained in Chapter 1 – Definition and systematisation of cybercrimes.

There is no single legal regulation in Polish law containing all the provisions on liability for abuse of information technology. Norms of this kind are contained in several legal acts, in the Criminal Code, in particular in Chapter XXXIII and XXXV, the Act of 28 July 2023 on Combating Abuse of Electronic Communication,[32] the Act of 5 September 2016 on Trust Services and Electronic Identification,[33] the Act of 18 July 2002 on Provision of Services by Electronic Means,[34] the Act of 10 May 2018 on the Protection of Personal

[29] Read more: *High Tech Crimes Within The EU: Old Crimes New Tools, New Crimes New Tools. Threat Assessment 2007*, File Number: #247781, p. 10, https://www.enisa.europa.eu/topics/csirts-in-europe/files/event-files/ENISA_Europol_threat_assessment_2007_Dileone.pdf (accessed on: 1.06.2024).

[30] See: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (accessed on: 1.06.2024), *INTERPOL National Cybercrime Strategy. Guidebook*, 2021, https://www.interpol.int/content/download/16455/file/National%20Cybercrime%20Strategy%20Guidebook.pdf (accessed on: 1.06.2024), cf. also the types of cybercrimes of interest to the EC3 and discussed in IOCTA reports, https://www.europol.europa.eu/ (accessed on: 1.06.2024).

[31] A. Adamski, *Prawo karne…*, *op. cit.*, pp. 30 et seq.

[32] Act of 28 July 2023 on Combating Abuse in Electronic Communications, Journal of Laws 2023, item 170.

[33] Act of 5 September 2016 on Trust Services and Electronic Identification (consolidated text Journal of Laws 2024, item 422).

[34] Act of 18 July 2002 on the Provision of Services by Electronic Means (consolidated text Journal of Laws of 2020, item 344).

Data,[35] Act of 14 December 2018 on the Protection of Personal Data Processed in Connection with Preventing and Fighting Crime,[36] the Act of 4.02.1994 on Copyright and Related Rights,[37]and the Act of 30.06.2000 – Industrial Property Law.[38]

Criminal proceedings conducted in connection with the occurrence of acts of cybercrime are initiated with the adoption of various legal qualifications of the act – as classic offences against property (Article 286 § 1 CC – fraud, Article 279 § 1 CC – burglary), Article 287 § 1 CC – computer fraud or offences against protection of information (Article 267 § 1 CC – hacking). Analyses of cybercrime in Poland, usually focus on acts against the protection of information, without covering all categories of cases that can be considered cyber-enabled crimes and all legal qualifications that are the basis for initiating proceedings or instituting charges against the suspects. This makes these analyses not comprehensive and the conclusions reached on their basis too superficial. For example, in 2020, 12,321 proceedings were initiated for the act of Article 267 § 1–4 CC (so-called *hacking*), and in 2023 there were 1,790 such proceedings. The number of proceedings concerning computer fraud almost doubled from 10,960 in 2020 to 21,576 cases in 2021. Cybercrime classically does not include the act under Article 224a CC, which consists in notifying of an event that poses a threat to the life or health of many persons or to property of a significant size, or creates a situation intended to arouse the conviction of the existence of such a threat, by which an action of a public utility institution or an authority for the protection of security, public order or health is induced in order to avert the threat. Due to the specific nature of the perpetrators' actions – sending cascading emails with

[35] Act of 10 May 2018 on the Protection of Personal Data (consolidated text Journal of Laws 2019, item 1781).

[36] Act of 14 December 2018 on the Protection of Personal Data Processed in Connection with the Prevention and Combating of Crime (consolidated text Journal of Laws 2023, item 1206).

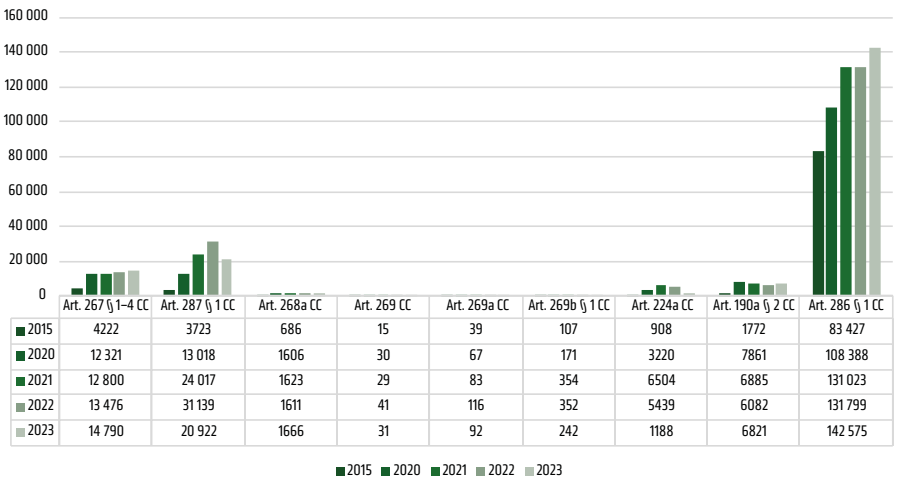
[37] Act of 4 February 1994 on Copyright and Related Rights (consolidated text Journal of Laws 2022, item 2509).

[38] Act of 30 June 2000 Industrial Property Law (consolidated text Journal of Laws 2023, item 1170).

information about a non-existent threat (usually the planting of an explosive) or the use of CLI spoofing – proceedings in this area are conducted by the cybercrime divisions. It is also worth noting that the number of prosecutions for cascading bomb alarms doubled from 3,220 cases initiated in 2020 to 6,504 cases initiated in 2021, putting a significant burden on law enforcement.

As Figure 2 shows, more cases were registered on the basis of Article 190a § 2 CC (identity theft) or Article 224a CC than on the basis of Article 268a CC, Article 269a CC or Article 269a CC, which are considered to be classic cyber-dependent crimes. The number of proceedings initiated on the basis of what are considered cyber-dependent offences is also much lower than the number of proceedings initiated on the basis of Article 286 § 1 of the CC (fraud). An analysis of the modi operandi of perpetrators of fraud shows that a large proportion of fraud is committed online and that these cases could be classified as cybercrime.

Figure 2. *Number of proceedings registered in the prosecutor's offices for selected legal qualifications*



	Art. 267 § 1–4 CC	Art. 287 § 1 CC	Art. 268a CC	Art. 269 CC	Art. 269a CC	Art. 269b § 1 CC	Art. 224a CC	Art. 190a § 2 CC	Art. 286 § 1 CC
2015	4222	3723	686	15	39	107	908	1772	83 427
2020	12 321	13 018	1606	30	67	171	3220	7861	108 388
2021	12 800	24 017	1623	29	83	354	6504	6885	131 023
2022	13 476	31 139	1611	41	116	352	5439	6082	131 799
2023	14 790	20 922	1666	31	92	242	1188	6821	142 575

Source: Own analysis based on data from the PROK-SYS system.

In order to better analyse the phenomenon of cybercrime in Poland, the coordination category "cybercrime" was introduced in the prosecution IT system PROK-SYS on 1 July 2024. Any case can be marked as a cybercrime, regardless of the legal qualification of the registration. From 1 to 6 July 2024, 437 registered cases were flagged with this coordination, of which 354 cases (75%) were registered under Article 286 § 1 CC (fraud). These data should be analysed in further statistical periods, as they may help to understand the structure of cybercrime in Poland and provide better guidance for law enforcement agencies.

From a procedural perspective, computer crimes in the literature include those acts whose prosecution requires law enforcement and justice authorities to gain access to information processed in computer or information systems.[39] With such a view, the vast majority of offences would have to be regarded as cybercrimes, due to the widespread preservation of data and its carriers (e.g., records of surveillance footage, telecommunication data, logs of various services, data of social network users, extraction of data from mobile phones) to various categories of acts.

2.3.2. CYBER-DEPENDENT CRIMES IN THE POLISH CRIMINAL LAW

In Poland, the basic provisions constituting the grounds for criminal liability for acts that are considered cyber-dependent crimes in the Budapest Convention are contained in Chapter XXXIII of the Criminal Code titled "Offences Against the Protection of Information". Cyber-dependent crimes are specifically referred to in Article 267 CC, Article 268 § 2 CC, Article 268a CC, Article 269 CC, Article 269a CC, Article 269b CC.

Cyber-dependent crimes regulated outside of the Criminal Code may include the offence under Article 40 of the Trust and Electronic Identification Services Act, which involves the creation of a qualified electronic signature or an advanced electronic signature using electronic signature creation data assigned to another

[39] A. Adamski, *Prawo karne…*, *op. cit.*, pp. 30 et seq.

person. Although the Council of Europe Convention on Cybercrime classifies the offence of computer forgery as a cyber-enabled crime, the scope of computer forgery is different from the offence set out in Article 40 of the Trust and Electronic Identification Services Act. This act is an offence, violating the attributes of information security, of the confidentiality – in terms of the data used to create a signature, which can only be used by the person for whom the private and public key indicated in the certificate was generated, as well as authenticity – the origin – of the document from an authorised person indicated in the electronic signature certificate. Moreover, this offence cannot be committed otherwise than with the use of computer data.

Cyber-dependent crimes should not include misuse of electronic communications such as smishing or spoofing, as these involve impersonating a user or an element of the telecommunications network infrastructure and should therefore be included in cyber-enabled crimes. The Polish literature also does not include among cybercrimes the act under Article 285 § 1 CC, which consists in connecting to a telecommunications device and activating telephone impulses on someone else's account.

Cybercrime in the colloquial sense is most often identified with hacking. In the legal literature, the term "hacking" occurs in a broad or narrow sense. It distinguishes "hacking sensu stricto" – the behaviour of gaining unauthorised access to an information system or computer data – from "hacking sensu largo" as any attack on the security of information systems and data, including, for example, the disruption of the operation of an information system, the modification or destruction of computer data.[40]

The Convention on Cybercrime[41] imposes an obligation on state parties in Article 2 to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any

[40] F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016. According to the quoted author, hacking is, in the colloquial sense, "a collective term for virtually all crimes committed online (except, for example, the distribution of pornography or copyright infringement)".

[41] Council of Europe Convention of 23.11.2001 on Cybercrime (CETS No. 185).

part of a computer system without right. A state party may require 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 that is connected to another computer system. Ratification of the Convention first required individual states to ensure that their domestic law complied with its norms.

Defining cybercrime and, more narrowly, hacking may also be influenced by the ongoing work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established by Resolution 74/247 (2019) of the General Assembly. Regardless of the final consensus on the material scope of the convention, the regulation should cover the conduct defined in Article 2 of the Convention on Cybercrime and in Article 267 of the Polish Criminal Code.

The Polish Criminal Code (CC) criminalises illegal access to information in Article 267, according to which shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty for up to 2 years anyone who:

- gains access to information not intended for him by opening a sealed letter, plugging into a telecommunications network, or by breaching or bypassing an electronic, magnetic, computer or other special protection of such information (§ 1),
- gains access to an entire computer system or any part thereof without authorisation (§ 2),
- with the purpose of gaining unauthorised access to information, installs or employs a wire-tapping or visual device, or other device or software (§ 3), or
- discloses to another person information obtained in the manner referred to in § 1–3 (§ 4).

The prosecution of this offence, referred to in the legal doctrine as the crime of hacking is carried out at the aggrieved party's motion (§ 5).

The regulation of hacking in Poland is criticised because of the low upper limit of the criminal threat and the motion-based nature. It is proposed to raise the upper sentencing limit and to distinguish a minor case.

When investigating the phenomenon of hacking, it is also necessary to assess the impact of the perpetrators' actions on the real and virtual space – in particular, taking into account the intertwining of these two dimensions and the kinetic effect of attacks initiated in cyberspace. In view of the status of the pandemic as well as the significant risks to patients' lives and well-being, the cyberattack on Brno University Hospital was considered an attack on critical infrastructure,[42] whereas due to a patient's death in connection with a ransomware attack, German authorities are investigating the perpetrators on suspicion of negligent manslaughter. In view of the above, the legal grounds for initiating criminal proceedings or charges for suspects may be based on a cumulative qualification involving the concurrence of cybercrime provisions with provisions protecting life and health.

The offence of hacking may also be in cumulative concurrence with offences against property. The Supreme Court, in its judgment of 22 March 2017,[43] held that breaking the electronic barrier in a bank's non-cash payment system and taking property in the form of monetary values stored in the bank's IT system can be qualified as an offence under Article 279 § 1 CC (burglary). Due to the fact that the perpetrators, by providing the login and password to electronic banking, break through or bypass the security of electronic banking and gain unauthorised access to information not intended for them, Article 267 § 1 CC will remain in cumulative concurrence with Article 279 § 1 CC. Due to the fact that the perpetrators, acting with the aim of gaining a financial benefit without authorisation, affect the automatic processing of computer data by introducing a new computer data record on the account of an e-banking customer, Article 287 § 1 CC is also indicated among the coinciding provisions in court rulings.

[42] *Pandemic profiteering: how criminals exploit the COVID-19 crisis*, Europol, https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (accessed on: 1.06.2024).

[43] Judgment of the Supreme Court of 22 March 2017, III KK 349/16.

The acquisition of computer passwords (in scenarios where the perpetrators first create a fake website impersonating a bank in order to obtain login credentials) will constitute a separate offence under Article 269b § 1 CC.

2.3.3. CYBER-ENABLED CRIMES IN THE POLISH CRIMINAL LAW

2.3.3.1. *Computer Fraud – Article 287 CC*

Pursuant to Article 287 § 1 of the CC, described as computer fraud in Poland, unauthorised affecting automatic processing, collecting or transmitting of computer data, altering or deleting computer data record or entering a new computer data record with the purpose of gaining material benefit or inflicting damage upon another person is penalised. In the basic type, the offence is punishable by imprisonment for a term of between 3 months and 5 years. In a minor case specified in § 2, the perpetrator is subject to a fine, limitation of liberty or imprisonment of up to one year. The principal object of protection of the offence specified in Article 287 CC is property, however, the construction of the statutory elements of the act under Article 287 § 1 CC does not require the occurrence of an effect consisting in the disposition of property, which is the equivalent of disposing of property under Article 286 §1 CC. The elements of the act under Article 287 § 1 CC do not include the effective damage, as well as the intention to misappropriate, which is necessary under Article 279 § 1 CC.[44] As a collateral good, the integrity and availability of computer data and the inviolability of its automatic processing, collection or transmission are protected. The commission of computer fraud occurs already at the moment when the perpetrator manipulates the data. If the interference is preceded by breaking or bypassing specific safeguards and thus gaining unauthorised access to data (violation of data confidentiality), the perpetrator also commits

[44] Judgment of the Appellate Court of Szczecin of 14.10.2008, II AKa 120/08, Legalis.

an act under Article 267 § 1 CC, which, as commentators point out, will remain in cumulative concurrence with Article 287 § 1 CC.[45]

The literature also indicates that the act under Article 287 § 1–2 CC is rather "manipulation of IT data in the field of property rights".[46] Although the legislator used the term "fraud" in Article 287 § 3 CC, the elements of the act under Article 287 § 1 CC differ from the elements of the act under Article 286 § 1 CC. Unlike Article 286 § 1 CC, the object of the perpetrator's act is not a person, but the device or medium on which computer data is recorded, as the perpetrator does not affect the decision-making process of another person, but the automatically occurring data processing processes.[47]

Computer fraud is a common, intentional offence belonging to the category of so-called directional offences. The perpetrator's behaviour is intended to be directed towards a specific purpose, which is either to achieve a pecuniary benefit or to cause damage to another person, and therefore this offence can only be committed with direct intent.

Article 287 CC refers to Article 8 of the Council of Europe Convention on Cybercrime, which defines computer fraud as the intentional, unlawful causing of loss of property to another person by: (1) entering, altering, deleting or deleting computer data, (2) any interference with the functioning of a computer system with the intent to defraud or with the fraudulent intent to obtain an economic advantage for oneself or another person. However, unlike the act set out in Article 8 of the Council of Europe Convention on Cybercrime, the statutory elements of the act set out in Article 287 CC do not include causing the effect of loss of property to another person by manipulating data or interfering with the functioning of a computer system for the purpose of gaining economic advantage or causing damage.

---

[45] B. Michalski, *Przestępstwa przeciwko mieniu. Rozdział XXXV Kodeksu Karnego. Komentarz*, Warszawa 1999, p. 224. See also M. Gałązka, [in:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*, Warszawa 2021, Article 287, where it is indicated that Article 267 § 1 of the PCC may be regarded as a prior co-convicted act or a fragment of a continuous act.

[46] M. Gałązka, [in:] A. Grześkowiak, K. Wiak (red.), *op. cit*., Art. 287.

[47] A. Adamski, *Computer…*, *op. cit*., pp. 115–122.

2.3.3.2. *Fraud – Article 286 CC*

An analysis of the descriptions of cases, acts or charges in proceedings conducted in Poland indicates that acts that can be considered cybercrimes account for approximately 40% of offences classified under Article 286 § 1 CC as fraud (e.g., fake online shops, investments fraud, BEC, CEO fraud, "Nigerian fraud", fraud on online marketplaces). Offences qualified under Article 286 PCC are not traditionally recognised as cybercrime or included in statistics in this area. Given that this qualification extremely often appears in the basis for criminal proceedings or charges, it cannot be omitted from the analysis.

Fraud is a prohibited act, as defined in Article 286 § 1 CC, consisting in leading another person to a disadvantageous disposition of one's own or another person's property by means of misrepresentation or exploitation of a mistake or incapacity to grasp the intended action, in order to obtain a pecuniary benefit. As the Supreme Court points out, the element that distinguishes fraud from other offences against property is the voluntary disposition of property in favour of the perpetrator, and the interference of the criminal law is justified by the fact that the disposition is the result of a misjudgement of the facts by the person making it, which the perpetrator at least consciously exploits.[48]

The elements defining the criminal activity are: introducing a mistake, exploiting a mistake, or exploiting the incapacity of a person to grasp the action taken[49] As indicated by the Supreme Court, misrepresentation means that the perpetrator, by means of deceitful actions, leads another person to a false idea of the actual state of affairs, while the exploitation of a mistake consists in the perpetrator taking advantage of the already existing opinions or ideas of the person harmed.[50] The exploitation of the incapacity of a person to properly

[48] Decision of the Supreme Court of 6.5.2014, IV KK 12/14, Legalis; post. SN of 25.5.2006, IV KK 403/05, Legalis.

[49] Judgement of the Supreme Court of 2.12.2002, IV KKN 135/00, Legalis; Judgment of the Supreme Court of 18.6.2019, V KK 246/18, Legalis.

[50] Judgement of the Supreme Court of 27.10.1986, II KR 134/86, Legalis.

comprehend the action taken is connected with specific features of the person making the property disposal and consists in leading to a disadvantageous property disposal of a person who does not have the capacity to correctly assess the actions taken.[51] This offence is a substantive offence (as indicated by the functional signifier "leads to"), and its effect is the unfavourable disposal of one's own or someone else's property, i.e., reduction of the victim's property, covering both the actual damage to the victim's property and the expected, but lost benefits, as well as deterioration of the victim's financial situation. The act under Article 286 § 1 CC is also an intentional offence, included in the so-called intentional variety of directional offences. It can only be committed with direct intent.

With respect to classic frauds (Article 286 § 1 CC), proceedings are conducted in Poland concerning fraud on online marketplaces, running fake online shops, fictitious collections for the purposes related to support of ill persons and their families, the so-called "Nigerian fraud" – regardless of the social engineering scenario used (also in the scope of the so-called "Love Scam"), investment fraud, BEC (Business Email Compromise) or CEO fraud. Fraudulent acts will also include acts consisting in leading the victim to a disadvantageous disposition of property by misleading him or her as to the need to pay an invoice or acts consisting in sending an invoice with a modified bank account number by an entity impersonating a contractor.[52] However, a different legal qualification of the act should be adopted if the aim of the perpetrator was to infect the victim with malicious software.[53]

[51] Judgment of the Appellate Court in Wrocław of 18.12.2015, II AKa 307/15, Legalis.

[52] CP Report 2020, p. 82.

[53] CSIRT GOV Report for 2020, pp. 26–28.

2.3.3.3. *Identity Theft – Article 190a § 2 CC*

Impersonation is typical of cybercrime perpetrators. Identity theft can therefore be both the perpetrators' main objective and a means to achieve another goal (concealing one's identity or enhancing the effectiveness of a socio-technical-based attack).

The offence of identity theft was introduced into the Criminal Code by the Act of 25.2.2011 amending the Criminal Code.[54] The aim of the regulation was to create an instrument of legal protection in response to persistent harassment (stalking), the manifestations of which also include impersonating the victim by, for example, creating personal accounts on social networks without the victim's knowledge and consent. This type of behaviour would not always fall within the framework of the multi-factor behaviour constituting persistent harassment, which is why the legislator decided to criminalise such a phenomenon separately.[55]

The original elements of the offence of identity theft were regulated narrowly. Furthermore, the act could only be committed with the direct intent (dolus directus coloratus) to cause harm to the person whose data was used. Such a state of affairs was criticised in the literature.[56] In the face of criticism of the regulation, which did not reflect current models of impersonation, legislative action was instituted. According to the amendment[57] of 1 October 2023, Article 190a § 2 CC has been amended as follows: "the same punishment shall be imposed on anyone who, by impersonating another

---

[54] Act of 25 February 2011 amending the Act – Criminal Code, Journal of Laws 2011 No. 72, item 381.

[55] Government Bill to amend the Act – Criminal Code, print No. 3553, 27.10.2010, http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/3553 (accessed on: 1.06.2024).

[56] A. Gryszczyńska, *Kradzieże tożsamości w sprawach z zakresu cyberprzestępczości*, [in:] *Rocznik Bezpieczeństwa Morskiego. Przestępczość Teleinformatyczna 2019*, J. Kosiński, G. Krasnodębski (red.), Gdynia 2020, p. 223; M. Mozgawa, *Opinion on the bill on amendments to the Act – Criminal Code* (Sejm print no. 3553), p. 8, http://orka.sejm.gov.pl/rexdomk6.nsf/Opdodr?OpenPage&nr=3553 (accessed on: 1.06.2024); A. Lach, *Karnoprawna reakcja na zjawisko kradzieży tożsamości*, 2015, LEX/el.

[57] Act of 7 July 2022 amending the Act – Criminal Code and certain other acts (Journal of Laws, item 2600, as amended).

person, uses his/her image, other personal data or other data by means of which he/she is publicly identified, thereby causing him/her financial or personal damage".

With the amendment, dolus directus coloratus is no longer required, however, the offence has become an effect offence and will be committed if the person impersonated incurs damage. Considering the modus operandi of the perpetrators and the purposes for which they impersonate, this provision should be amended again. The offence is committed when the person impersonated as well as another person (e.g., the victim of a fraud facilitated by the impersonation of a trustworthy person) incurs damage.

2.4. The New Regulation Concerning Abuse of Electronic Communications

New challenges and the exploration of new loopholes and attack scenarios are also prompting legislative action. Attacks based on the impersonation of telephone numbers of public officials, police units and banks (CLI spoofing) have led to the initiation of a legislative process to combat the abuse of electronic communications. On 28 July 2023, the law on combating abuse in electronic communication was enacted, which introduces not only new types of criminal acts and criminal sanctions for sending messages impersonating another entity, but also a regulation of an administrative nature relating to the blocking of short text messages (SMS) containing content included in the pattern of messages deemed to be abusive. This law is intended to provide a basis not only for combating smishing, vishing and CLI spoofing but also for blocking domain names impersonating other entities.[58]

The Act on Combating Abuse in Electronic Communications introduces an open catalogue of electronic communication abuse, with the draft defining four basic forms of electronic communication abuse, which are:

[58] https://orka.sejm.gov.pl/opinie9.nsf/nazwa/3069_u/$file/3069_u.pdf (accessed on: 1.06.2024).

1. generating artificial traffic – i.e., sending or receiving messages or voice calls on the telecommunications network using telecommunications equipment or programs, the purpose of which is not to make use of a telecommunications service but to register them at the point of connection of telecommunications networks or by billing systems;
2. smishing – the sending of a short text message (SMS) in which the sender impersonates another entity in order to induce the recipient of the message to perform a specific action, in particular to provide personal data, disadvantage property, open a website, initiate a voice call or install software;
3. CLI spoofing – the unauthorised use or exploitation by a user or telecommunications undertaking making a voice call of address information identifying a natural person, a legal person or an unincorporated entity other than that user or telecommunications undertaking, for the purpose of impersonating another entity, in particular to create fear or a feeling of insecurity or to induce the recipient of that call to perform a specific action, in particular to communicate personal data, to disadvantage property or to install software;
4. unauthorised modification of address information – this is the unauthorised modification of information about the number or identifier of the user sending the communication (identifiers can be, e.g., electronic addresses, names, codes or IP addresses) making it impossible or significantly hindering the determination, by authorised entities or telecommunications undertakings involved in the delivery of the communication, of the telephone number or identifier used to send an electronic communication.

The criminal provisions criminalising the aforementioned abuses in electronic communication are contained in Articles 29–32.

Article 30, which introduces criminal liability for smishing, in addition to liability for sending an SMS message, also criminalises the sending of a message by means of other interpersonal communication services, in which the offender impersonates another entity in order to induce the recipient of the message to transfer personal data, to make a disadvantageous disposition of property,

to open a website, to initiate a voice connection, to install software, to transfer computer passwords, access codes or other data allowing unauthorised access to information stored in a computer system, data communication system or data communication network. This will enhance the fight against groups involved in sending e-mails or instant messaging messages (WhatsApp, Telegram, etc.). This is because the offence under Article 30 will already have been committed at the moment the phishing message is sent, not only when the victim provides login data to the phishing website (Article 269b § 1 CC) or when the perpetrators gain unauthorised access to the victim's data using passwords obtained on the phishing website (Article 267 § 1 CC).

2.5. The Scope of Criminalisation of Cybercrime in Poland in Comparison to International Regulations

Fight against cybercrime was the subject of analysis and legislative actions as early as at the turn of the 1980s and 1990s. These actions were taken in particular by the Council of Europe and resulted in the adoption, on 23 November 2001 in Budapest, of the Convention on Cybercrime of the Council of Europe, which subsequently became the basis for international cooperation in this respect.

In the European Union, the issue of cybersecurity and combating cybercrime has long been addressed only in systemic instruments and fragmentary regulations. In recent years, important legal instruments in this area have included Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

A summary mapping the offences set out in the Cybercrime Convention and Directive 2013/40/EU to Polish criminal law is presented in Table 2.

At this point, it should be pointed out that the conformity of some of the criminal provisions indicated in the table with the requirements of the Convention and the Directive continues to raise concerns, despite several attempts at adjustment. In particular, the definition of document, affecting the scope of criminalisation

of the offence of computer forgery, has been criticised. Critical remarks are also made about Article 269b § 1, Article 268a and the construction of computer fraud (Article 287 § 1 CC).[59]

Table 2. *The scope of criminalisation of cybercrime in Poland in comparison Cybercrime Convention and Directive 2013/40/EU*

Cybercrime Convention	Directive 2013/40/EU	Polish Criminal Code
Article 2 – Illegal access	Article 3 – Illegal access to information systems	Article 267 § 1–2 CC
Article 3 – Illegal interception	Article 6 – Illegal interception	Article 267 § 2 CC, Article 267 § 3 CC
Article 4 – Data interference	Article 5 – Illegal data interference	Article 268 § 2 CC, Article 268a CC, Article 269 CC
Article 5 – System interference	Article 4 – Illegal system interference	Article 269a CC
Article 6 – Misuse of devices	Article 7 – Tools used for committing offences	Article 269b CC
Article 7 – Computer-related forgery		Article 270 § 1 CC (including the definition of a document Article 115 § 14 CC)
Article 8 – Computer-related fraud		Article 287§ 1 CC
Article 9 – Offences related to child pornography		Article 202 § 3, § 4, § 4a CC
Article 10 – Offences related to infringements of copyright and related rights		Article 115–119, Act of 4 February 1994 on Copyright and Related Rights

Source: Own elaboration.

The scope of criminalisation of cybercrime in Poland, may also be influenced by the ongoing work of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established by General Assembly

[59] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę*, [in:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, G. Szpor (red.), Warszawa 2021, pp. 345–356.

Resolution 74/247 (2019).[60] In the work on the new UN Convention, the most contentious issue is to determine the material scope of the new instrument. It is not disputed that the Convention should cover cyber-dependent crimes, i.e., crimes against the confidentiality, integrity and availability of computer systems, networks and data as well as the misuse of such systems, networks and data. Certain state parties indicate that the Convention should also cover narrowly defined cyber-enabled crimes (as defined in the Convention on Cybercrime including offences related to child pornography). A number of states parties, however, have a much broader approach, seeking to extend the new Convention to cover all crimes committed using information and communications technologies.

2.6. Summary and Conclusions

The omnipresence of information and communication technologies in both social and economic life has created new avenues for the infringement of legally protected goods. Attacks on new legal goods related to the essence of the information society (confidentiality, accessibility, integrity of data and information systems) have emerged, as have the methods of infringing traditionally protected goods (property, freedom, dignity). This necessitates the amendment of the substantive criminal law to protect against the new threats.

Given the cross-border nature of cybercrime, the work of the Council of Europe and the European Union has had a significant impact on the shape of criminal regulation in Poland in this area. The 2021 Council of Europe Convention and Directive 2013/40/EU on attacks against information systems define the minimum scope of criminalisation of cybercrime. Despite comments made over the years that Polish legislation does not ensure compliance with the Convention standards, the key provisions relating to cybercrime

[60] Resolution 74/247. 2019. Resolution adopted by the General Assembly on 27 December 2019, A/RES/74/247, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement (accessed on: 1.06.2024).

in Poland have not been amended in the directions indicated by representatives of criminal law doctrine.

The criticised slowness of changes to criminal code provisions relating to cybercrime[61] contrasts with the speed of extra-code provisions, resulting from ad hoc measures related to the increase in specific attacks or the exploration of gaps and vulnerabilities (e.g., the introduction of criminal liability for CLI spoofing and smishing). Over the past few years, the provisions regulating liability for cyber-dependent crimes in the Criminal Code have been encapsulated by extra-code regulations stemming from administrative law acts. They supplement the Code regulation, but significant doubts are raised by legal practitioners as to their relation to the provisions of the Criminal Code. Moreover, some of the non-Code provisions are hardly known even by legal practitioners. For the sake of regulatory consistency, it is advisable to limit the placement of criminal law provisions outside the Criminal Code.

At the same time, statistical analyses of cybercrime cases indicate that the basis of the criminal liability of the perpetrators is mainly established by provisions protecting traditional legal assets (mainly property), in particular Article 286 § 1 CC. Following the amendment to the definition of movable item and the recognition of funds deposited in account as a movable item (Article 115 § 9 CC), the breaking of the security features of an online bank account combined with the taking for the purpose of appropriation of the funds deposited therein is qualified as an act under Article 279 § 1 CC (burglary). On the one hand, this is related to the modus operandi and purpose of the perpetrators, on the other hand to the disproportion of the upper limit of the criminal threat (the crime of fraud is punishable by up to 8 years of imprisonment, burglary – by up to 10 years of imprisonment and the crime of hacking – by up to 2 years of imprisonment).

Following the introduction of criminal liability for smishing and spoofing, as well as the amendments to Article 190a § 2 CC

[61] A. Adamski, *Europejskie standardy prawnokarnej ochrony sieci i informacji oraz ich implementacja do ustawodawstwa polskiego*, [in:] *Internet. Strategie bezpieczeństwa*, G. Szpor, A. Gryszczyńska (red.), Warszawa 2017, pp. 23–45.

(identity theft), the main demands for extending the penalisation of cybercrime have been fulfilled in Poland. The wording of individual provisions still raises some concerns (scope of Article 269b § 1 CC, definition of document (Article 115 § 14) affecting the scope of the offence of computer forgery). Definitely greater deficiencies are diagnosed in the procedural provisions, due to the lack of provisions referring to remote search or extended search, as well as the controversy related to the possibility of applying an undercover surveillance as a result of the use of RAT-type software.

In conclusion, it may be said that the development of cybercrime, however, leads to the need for constant evaluation and improvement of the existing legal regulations, as changes in the threat landscape must be followed by changes in substantive and procedural law. Undoubtedly, another trigger for change will be the need to take into account criminal liability related to the use or abuse of artificial intelligence technology.

REFERENCES

Act of 4 February 1994 on Copyright and Related Rights (consolidated text Journal of Laws 2022, item 2509).

Act of 6 June 1997 – Criminal Code (consolidated text Journal of Laws of 2024, item 17, as amended).

Act of 30 June 2000 Industrial Property Law (consolidated text Journal of Laws 2023, item 1170).

Act of 18 July 2002 on the Provision of Services by Electronic Means (consolidated text Journal of Laws of 2020, item 344).

Act of 5 September 2016 on Trust Services and Electronic Identification (consolidated text Journal of Laws 2024, item 422).

Act of 10 May 2018 on the Protection of Personal Data (consolidated text Journal of Laws 2019, item 1781).

Act of 5 July 2018 on the National Cyber Security System (consolidated text Journal of Laws 2022, item 1863, as amended).

Act of 14 December 2018 on the Protection of Personal Data Processed in Connection with the Prevention and Combating of Crime (consolidated text Journal of Laws 2023, item 1206).

Act of 28 July 2023 on Combating Abuse in Electronic Communications (Journal of Laws 2023, item 170).

Adamski, A., *Europejskie standardy prawnokarnej ochrony sieci i informacji oraz ich implementacja do ustawodawstwa polskiego*, [in:] *Internet. Strategie bezpieczeństwa*, Szpor, G., Gryszczyńska, A., (red.), Warszawa 2017.

Adamski, A., *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę*, [in:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, Szpor, G., (red.), Warszawa 2021.

Adamski, A., *Prawo karne komputerowe*, Warszawa 2000.

Applegate, S.D., "*The dawn of Kinetic Cyber*", 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn 2013, pp. 1–15.

Bill to amend certain laws in relation to the prevention of identity theft, List Number: UD472, https://legislacja.gov.pl/projekt/12367257 (accessed on: 1.06.2024).

C.H. Beck Publishers Report – LegalTech 2023, https://legalis.pl/legaltech-raport-2023/ (accessed on: 1.06.2024).

Council of Europe Convention of 23.11.2001 on Cybercrime (CETS No. 185).

Cyber Security Strategy of the Republic of Poland for 2019–2024, Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cyber Security Strategy of the Republic of Poland for 2019–2024, Monitor Polski 2019, item 1037.

DataReportal, *Digital 2022*, https://datareportal.com/reports/digital-2022-global-overview-report (accessed on: 1.06.2024).

DataReportal, *Digital 2023*, https://datareportal.com/reports/digital-2023-global-overview-report (accessed on: 1.06.2024).

Decision of the Supreme Court of 6.5.2014, IV KK 12/14, Legalis; SN of 25.5.2006, IV KK 403/05, Legalis.

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, OJ EU L 218, 14.8.2013, pp. 8–14.

Eckart, J.P., *The Department of Justice Versus Apple Inc. The Great Encryption Debate Between Privacy and National Security*, "Catholic University Journal of Law and Technology" 2019, Vol. 27, Issue 1, https://scholarship.law.edu/jlt/vol27/iss2/3.

ENISA Foresight Cybersecurity Threats for 2030, 2023, https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030 (accessed on: 1.06.2024).

Gryszczyńska, A., *Kradzieże tożsamości w sprawach z zakresu cyberprzestępczości*, [in:] *Rocznik Bezpieczeństwa Morskiego. Przestępczość Teleinformatyczna 2019*, Kosiński, J., Krasnodębski, G. (red.), Gdynia 2020.

Gryszczyńska, A., *Oszustwa i oszustwa komputerowe – globalni i lokalni gracze*, [in:] *Internet. Global Games*, Szpor, G., Gryszczyńska, A., Wiewiórowski, W.R. (red.), Warszawa 2021.

Gryszczyńska, A., Klawikowski, A., *Nowe wyzwania dla Prokuratury związane ze zwalczaniem przestępczości gospodarczej i cyberprzestępczości*, "Prokuratura i Prawo" 2022, special issue: „Prosecutor's Office in the service of the state and society", pp. 35–56, https://www.gov.pl/web/prokuratura-krajowa/wydanie-specjalne-prokuratura-w-sluzbie-panstwu-i-spoleczenstwu (accessed on: 1.06.2024).

Gryszczyńska, A., Szpor, G., *Hacking in the (cyber)space*, "GIS Odyssey Journal" 2022, Vol. 2, No. 1, pp. 141–152, https://doi.org/10.57599/gisoj.2022.2.1.141, https://www.gisjournal.us.edu.pl/index.php/gis-odyssey-journal/article/view/64 (accessed on: 1.06.2024).

Incident Classification/Incident Taxonomy according to eCSIRT.net, International Version Don Stikvoort, 11 January–19 December 2012 (version mkVI of 31 March 2015), https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (accessed on: 10.5.2023).

Judgment of the Appellate Court of Szczecin of 14.10.2008, II AKa 120/08, Legalis.

Judgment of the Appellate Court in Wrocław of 18.12.2015, II AKa 307/15, Legalis.

Judgement of the Supreme Court of 27.10.1986, II KR 134/86, Legalis.

Judgement of the Supreme Court of 2.12.2002, IV KKN 135/00, Legalis.

Judgment of the Supreme Court of 22 March 2017, III KK 349/16.

Judgment of the Supreme Court of 18.6.2019, V KK 246/18, Legalis.

Kosiński, J., *Cyberprzestępczość AD 2020 – stan aktualny i prognozy*, [in:] *Internet. Cyberpandemia*, Szpor, G., Gryszczyńska, A. (red.), Warszawa 2020.

Malicious Uses and Abuses of Artificial Intelligence, Europol, 2022, https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf (accessed 12.5.2023).

Molenda, K., *Rozpoznanie adwersarzy w wojskowych systemach teleinformatycznych*, [in:] *Internet. Cyberpandemia*, Gryszczyńska, A., Szpor, G. (red.), Warszawa 2020.

Radoniewicz, F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Reddy, N., *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations*, Apress, New York 2019.

Regulation of the Minister of Justice of 7 April 2016. Rules of Procedure for the Internal Office of Common Organisational Units of the Public Prosecutor's Office (i.e., Journal of Laws of 2017, item 1206, as amended).

Report on the state of Poland's cybersecurity in 2021, CSIRT GOV, 2022, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/977,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2021-roku.html, p. 9 (accessed on: 1.06.2024).

Report on the state of Poland's cybersecurity in 2022, CSIRT GOV, 2023, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/979,-Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2022-roku.html (accessed on: 1.06.2024).

Resolution 74/247.2019. Resolution adopted by the General Assembly on 27 December 2019, A/RES/74/247, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement (accessed on: 1.06.2024).

State activities in preventing and combating the consequences of selected internet crimes, including identity theft, Supreme Audit Office, Record No: P/21/042/KPB, 2023.

Szpor, G., Gryszczyńska, A., *Hacking in the (cyber)space*, "GIS Odyssey Journal" 2022, Vol. 2, No. 1, 2022, pp. 141–152, https://doi.org/10.57599/gisoj.2022.2.1.141; https://www.gisjournal.us.edu.pl/index.php/gis-odyssey-journal/article/view/64.

The Budapest Convention (ETS No. 185) and its Protocols, in Poland ratified pursuant to Dz. U. 2015 item 728.

The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2018, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (accessed on: 1.05.2024).

The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2019, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (accessed on: 1.06.2024).

The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2020, https://www.nask.pl/pl/raporty/raporty/4289,RAPORT-CERT-2020.html (accessed on: 1.06.2024).

The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2021, https://cert.pl/uploads/docs/Raport_CP_2021.pdf (accessed on: 1.06.2024).

The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2022, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (accessed on: 1.06.2024).

The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf (accessed on: 1.06.2024)

Worona, J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020.

DR. JUDIT JACSÓ, FULL PROFESSOR

University of Miskolc / Vienna University of Economics and Business | DOI: 10.32041/9788367149761/3

Chapter 3. New Developments and Challenges in the Fight Against Money Laundering by Means of Cybercrime – Methods and Risks

3.1. Introduction

The chapter aims to analyse the development tendencies of money laundering from the 1980s to nowadays, with particular emphasis on the links between money laundering and cyber-criminality. The globalisation, digitalisation and the new technological developments poses serious risks in the fight against money laundering, since criminal offenders are able to use the new and unregulated methods extremely quickly and effectively. The spread of cybercrime was also affected by the COVID-19 pandemic.[1] Therefore, new technologies create new methods for the commission of money laundering, which requires legislators and law enforcement bodies to create and use new measures.

The use of information technologies has become part of our everyday human life. The technological advancements in the 21st century continue to influence society, but its positive elements can also be used for negative purposes.[2] Technology companies are entering the market to provide financial services over the internet by

[1] A. Gryszczyńska, *The impact of the COVID-19 pandemic on cybercrime*, "Bulletin of the Polish Academy of Technical Sciences" 2021, Vol. 69, No. 4, e137933, pp. 1–9.

[2] C. Wronka, *"Cyber-laundering": the change of money laundering in the digital age*, "Journal of Money Laundering Control" 2021, Vol. 25, No. 2, pp. 330–344, DOI: 10.1108/JMLC-04-2021-0035.

introducing new technologies.[3] However, these services can also be exploited by criminals.

It should be stressed that money laundering is a constantly changing phenomenon.[4] Hence, the fight against money laundering is a continuously developing area, which can be seen in international, EU, and domestic regulation. The hypothesis is that the current measures in the European Union are neither adequate nor effective in the fight against cyber-laundering, and that the rules need to be changed. To address this issue, it is necessary to briefly examine the historical development and regulation of money laundering from the beginning, i.e., in the 1980s. The second part of the study will examine the methods and stages of money laundering in the cyber stage and the relation between money laundering and cybercrime. It is necessary to understand the phenomenon of cyber-laundering and crypto-laundering in order to find an effective tool against money laundering in the virtual world.

New technologies facilitate money laundering. The anonymity in the digital world can easily be used to commit crimes, especially money laundering.[5] Money launderers benefit from the decentralisation of blockchain technologies as it lacks a central authority for payment authorisation and control, enabling suspicious transactions to go unnoticed and unreported. Additionally, the pseudonymous nature of the blockchain allows for easy use of tokens in money laundering, as public keys are not linked to real identities, and the use of tumblers or privacy tokens can enjoy near-complete anonymity. Furthermore, the cross-border transferability of crypto asset makes it simple to disguise the illicit origin of assets, enabling the transfer of wealth in the form of cryptocurrency without the need for border controls or physical meetings between money launderers,

[3] See Z. Nagy, *A digitalizáció hatása a pénzügyi piac szabályozására*, "Miskolci Jogi Szemle" 2020, No. 1, pp. 24–25.

[4] I. Ambrus, K. Mezei, *The new Hungarian legislation on money laundering and the current challenges of cryptocurrencies*, "Danube: Law and Economics Review" 2022, Vol. 13, Issue 4, p. 257.

[5] Y. Nizovtsev, O. Parfylo, O. Barabash., S.G. Kyrenko, N. Smetanina, *Mechanisms of money laundering obtained from cybercrime: the legal aspect*, "Journal of Money Laundering Control" 2022, Vol. 25, No. 2, pp. 297–305.

intermediaries, and recipients.[6] In short, cryptocurrencies/crypto assets have the same three characteristics: decentralisation, anonymity and globality.[7]

3.2. Anti-Money Laundering Regulation (AML) – Historical Overview and International Legal Framework

After a brief historical overview, this chapter presents international instruments that have an impact on national action against money laundering. Hungary's and Poland's obligations in the fight against money laundering and terrorist financing are primarily determined by international conventions, the European Union's anti-money laundering directives, and the 40 recommendations of the Financial Action Task Force (FATF).

3.2.1. SOURCE AND FIRST REGULATION OF MONEY LAUNDERING

The term "money laundering" was first used in the 20th century. The regulation of money laundering as a federal crime and anti-money laundering enforcement can be traced back to the United States,[8] where the first Money Laundering Control Act (MLCA) was passed by the United States Congress in 1986. Since then, money

[6] Ph. Maume, L. Haffke, *Kapitel 4 Compliance und Datenschutz § 15 Geldwäsche-Compliance*, [in:] P. Mauma, L. Maute, M. Fromberger, *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020, p. 420.

[7] R. Brandl, J. Bülte, *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung – Perspektive Sorgfaltsverpflichtete*, [in:] R. Leitner, R. Brandl (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Vienna 2023, pp. 106–107.

[8] J. Jacsó, *A pénzmosás elleni nemzetközi fellépés eszközei*, "Magyar Jog" 2000, No. 9, p. 545; I.L. Gál, *A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban*, "Európai Jog" 2007, No. 1, p. 12.

laundering has been punishable in the USA.[9] However, the Bank Secrecy Act (BSA) was established in 1970, even before the abovementioned legislation. The BSA enacted the requirements for reporting by banks and other financial institutions and private individuals to help identify the source of currency and other monetary instruments transported or transmitted into or out of the USA or deposited in financial institutions (introduced an automatic reporting obligation for banks over $10,000).[10] The BSA requires financial institutions to have adequate anti-money laundering (AML) programs, and instructs financial institutions to file suspicious activity reports (SARs). Cyber-enabled crime are illegal activities (e.g., fraud, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers. One of the most important institutions in the Anti-Money Laundering Framework in the USA is the Financial Crimes Enforcement Network (FinCEN) established by the U.S. Department of the Treasury in 1990 in order to provide a government-wide multisource financial intelligence and analysis network.[11]

The fight against money laundering has moved from the USA to Europe and has a three-decade history. The criminals' aim is to prevent the funds from being tracked by law enforcement authorities and to make them appear legal. A significant proportion of funds of criminal origin enter the legal economy through financial institutions and other economic actors. The most important international framework is briefly presented below.

[9] U.S. Code § 1956 Laundering of monetary instruments and § 1957 Engaging in monetary transactions in property derived from specified unlawful activity.

[10] https://www.fincen.gov/history-anti-money-laundering-laws (accessed on: 4.05.2023); S. Jettner, *Money laundering*, "American Criminal Law Review" 2023, Vol. 60, No. 3, p. 1072.

[11] https://www.fincen.gov/ (accessed on: 4.05.2023).

3.2.2. INTERNATIONAL LEGAL FRAMEWORK

3.2.2.1. *United Nations Legal Framework*

On the international level, the first important step was the United Nations (UN) Vienna Convention[12] in 1988. This convention was significant because it was the first international document which defined money laundering. It has been described in Article 3.1 as:

> the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions.

It must be emphasised that the convention defines a broad means of property: it means "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets".[13] The Vienna Convention contains provisions on the confiscation, which was the first step at the international level to promote the confiscation of criminal proceeds.

The UN Palermo Convention[14] against transnational organised crime is also very important. Based on the Vienna Convention, the scope of predicate offences only covered drug crimes, which was significantly expanded by the Palermo Convention. Hungary and Poland have ratified each convention. An added value of these conventions is the creation of a "uniform vocabulary and a shared sense of terms in the field of both national criminalisation and international cooperation".[15] In accordance with the Palermo Convention,

---

[12] UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances adopted in Vienna in 1988 (Vienna Convention).

[13] Art. 1 letter q Vienna Convention.

[14] UN Convention against Transnational Organized Crime adopted in Palermo in 2000 (Palermo Convention).

[15] Á. Péceli, *The legal framework and the difficulties of combating money laundering*, [in:] G. Virág (ed.), *Combating Cybercrime, Corruption and Money*

the member states shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money laundering.[16]

3.2.2.2. *Relevant Conventions of the Council of Europe (Strasbourg Convention and Warsaw Convention)*

The Council of Europe already dealt with the phenomenon of the money laundering in 1980, and adopted the first international instrument, a recommendation against money laundering. However, this act was not binding.[17] The Council of Europe adopted a convention on money laundering, search, seizure and confiscation of the proceeds from crime in 1990 (Strasbourg Convention[18]). The description of money laundering[19] was based on the Vienna Convention. However, the Convention extended the criminal liability to negligent money laundering as punishable, even though it is only an optional provision.[20] The object of the money laundering is "property", that "includes property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title to, or interest in such property".[21]

Laundering, "Training for Judicial Academies of Visegrad 4 Countries. Studies on Criminology" 2022, Vol. 59, Special issue 2, p. 221.

[16] Art. 7 pt 1(b) Palermo Convention.

[17] Recommendation No. R (80)10 on measures against the transfer and the safekeeping of funds of criminal origin. See more: J. Jacsó, *Bekämpfung der Geldwäscherei in Europa unter besonderer Berücksichtigung des Geldwäschestrafrechts von Österreich, der Schweiz und Ungarn. Neuer Wissenschaftlicher Verlag*, Berlin–Wien–Zürich 2007, p. 40.

[18] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, European Treaty Series-No. 141, Strasbourg, 8.11.1990.

[19] Art. 6 Strasbourg Convention.

[20] Á. Péceli, *The legal framework…*, *op. cit.*, p. 224.

[21] Art. 1 letter b Strasbourg Convention. Other relevant terms: "proceeds" means any economic advantage from criminal offences; "instrumentalities" means any property used or intended to be used, in any manner wholly or

The scope of predicate offences was just as significantly expanded, but did not include a catalogue of crimes.[22] It also contained important provisions from the point of view of proving the money laundering: knowledge, intent or purpose required as an element of an offence set forth may be inferred from objective, factual circumstances, and it shall not matter whether the predicate offence was subject to the criminal jurisdiction of the given state.[23] However, it must be underlined that it did not prescribe the criminal responsibility of the perpetrator of the predicate offense for money laundering (self-laundering). It should also be emphasised that the Strasbourg Convention takes into account the cross-border characteristics of money laundering for the first time,[24] so it defines the principles of international cooperation.[25] For the effective cooperation it is essential to approximate the national regulation of substantive criminal law on money laundering.

A significant milestone at the level of the Council of Europe was the adoption of the Warsaw Convention.[26] It provides a comprehensive legal framework to prevent, investigate, and prosecute money laundering and terrorism financing offenses. It sets out clear and stringent obligations for states to take appropriate measures to combat these crimes. According to the convention, the signatures countries:

> shall adopt such legislative and other measures as may be necessary to institute a comprehensive domestic regulatory and supervisory or monitoring regime to prevent money laundering and shall take due account of applicable

in part, to commit a criminal offence or criminal offences. Art. 1 letters a, c Strasbourg Convention.

[22] See J. Grzywot, *Virtuelle Kryptowährungen und Geldwäsche*, [in:] *Internetrecht und Digitale Gesellschaft*, Vol. 15, Berlin 2019, pp. 62–63.

[23] Art. 6(2) letter c Strasbourg Convention.

[24] J. Jacsó, *Bekämpfung…*, *op. cit.*, p. 40.

[25] Chapter III Strasbourg Convention.

[26] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Council of Europe Treaty Series-No. 198, 16.5.2005. (Warsaw Convention).

> international standards, including in particular the recommendations adopted by the Financial Action Task Force on Money Laundering (FATF).[27]

The convention also contains regulations on the introduction of corporate liability.[28] However, not only does it require the domestic legislators to take into account the FATF Recommendation, it can also be observed in its provisions. For example, among the measures to prevent money laundering, it uses a risk-based approach in accordance with the FATF Recommendations.[29] Legislative or other measures shall be adopted as may be necessary to detect the significant physical cross border transportation of cash and appropriate bearer-negotiable instruments.

It facilitates the exchange of information and mutual legal assistance to investigate and prosecute cases effectively across borders. The convention promotes the identification, seizure, and confiscation of proceeds from crime and assets linked to terrorist financing. Effective asset recovery mechanisms are vital to disrupting criminal networks and deterring such activities. It must be emphasised that the Warsaw Convention encourages the establishment and efficient functioning of national financial intelligence units (FIUs). The FIU plays a crucial role in analysing financial information to identify suspicious transactions and potential money laundering or terrorism financing activities. The most important added value of the Warsaw Convention is that it takes the first step in separating the laundering offence from the predicate offence, thus making it possible to establish criminal liability for money laundering without precisely identifying the predicate offence.[30] Both countries Hungary and Poland ratified the conventions.[31]

It must be highlighted that the majority of cases in money laundering involve cross-border money-mule operations, where both

---

[27] Art. 13 – Measures to prevent money laundering, Warsaw Convention.

[28] Art. 10 Warsaw Convention.

[29] Art. 13 – Measures to prevent money laundering, Warsaw Convention.

[30] Á. Péceli, *The legal framework…*, *op. cit.*, p. 224.

[31] See about the ratification: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=198 (accessed on: 4.05.2023).

the predicate offence and the transfer of proceeds occur in distant jurisdictions. International cooperation is crucial for these cases, but finding a legal basis for reaching countries on the other side of the globe can be challenging. This is where the multilateral conventions of the United Nations and the Council of Europe play a very important role by providing a legal framework for dialogue and mutual assistance in global money laundering cases. Ádám Péceli draws attention in his study to the conventions that form the basis of international cooperation.[32]

3.2.2.3. *Universal Anti-Money Standards (FATF)*

The Financial Action Task Force (FATF[33]) is an independent inter-governmental body established in 1989.[34] The FATF currently has 39 members, and the European Commission is a member. This organisation develops and promotes policies to protect the global financial system against money laundering, terrorist financing,[35] and the financing of the proliferation of weapons of mass destruction. The 40 recommendations of FATF are regulatory and operational measures that define a comprehensive framework provided for the basics of each country's AML/CFT system (preventive and repressive measures).[36]

---

[32] Á. Péceli, *The legal framework…*, *op. cit*., p. 224.

[33] See more about the FATF Standard in the chapter about "Preventive means against cyber-laundering in the European Union".

[34] A. Pursiainen, *The FATF and Evolution of Counterterrorism Asset Freeze Laws in the Nordic Countries: We Fought the Soft Law and the Soft Law Won*, [in:] K. Karjalainen, I. Tornberg, A. Pursiainen (eds.), *International Actors and the Formation of Laws*, Springer Cham 2022, p. 135.

[35] The mandate of FATF was in 2001 expanded to include the prevention of terrorism financing.

[36] L.A. Barátki, *A FATF standard és nemzeti szintű végrehajtása*, "Büntetőjogi Szemle" 2021, No. 2, pp. 3–11; B. Udvarhelyi, *Az FATF szerepe a pénzmosás elleni küzdelemben*, [in:] I. Stipta (ed.), *Miskolci Egyetem Doktoranduszok Fóruma. Miskolc, 2012. november 8. Állam- és Jogtudományi Kar szekciókiadványa*, Miskolci Egyetem Tudományszervezési és Nemzetközi Osztály, Miskolc 2013, pp. 193–198.

It is important to emphasise that the FATF Recommendations have a "soft law" nature, without a legally binding effect for members and other countries, and FATF does not have direct legal enforcement power. Despite this fact, countries implement the international standard in order to combat money laundering and terrorist financing. The mechanism can be influential in encouraging countries to comply with its standards. This is achieved by the FATF using special mechanisms: the FATF regularly conducts mutual evaluations (this means not only the technical but also the efficiency test compliance) of its member countries' anti-money laundering and counter-terrorist financing efforts, and the results are published in publicly available reports. Countries that fail to meet the FATF's standards risk being placed on a "grey list" or "blacklist",[37] which can have reputational and economic consequences.[38]

3.2.2.4. *Legal Framework of the European Union*

Money laundering poses significant problems at the Union level of the European Union as well, because it damages the integrity, stability and reputation of the financial sector and threatens the internal market and the internal security of the Union. The lack of EU action against money laundering could lead Member States to adopt measures to protect their financial systems that could be inconsistent with the single market.[39] See the detailed analysis in the next chapter.

---

[37] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html (accessed on: 6.07.2023)

[38] See: https://www.fatf-gafi.org/en/topics/mutual-evaluations.html (accessed on: 6.07.2023). See about the global influence of FATF: A. Pursiainen, *The FATF…*, *op. cit.*, pp. 135–172.

[39] See: J. Jacsó, *A pénzmosás elleni fellépés az Európai Unióban a vonatkozó irányelvek tükrében*, [in:] M. Lévay (ed.), *Az Európai Unióhoz való csatlakozás kihatásai a bűnözés és más devianciák elleni fellépés területén*, Bíbor Kiadó, Miskolc 2004, pp. 143–144; J. Jacsó, *Legújabb fejlemények a pénzmosás szabályozás terén az Európai Unióban*, [in:] I.L. Gál (ed.), *A pénzmosás elleni küzdelem aktuális kérdései*, Pécs 2005, p. 99; B. Udvarhelyi, *Pénzmosás elleni küzdelem az Európai Unióban*, [in:] I. Stipta (ed.), *Studia Iurisprudentiae Doctorandorum Miskolciensium,* Tomus 12, Miskolc 2013, p. 458.

3.3. Methods and Stages of Money Laundering in Cyberspace

Cyberspace is the "virtual" world, denotes the environment created by links between computers and the infrastructure of the Internet. As opposed to the Internet itself, however, cyberspace is the place produced by these links.[40] The development of new technologies fosters financial and economic crime in general, and money launderers in particular use the Internet for the transfer of assets derived from crime.[41] However, the World Wide Web not only facilitated and accelerated communication between people and the sharing of information, but also enabled cross-border crime.[42] The virtual methods used to launder proceeds of criminal activities and finance illicit activities are constantly evolving.[43] Offenders increasingly use innovative technologies to launder criminal assets.

The FATF, the global standard-setting organisation in the fight against money laundering and terrorist financing, regularly publishes thematic reports on its website, in which the organisation presents the relevant methods.

3.3.1. STAGES OF MONEY LAUNDERING IN CYBERSPACE

There are in general three phases of money laundering: placement, layering (distancing) and integration. Together, these three stages constitute the process of legalising illicit property in order to conceal and disguise the connection between the predicate offence and its

[40] https://www.britannica.com/topic/cyberspace (accessed on: 4.07.2023).

[41] K. Kądziołka, *Analysis of the crime rate in Poland in spatial and temporal term*, "Central and Eastern European Journal of Management and Economics" 2016, Vol. 4, No. 1, p. 84.

[42] K. Mezei, *A kiberbűnözés aktuális kihívásai a büntetőjogban*, Budapest 2020, pp. 23–24.

[43] https://www.fatf-gafi.org/en/publications/Methodsandtrends.html (accessed on: 4.05.2023).

benefits. It must be underlined that not all of them are necessarily present in all cyber laundering cases.[44]

1. Placement stage*:* "Placement" is the process of moving dirty money into the legal economy through the financial system or virtual financial system and away from the illegal source. This stage allows criminals to deposit the proceed from the crimes directly typically into bank accounts, after that the criminals use the global payment system and financial institutions. In this stage, the perpetrators can take advantage from the benefits of the new technologies, especially the Internet-based financial systems. This step carries the greatest risk for the criminal. However, it must be underlined that from the point of view of investigation, this is where the opportunity for effective combat a crime is greatest. Most anti-money laundering measures focus on this stage (e.g., obligations of financial and economic actors: the rules of "know your customer", or reporting obligations).
2. Layering stage*:* Layering is the second most-important stage of money laundering. The aim is to make it hard for authorities to detect the money. The goal of the criminals is to get the criminal property as far away from the source, as far from the predicate offence, as possible. This can be done by mixing the dirty money with clean money.[45] Converting fiat currency to crypto currency or foreign currency is also a common method. The offenders prefer to use online banking services and to move money around the world.
3. Integration stage*:* In this final stage of money laundering, the so-called "cleaned" money is successfully reintroduced into the economy. The danger is that the integrated cash can

[44] L. Dornfeld, *Money laundering in the cyberspace*, [in:] Á. Farkas, G. Dannecker, J. Jacsó, *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, p. 458; D.A. Leslie, *Legal Principles for Combatting Cyber laundering*, New York 2014, pp. 14–16.

[45] D.A. Leslie, *Legal…*, *op. cit.*, p. 16.

also be used to future criminal activity. By this stage, it is most difficult to trace the criminal assets back to their illegal origin.

The most common methods for the process of money laundering include online banking and payment, use of virtual currency, online casinos, video games, and e-commerce.[46]

The FATF has looked specifically at issues relating to so-called "professional money laundering" (PML). This term is used to refer to money launderers who specialise "in enabling criminals to evade anti-money laundering and counter terrorist financing safeguards and sanctions in order to enjoy the profits from illegal activities".[47]

3.3.2. CASH COURIERS AND THE MONEY MULE PHENOMENON

The intensive use of cash is one of the simplest ways to launder money (cash couriers). The physical movement of cash across international borders is indeed one of the traditional and most basic methods of laundering money, as it helps criminals conceal the origin of their illicit assets and break the audit trail in the bank system.[48] The technological advancements have made digital financial transactions more prevalent and convenient, but the importance of cash couriers has not changed. Cyber-criminals need money laundering to legalise criminal assets, too. The use of electronic transactions in committing a crime can leave digital footprints that can be traced, so criminals may resort to cash withdrawals to break the audit trail. Laundering traditional and virtual assets is one of a wide range of crimes committed by cybercriminals.[49]

---

[46] See details by L. Dornfeld, *Money...*, *op. cit.*, pp. 459–462.

[47] FATF Report Professional Money Laundering, July 2018, Paris, www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html (accessed on: 10.04.2023), p. 6.

[48] FATF Report Money Laundering Through the Physical Transportation of Cash October 2015.

[49] https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (accessed on: 4.05.2023).

One of the most common methods of money laundering is the so-called "money mule", which involves acts the use of money "couriers".[50] In the broadest sense, a money mule is someone "who transfers or moves illegally acquired money on behalf of someone else" according to the definition given it by FBI.[51] A money mule is a person who "receives money from a third party in their bank account and transfers it to another one or takes it out in cash and gives it to someone else, obtaining a commission for it."[52] Money mules can move funds in various ways, among which are the following: bank accounts, cashier's checks, virtual currency, prepaid debit cards, and money service businesses.[53] Money mules can move online not only through traditional ways, e.g., via bank accounts, and through virtual assets as well. It is important to underline, through the European Money Mule Actions (EMMA[54]) more than 90% of money mule transactions identified are linked to cybercrime.[55]

Based on an investigation carried out by the General Prosecutor's Office in 2020, this method is typical in Hungary: "The 86% majority of the cases were laundering crimes of money mule figures committed by third parties, legalising the proceeds of fraud or IT

[50] K. Phillips, J.C. Davidson, R.R. Farr, C. Burkhardt, S. Caneppele, M.P. Aiken, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, "Forensic Sciences" 2022, Vol. 2, Issue 2, p. 382; K. Mezei, *Pénzmosás a gyakorlatban, különös tekintettel a saját pénzmosásra és az ún "money mule" jelenségre*, "Kriminológiai Közlemények" 2019, No. 79, p. 166.

[51] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules (accessed on: 3.08.2023).

[52] https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling (accessed on: 3.08.2023).

[53] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules (accessed on: 3.08.2023).

[54] EMMA is an anti-money mule operation, an international action coordinated by Europol in cooperation with countries, Eurojust, Interpol, the European Banking Federation (EBF) and the Fintech FinCrime Exchange, https://www.europol.europa.eu/media-press/newsroom/news/european-money-mule-action-leads-to-1-803-arrests (accessed on: 3.08.2023).

[55] See: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling (accessed on: 5.08.2023)

fraud committed in foreign jurisdictions", points out Péceli.[56] From the point of view of legal practice, it is a problem that money mules often do not know that they are participating in the commission of a crime. In the Hungarian practice, he was initially held responsible for negligent money laundering.[57] By the case of money mule it is very important to examine the knowledge of the money mule, because it will be the basis for the classification of the crime (e.g. the amount of money in the bank account, the relationship between the accused and his principal). They are typically responsible for money laundering committed with *dolus eventualis* negligence can only be established in a very narrow circle. The Money Evaluation Report (Fifth Evaluation Round, 2016)[58] indicated that the intent of the perpetrator can be inferred from external circumstances.[59] The Decision of the Curia from 2021 in Hungary notes the following: Without any real intention, the perpetrator opens an account to receive future funds of unclear origin and specifically to be concealed, with the obligation to withdraw the funds in cash and to hand them over to the unknown payer. In such circumstances, the opening of the account is itself a means of concealing the origin of the money received and of preserving the anonymity of the person who is the principal; and that the purpose of the act was precisely that.[60]

[56] Á. Péceli, *Hungary's experiences in combating money laundering*, [in:] G. Virág (ed.), *Combating Cybercrime, Corruption and Money Laundering*, "Training for Judicial Academies of Visegrad 4 Countries. Studies on Criminology" 2022, Vol. 59, Special issue 2, p. 255.

[57] See on classification as negligent money laundering: K. Mezei: *Pénzmosás…*, *op. cit.*, pp. 161–167; G. Kármán, Á. Mészáros, K. Tilki, *Pénzmosás a gyakorlatban*, "Ügyészségi Szemle" 2016, No. 3, pp. 87–89.

[58] https://rm.coe.int/anti-money-laundering-and-counterterrorist-financing-measures-hungary/16807161b4 (accessed on: 3.06.2023).

[59] Á. Péceli, *Hungary's experiences…*, *op. cit.*, p. 251.

[60] See Court Decision: BH 2021.278. Details by: K. Mezei, *A pénzmosás egyes esetei a bírói gyakorlat tükrében, különös tekintettel a saját és a gondatlan pénzmosásra*, "Kúriai Döntések" 2023, No. 3, p. 529.

3.4. Connection Between Money Laundering and Cybercrime

3.4.1. BASIC REMARKS ABOUT CYBERCRIME

Cybercrime can be seen as a product of the 21st century. But first of all, we must answer the question: What does this term mean? The terms "cyber" and "cyberspace" means the virtual world.[61] The term "cybercrime" primarily denotes crime being committed in virtual space. The spread of cybercrime is related to the fact that with the creation of the World Wide Web in the 1990s, an increasing proportion of the world's population has become internet users, according to the figures of the Internet World Statistic almost 70% in June 2022.[62] We must also take into account that a user cannot only connect to digital networks with only one computer device.[63]

Cybercrime can also be understood as a specially form of organised crime (organised cybercrime).[64] One of its characteristics is the borderless nature of cybercrime, which poses a threat to many areas of social and economic life as well as the financial sphere. As McGuire and Dowling pointed out many 'organised' cybercriminals do not operate in the traditional way, they work as loose online networks of organised cyber criminals as part of global online marketplaces. These online groups typically function with a more flexible and decentralised structure,[65] which makes it difficult to fight against them and increases the need to use the anti-money laundering institutional system.

In 1994, the United Nations published its study on IT crime under the title UN Manual on the Prevention and Control of Computer-Related Crime, which defined the possible forms of computer-related

[61] E. Huber, *Cybercrime Eine Einführung*, Wiesbaden 2019, p. 16.

[62] https://www.internetworldstats.com/stats.htm (accessed on: 15.07.2023).

[63] I. Lajtár, *A kiberbűnözésről*, "Ügyészek Lapja" 2019, No. 1, p. 47.

[64] M. McGuire, S. Dowling, *Cybercrime: A review of the evidence Research Report 75 Summary of key findings and implications*, "Home Office Research Report" 2013, No. 75, October, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (accessed on: 4.05.2023); E. Huber, *Cybercrime…*, *op. cit.*, p. 41.

[65] M. McGuire, S. Dowling, *Cyber…*, *op. cit.*, pp. 13–14.

crime and emphasised the importance of international cooperation in the fight against the new type of crime.[66]

The Convention on Cybercrime (Budapest Convention) was adopted by the Council of Europe[67] in 2001, and entered into force in 2004. It was the first international treaty seeking to react to Internet and computer crime (cybercrime) by harmonising national laws, improving investigative techniques, and increasing cooperation among national and international authority.

It must be underlined that there is no uniform definition of cybercrime. There is currently no uniform definition for and distinction between the terms "online crime", "cybercrime" and "internet crime". Basically, cybercrime is understood to mean all crimes that are committed using information and communication technology (ICT) or against it.[68] The term cybercrime is widely used today, particularly in international literature, but also, for example, in the Convention on Cybercrime.[69] Cybercrime can be considered a collective term, which has two main categories: (a) crimes that can only be committed with information systems (cybercrimes in the narrower sense) and (b) crimes that can also be committed using an information system (cybercrime in a broader sense).

David S. Wall called the process of the development of cybercrime the evolution of computer crime and accordingly distinguishes between three generations of cybercrimes:

a) first generation: crimes committed with the use of computers to assist traditional offending,
b) second generation: crimes committed using a network (primarily the Internet), and
c) third generation: true cybercrimes wholly mediated by technology.[70]

---

[66] A.A. Lakatos, *Az informatikai bűncselekmények és a bitcoin*, "Belügyi Szemle" 2017, Vol. 65(1), p. 24.

[67] See the website of the Council of Europe about cybercrime: https://www.coe.int/en/web/cybercrime/home (accessed on: 2.08.2023).

[68] E. Huber, *Cybercrime…*, *op. cit.*, p. 15.

[69] K. Mezei, *A kiberbűnözés szabályozási kihívásai a büntetőjogban*, "Ügyészek Lapja" 2019, Issue 4–5, http://ugyeszeklapja.hu/?p=2592 (accessed on: 4.05.2023).

[70] L. Dornfeld, *Money…*, *op. cit.*, p. 457.

We could ask: To which generation of cybercrime does money laundering belong? In this classification, money laundering is a crime which belongs to the first two generations.

The latest literature distinguishes between two form of cybercrime: a) traditional crimes committed in the new space and b) crimes related to the IT system and space[71]; or cybercrimes in a narrower and in a broader sense.[72] Among the former category of delicts, we can find those which are committed exclusively in the virtual space or in electronic form, and they can be committed in connection with conceptually existing objects and tools, such as information system, cash-substitute payment instruments or data related torts. Cybercrime in the broader sense include crimes that can be committed also in a non-cyber environment but are realised in the digital world, which are increasingly common these days. Money laundering falls into the broader category (another example is child pornography).

As it was already mentioned, money laundering is an accessory crime, therefore, criminal offences that can be classified as cybercrimes may also appear as predicate offences, if they are of a financial gain-generating nature. Two more scenarios are conceivable here: (a) the basic offense is a cyber-crime, but money laundering is committed with the use of non-computer technology and (b) both the predicate offence and the money laundering take place in the cyberspace. The greatest danger is related to the latter case, since the detection of the crime can be made more difficult if it is committed online.

3.4.2. THE MEANING OF CYBER-LAUNDERING

Parallel with the spread of Internet use and the exponential growth of new payment technologies (electronic payment system), part of the money laundering process has moved into the virtual space,

[71] Z. Nagy, *A kiberbűncselekmények fogalma és csoportosítása*, [in:] T. Kiss (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020, pp. 33–34.
[72] I. Ambrus, *Digitalizáció és büntetőjog*, Budapest 2021, p. 290.

which has presented a new challenge to law enforcement authorities.[73] The concept of *cyber-laundering* began to be used to describe this new phenomenon. In the literature several definitions were used at the beginning: e-laundering, electronic money laundering, digital money laundering. This is related to the fact that cyber-laundering is based on the concept of e-payments, or virtual money laundering.[74] However, "cyber-laundering" has become the most commonly used term.[75] According to Wronka's approach "the criminal practice of money laundering in cyberspace through online transactions has been termed cyber-laundering".[76] There is a literature approach, according to which cyber-laundering belongs to the group of "combinational cybercrime offences", this include "acts that combine a number of different offences in sole acts".[77]

Cyber-laundering is a term that combines cybercrime and money laundering, representing the convergence of these two illicit activities, which is why the fight against it is a special challenge. However, the purpose of cyber-laundering is no different from the traditional form of money laundering, i.e., to make it impossible to identify the origin of illegally acquired money, i.e., money gained by means of crime.

According to the definition of Leslie, cyber-laundering "is the use of a computer to form a transaction or a relationship involving property or benefit, whether tangible or intangible, which is derived

---

[73] C. Wronka, *"Cyber-laundering"…*, *op. cit.*, p. 330; E. Ilbiz, Ch. Kaunert, *Sharing Economy for Tackling Crypto-Laundering: The Europol Associated 'Global Conference on Criminal Finances and Cryptocurrencies'*, "Sustainability" 2022, Vol. 14, Issue 11, p. 6.

[74] R. Stokes, *Virtual money laundering: the case of Bitcoin and the Linden dollar*, "Information and Communications Technology Law" 2012, Vol. 21, Issue 3, pp. 221–236.

[75] K. Phillips *et al.*, *Conceptualizing…*, *op. cit*, p. 387; C. Wronka, *"Cyber-laundering"…*, *op. cit.*, p. 330.

[76] C. Wronka, *"Cyber-laundering"…*, *op. cit.*, pp. 330–344.

[77] According to the systematization there are 5 groups of cybercrimes, see: K. Phillips *et al.*, *Conceptualizing…*, *op. cit.*, p. 387; G. Tsakalidis, K. Vergidis, *A systematic approach toward description and classification of cybercrime incidents*, "IEEE Transactions on Systems, Man, and Cybernetics: Systems" 2017, Vol. 49, p. 716.

from criminal activity".[78] Leslie also points out that the classification of cyber-laundering encompasses three main standpoints:

a) the first opinion considers it a subset of cybercrime, focusing primarily on its technical aspects,
b) the second perspective views it as an innovative method for money laundering,
c) the third viewpoint treats cyber laundering as a distinct phenomenon, blending elements from both cybercrime and traditional money laundering. In must be underlined, that cyber-laundering is not a crime separate from that of money laundering.[79]

In broadest sense cyber-laundering can be defined as a new form of money laundering in the digital age, where the criminals use digital platforms for the transfer of the illegally obtained assets from the predicate offences and making them appear to be of a legitimate origin. Cyber-laundering is usually linked to organised crime and terrorism.

In recent years the rapid expansion in the types of crypto-assets and the purposes for which has been observed.[80] When cryptocurrencies are used in the money laundering process, we can speak about crypto-laundering.[81] The use of cryptocurrencies is associated with a high risk of money laundering and terrorist financing.[82] Cryptocurrencies have become a new tool for crime groups to use this for illicit activities, for launder illegally obtained assets, which aim is to avoid law enforcement agency (LEA) investigations. However, it is essential that cryptocurrencies themselves are not inherently tools for crime; it is the misuse and exploitation of these technologies by individuals or groups that lead to such issues.

---

[78] D.A. Leslie, *Legal…*, *op. cit.*, p. 56.

[79] D.A. Leslie, *Legal…*, *op. cit.*, p. 61; L. Dornfeld, *Money…*, *op. cit.*, p. 457; K. Mezei, *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, PhD dissertation, Pécs 2019, p. 138.

[80] L. Staffler, *Business Criminal Law A primer for Management and Economics*, Wiesbaden 2022, p. 245.

[81] E. Ilbiz, C. Kaunert, *Sharing…*, *op. cit.*, p. 6.

[82] K. Mezei, *A kiberbűnözés aktuális kihívásai a büntetőjogban*, Budapest 2020, p. 201.

It can be determined in summary that cyber-laundering (especially with crypto laundering) is a growing phenomenon which by the lack of implementation of anti-money laundering measures (e.g., identification verifications or other know-your-customer procedures or unregulated trading platform, insufficient security) is promoted on the Internet.[83] In this field, it must be underlined that Eurojust's casework shows that crypto-currencies are increasingly misused by criminals to launder their criminal profits.[84] The question about money laundering with crypto-currencies will be details analysed in the next point.

3.4.3. AML POTENTIAL RISK OF VIRTUAL CURRENCIES AND CRYPTO ASSETS

3.4.3.1. *Conceptual Clarification of Definitions*

For conceptual definitions, we rely primarily on the FATF standards for virtual currency. In accordance with the definition of FATF, virtual currency is a digital representation of value which can be digitally traded and functions as a medium of exchange and/or a unit of account and/or a store of value, but does not have legal tender status in any jurisdiction.[85] Virtual currency is one kind of internet-based payment system. Virtual currency is distinguished from fiat currency (real money) and from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. Digital currency is an umbrella

[83] B. Horten, M. Gräber, *Cyberkriminalität Übersicht zu aktuellen und künftigen Erscheinungsformen*, "Forensische Psychiatrie, Psychologie, Kriminologie" 2020, Vol. 14, p. 236; I. Ambrus, K. Mezei, *The new Hungarian legislation on money laundering and the current challenges of* cryptocurrencies, "Danube: Law and Economics Review" 2022, Vol. 13, Issue 4, p. 257.

[84] https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering (accessed on: 3.07.2023).

[85] *FATF Report Virtual Currencies – Key Definitions and Potential Anti-money Laundering and Counter-terrorist Financing Risks*, June 2014, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html (accessed on: 2.08.2023), p. 4.

term and is used in the broader sense that virtual currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency".[86] Several groups of currencies can be distinguished. Convertible (open) virtual currency can be exchanged for real money or other virtual currencies, while non-convertible currency cannot be exchanged for fiat currency.[87] The FATF report also contains provision in connection with cryptocurrency, that "refers to a math-based, decentralised convertible virtual currency that is protected by cryptography, i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred".[88]

In accordance with the definition of the FATF Recommendation (adopted version February 2023), a virtual asset is:

> a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Virtual asset service provider:

> means any natural or legal person who is not covered elsewhere under the Recommendations, and, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies;

[86] *FATF Report Virtual Currencies…*, *op. cit.*, p. 4.

[87] It is officially transferrable only within a specific virtual environment and is not convertible, however, this rule can be abused. Other group is: *centralised* and *non-centralised virtual currency*. See *FATF Report Virtual Currencies…*, *op. cit.*, p. 4.

[88] FATF Report Virtual Currencies, *op. cit.*, p. 5.

> ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[89]

The idea of crypto-currencies is to create an alternative to book money and fiat money, which can be used as a central-bank-independent, digital means of payment for goods or services.[90] Criminals always find unregulated areas, therefore crypto-assets, especially crypto-currencies, were increasingly used in the process of legalising criminal assets. Crypto assets were outside the scope of EU legislation and have been unregulated for a long time. The crypto assets are neither issued nor guaranteed by a central bank or a public authority. It is important to highlight that we should use the term crypto asset instead of the term crypto currency or crypto money, because these may only be used to designate what is issued by a central bank as a unit specified in payment transactions. Crypto currencies such as Bitcoin do not meet these requirements.[91] They create a risk for financial stability and also for financial crime. Bitcoin used as alternative currency for drug dealing and money laundering as a result of its high degree of anonymity. At the beginning the new digital "money" represented a challenge for public authorities, given the legal uncertainty, and they are used by criminals, fraudsters and money launderers to perform illegal activities.[92]

---

[89] FATF International Standards on combating money laundering and the financing of terrorism & proliferation FATF Recommendation. (Adopted on 16 February 2012 and regularly updated since. Last updated in February 2023), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (accessed on: 4.05.2023).

[90] A. Izzo-Wagner, L.M. Siering, *Kryptowährungen und geldwäscherechtliche Regulierung*, Wiesbaden 2020, p. 2.

[91] Ibidem, p. 4.

[92] European Central Bank: Virtual currencies schemes October 2012, p. 6; www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (accessed on: 07.07.2023).

According to the European Bank Authority, a virtual currency is "a form of unregulated digital money that is not issued or guaranteed by a central bank and that can act as means of payment".[93] Virtual currencies come in many forms, beginning as currencies within online computer gaming environments and social networks, and developing into means of payment accepted "offline" or in "real life". It is now increasingly possible to use virtual currencies as a means to pay for goods and services with retailers, restaurants and entertainment venues. These transactions often do not incur any fees or charges, and do not involve a bank. More recently, the virtual currency 'Bitcoin' has set the standard for a new generation of decentralised, peer-to-peer virtual currencies – often also referred to as crypto currencies. Following the currency's recent growth, dozens of other virtual currencies have arrived in Bitcoin's wake.

Crypto assets are often associated with Bitcoin. Based on blockchain technology to record a transaction, it is the first digital currency in the world as well as the most well-known and widely used cryptocurrency. The development began with the launch of the Bitcoin network and the so-called "Bitcoin white paper"[94] in 2008.[95]

It is important to underline that Bitcoin cannot be considered as electronic money in the general sense, because no organisation has oversight over it and there is no asset backing it up, as Dornfeld emphasises.[96]

There are several types of services that can be used with crypto currencies:[97]

a) the exchange of money (both between traditional [fiat] money and crypto-assets and between different crypto-assets);
b) financing transactions (in particular P2P transactions, loans in crypto assets, transactions using crypto assets as collateral):

[93] EBA/WRG/2013/01 12 December 2013 Warning to consumers on virtual currencies.

[94] The term was used by S. Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*, bitcoin.pdf (accessed on: 4.05.2023).

[95] A. Izzo-Wagner, L.M. Siering, *Kryptowährungen…*, *op. cit.*, p. 2.

[96] L. Dornfeld, *Money…*, *op. cit.*, p. 458.

[97] Z. Halász, *Kihívások a pénzügyi fogyasztóvédelem szabályozásában: kriptoeszközök és ügyfélvédelem*, "Iustum Aequum Salutare" 2022, Vol. 1, p. 75.

– trading in crypto assets (operation of crypto exchanges),
– investment transactions and services involving crypto assets rather than traditional financial assets (in particular, custody services, portfolio management).

3.4.3.2. *Potential Risks Associated with Cryptocurrency*

There are several reasons why cryptocurrencies are attractive for criminals.[98] At international level it must be emphasised that the first *FATF Report about virtual currencies* in 2014 identified some reasons in relation to *convertible virtual currencies*, which are potentially vulnerable for using for purposes of money laundering (terrorist financing):

> First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.[99]

At the level of the European Union, the European Bank Authority drew attention to risks of the crypto-currency in generally in 2014.[100]

---

[98] See V. Halász, *The new challenges in Cyberspace for following illicit money flows*, [in:] Á. Farkas, G. Dannecker, J. Jacsó, *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 440–443.

[99] *FATF Report Virtual Currencies…, op. cit.*, p. 9.

[100] EBA Opinion "virtual currencies" EBA/Op/2014, July 2014, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 (accessed on: 4.05.2023), p. 6.

The EBA recommends that EU legislators consider declaring market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges as "obliged entities" under the EU Anti Money Laundering Directive and thus subject to its anti-money laundering and counter terrorist financing requirements.

As Brandl and Bülte point out, cryptocurrencies are perceived as a specific risk, an instrument of illegality in the practice of law enforcement and security authorities in Germany.[101] Traditionally, money has been the object of this crime, but today the offence is often committed to the crypto-currencies.

3.5. Conclusion and Proposals

The development of the digital technologies had opened the door to the new types and methods of criminal activities, including money laundering as well. It is the reason that cybercrime and money laundering are two of the biggest challenges of our time.

The COVID-19 epidemic and the expansion of the new payment technologies and innovative payment system has given new impetus to the spread of cybercrime and to money laundering. Crypto (currency) assets have expanded into practically every country and sector in the last decades. The unique characteristics of *blockchain-based technologies* offer an unprecedented opportunity to investigate organised crime and money laundering networks and to recover the illicit asset.

It was explained in the previous chapters that the international anti-money laundering institutions and the countries also waited a long time to find out how they could fight against crypto-crimes and cyber-laundering, especially crypto-laundering. The established institutional and framework system against money laundering since the 1990s could also be used to remove the financial base of cybercrime as a predicate offence of money laundering. The fight against money laundering was initially closely linked

[101] R. Brandl, J. Bülte, *Kryptowährungen…*, *op. cit.*, p. 112.

to the fight against organised crime (including drug trafficking). But today the so-called 'all-crime approach' has become significant, which means that all criminal activity could be a predicate offence of money laundering. This means that the crimes in the field of cybercrime can also be predicate offence of money laundering, if they result in financial advantage or assets.

Finally, I would like to highlight the new approach established by the Basel Institute on Governance and the Europol. Five recommendations were formed in order to help the public and private actors to prevent the abuse for money laundering purposes. There are following: The first and most important recommendation is the first one which required to break down silos between "traditional" and "crypto"', which means the crypto-assets related crime and money laundering should not be separated. Crypto-assets has to be treated like any other asset for the purposes of AML/CFT supervision and enforcement, it is important to include the crypto assets (and service providers) into the existing AML/CFT frameworks, such laws should be broad enough to cover crypto assets and capable to anticipate future evolutions in the crypto industry Secondly, it is required to regulate broadly and make full use of existing law). A new approach was established that the blockchain does offer promising opportunities to investigate and disrupt organised crime networks and to recover illicit assets. The third recommendation is to take advantage of the blockchain to disrupt organised crime. In addition, the need for training, adequate communication and the increase cooperation between public and private actor of the AML regime was also stated.[102]

[102] Basel Institute on Governance – Europol, *Seizing the opportunity: five recommendations for crypto assets-related crime and money laundering. 2022 Recommendations of the joint working group on criminal finances and cryptocurrencies*, p. 1; https://www.europol.europa.eu/publications-events/publications/seizing-opportunity-five-recommendations-for-crypto-assets-related-crime-and-money-laundering (accessed on: 2.08.2023).

REFERENCES

Ambrus, I., *Digitalizáció és büntetőjog*, Budapest 2021.

Ambrus, I., Mezei, K., *The new Hungarian legislation on money laundering and the current challenges of cryptocurrencies*, "Law and Economics Review" 2022, Vol. 13, Issue 4, pp. 256–268.

Barátki, L.A., *A FATF standard és nemzeti szintű végrehajtása,* "Büntetőjogi Szemle" 2021, No. 2, pp. 3–11.

Brandl, B., Bülte, J., *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung –Perspektive Sorgfaltsverpflichtete*, [in:] Leitner, R., Brandl, R. (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Vienna 2023, pp. 105–122.

Dornfeld, L., *Money laundering in cyberspace*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (eds.), *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 456–465.

Gál, I.L., *A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban*, "Európai Jog" 2007, No. 1, pp. 12–23.

Gryszczyńska, A., *The impact of the COVID-19 pandemic on cybercrime*, "Bulletin of the Polish Academy of Sciencies Technical Sciences" 2021, Vol. 69, No. 4, pp. 1–9.

Grzywot, J., *Virtuelle Kryptowährungen und Geldwäsche*, [in:] *Internetrecht und Digitale Gesellschaft*, Berlin 2019.

Halász, V., *The new challenges in Cyberspace for following illicit money flows*, [in:] Farkas, Á., Dannecker, G., Jacsó, J., *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 440–449.

Halász, Zs., *Kihívások a pénzügyi fogyasztóvédelem szabályozásában: kriptoeszközök és ügyfélvédelem*, "Iustum Aequum Salutare" 2022, No. 1, pp. 75–83.

Horten, B., Gräber, M., *Cyberkriminalität Übersicht zu aktuellen und künftigen Erscheinungsformen,* "Forensische Psychiatrie, Psychologie, Kriminologie" 2020, Vol. 14, pp. 233–241.

Ilbiz, E., Kaunert, C., *Sharing Economy for Tackling Crypto-Laundering: The Europol Associated Global Conference on Criminal Finances and Cryptocurrencies*, "Sustainability" 2022, Vol. 14, Issue 11, https://www.mdpi.com/2071-1050/14/11/6618/pdf-vor (accessed on: 4.05.2023).

Izzo-Wagner, A., Siering, L.M., *Kryptowährungen und geldwäscherechtliche Regulierung*, Wiesbaden 2020.

Jacsó, J., *A pénzmosás elleni fellépés az Európai Unióban a vonatkozó irányelvek tükrében*, [in:] Lévay, M. (ed.), *Az Európai Unióhoz való csatlakozás kihatásai a bűnözés és más devianciák elleni fellépés területén*, Bíbor Kiadó, Miskolc 2004, pp. 142–157.

Jacsó, J., *A pénzmosás elleni nemzetközi fellépés eszközei*, "Magyar Jog" 2000, No. 9, pp. 545–555.

Jacsó, J., *Az EU III. pénzmosási irányelve és magyarországi gyakorlati tapasztalatai*, "Rendészeti Szemle" 2009, No. 7–8, pp. 221–228.

Jacsó, J., *Bekämpfung der Geldwäscherei in Europa unter besonderer Berücksichtigung des Geldwäschestrafrechts von Österreich, der Schweiz und Ungarn,* Berlin–Wien–Zürich 2007.

Jacsó, J., *Gondolatok az Európai Unió pénzmosás elleni büntetőpolitikájáról a hatodik Pénzmosás elleni uniós irányelv tükrében*, [in:] Bárd, P., Borbíró, A., Gönczöl, K. (eds.), *Kriminológia és kriminálpolitika a jogállam szolgálatában. Tanulmányok Lévay Miklós tiszteletére*, Budapest 2019, pp. 401–411.

Jacsó, J., *Legújabb fejlemények a pénzmosás szabályozás terén az Európai Unióban*, [in:] Gál, I.L. (ed.), *A pénzmosás elleni küzdelem aktuális kérdései*, Pécs 2005, pp. 98–122.

Jacsó, J., Udvarhelyi, B., *A pénzmosás elleni fellépés aktuális tendenciái az Európai Unióban*, "Ügyészségi Szemle" 2017, No. 1, pp. 8–24.

Jacsó, J., Udvarhelyi, B., *The fight against money laundering in Hungary*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (eds.), *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud,corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 295–309.

Jettner, S., *Money laundering*, "American Criminal Law Review" 2023, Vol. 60, No. 3.

Karjalainen, K., Tornberg, I., Aleksi, P. (eds.), *International Actors and the Formation of Laws,* Springer, Cham 2022.

Kądziołka, K., *Analysis of the crime rate in Poland in spatial and temporal term*, "Central and Eastern European Journal of Management and Economics" 2016, Vol. 4, No. 1.

Kármán, G., Mészáros, Á., Tilki, K., *Pénzmosás a gyakorlatban*, "Ügyészségi Szemle" 2016, No. 3, pp. 82–97.

Lajtár, I., *A kiberbűnözésről*, "Ügyészek Lapja" 2019, No. 1, pp. 47–52.

Lakatos, A.A., *Az informatikai bűncselekmények és a bitcoin*, "Belügyi Szemle" 2017, Vol. 65(1), pp. 24–44.

Langlois, D., *The Revision of the EU Framework on the Prevention of Money Laundering*, "Eucrim – The European Criminal Law Associations' Forum" 2013, Issue 3, pp. 96–98.

Leslie, D.A., *Legal Principles for Combatting Cyberlaundering*, New York 2014.

Maume, Ph., Haffke, L., § 15 *Geldwäsche-Compliance*, [in:] Mauma, Ph., Maute, L., Fromberger, M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020, pp. 417–454.

McGuire, M., Dowling, S., *Cybercrime: A review of the evidence*, [in:] *Research Report. Summary of key findings and implications*, "Home Office Research Report" 2013, No. 75, October, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (accessed on: 4.05.2023).

Mezei, K., *A kiberbűnözés aktuális kihívásai a büntetőjogban*, Budapest 2020, pp. 23–24.

Mezei, K., *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, PhD dissertation, Pécs 2019.

Mezei, K., *A pénzmosás egyes esetei a bírói gyakorlat tükrében, különös tekintettel a saját és a gondatlan pénzmosásra*, "Kúriai Döntések" 2023, No. 3, pp. 523–530.

Mezei, K., *Pénzmosás a gyakorlatban, különös tekintettel a saját pénzmosásra* és *az* ún *'money mule' jelenségre*, "Kriminológiai Közlemények" 2019, No. 79, pp. 161–167.

Nagy, Z., *A digitalizáció hatása a pénzügyi piac szabályozására*, "Miskolci Jogi Szemle" 2020, No. 1, pp. 24–32.

Nagy, Z., *A kiberbűncselekmények fogalma és csoportosítása*, [in:] Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest, 2020.

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, bitcoin.pdf (accessed on: 4.05.2023).

Nizovtsev, Y.Y., Parfylo, O.A., Barabash, O.O., Kyrenko, S.G., Smetanina, N.V., *Mechanisms of money laundering obtained from cybercrime: the legal aspect*, "Journal of Money Laundering Control" 2022, Vol. 25, No. 2, pp. 297–305.

Péceli, Á., *Hungary's experiences in combating money laundering*, [in:] Virág, G. (ed.), *Combating Cybercrime, Corruption and Money Laundering*, "Training for Judicial Academies of Visegrad 4 Countries. Studies on Criminology" 2022, Vol. 59, Special issue 2, pp. 244–263.

Péceli, Á., *Money Laundering Techniques based on the FATF typologies and case experience. The evolution of national criminalisation and practice*, [in:] Virág, G. (ed.), *Combating Cybercrime, Corruption and Money Laundering*, "Training for Judicial Academies of Visegrad 4 Countries. Studies on Criminology" 2022, Vol. 59, Special issue 2, pp. 264–283.

Péceli, Á., *The legal framework and the difficulties of combating money laundering*, [in:] Virág, G. (ed.), *Combating Cybercrime, Corruption and Money Laundering*, "Training for Judicial Academies of Visegrad 4 Countries. Studies on Criminology" 2022, Vol. 59, Special issue 2, pp. 220–243.

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S., Aiken, M.P., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, "Forensic Sciences" 2022, Vol. 2, Issue 2, pp. 379–398.

Pursiainen, A., *The FATF and Evolution of Counterterrorism Asset Freeze Laws in the Nordic Countries: We Fought the Soft Law and the Soft Law Won*, [in:] Karjalainen, K.,Tornberg, I., Aleksi, P. (eds.), *International Actors and the Formation of Laws*, Springer, Cham 2022.

Staffler, L., *Business Criminal Law A primer for Management and Economics*, Wiesbaden 2022.

Stokes, R., *Virtual money laundering: the case of Bitcoin and the Linden dollar*, "Information and Communications Technology Law" 2012, Vol. 21, Issue 3, pp. 221–236.

Tsakalidis, G., Vergidis, K., *A systematic approach toward description and classification of cybercrime incidents*, "IEEE Transactions on Systems, Man, and Cybernetics: Systems" 2017, Vol. 49, pp. 210–227.

Udvarhelyi, B., *Az FATF szerepe a pénzmosás elleni küzdelemben,* [in:] Stipta, I. (ed.), *Miskolci Egyetem Doktoranduszok Fóruma. Miskolc, 2012. november 8. Állam- és Jogtudományi Kar szekciókiadványa*, Miskolci Egyetem Tudományszervezési és Nemzetközi Osztály, Miskolc 2013, pp. 193–198.

Udvarhelyi, B., *Pénzmosás elleni küzdelem az Európai Unióban*, [in:] Stipta, I. (ed.), *Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai*, Tomus 12., Miskolc 2013, pp. 455–471.

Wronka, C., *"Cyber-laundering": the change of money laundering in the digital age*, "Journal of Money Laundering Control" 2021, Vol. 25, No. 2, pp. 330–344.

DR. JUDIT JACSÓ, FULL PROFESSOR

University of Miskolc / Vienna University of Economics and Business | DOI: 10.32041/9788367149761/4

Chapter 4. Preventive Means Against Cyber-Laundering in the European Union

4.1. Introduction

The dynamic change in money laundering methods requires regulatory authorities including those in the European Union (EU) to constantly modify their regulations to effectively combat these illicit activities. The chapter deals with the preventive measures of the European Union against money laundering, with regard to cyber-laundering. It is difficult to estimate the scale of money laundering, given the high latency rate for legalised amounts.[1] The same can be established with regard to cyber-laundering.[2] In accordance with the Europol-report, between 0.7–1.28% of annual EU GDP is identified as being involved in suspect financial activity.[3]

[1] The estimated amount of money laundered globally in one year is 2–5%. According to the study of Bussmann and Vockrodt, this amount could be over EUR 100 billion a year in Germany (K.D. Bussmann, M. Vockrodt, *Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie*, "Compliance Berater" 2016, No. 5, p. 139).

[2] D.A. Leslie, *Legal Principles for Combatting Cyberlaundering*, New York 2014, pp. 4–5.

[3] Europol Financial Intelligence Group, *From suspicion to action converting financial intelligence into greater operational impact 2017*, p. 5, https://www.europol.europa.eu/publications-events/publications/suspicion-to-action-converting-financial-intelligence-greater-operational-impact#downloads (accessed on: 06.06.2023).

Since 1991, the European Union has been trying to create an effective and coherent framework against money laundering, which includes five anti-money laundering directives, requiring Member States to prescribe service providers with many obligations, the most important of which are the identification of their customers (Know Your Customer (KYC) and the Suspicious Transaction Reports (STRs)).

It is important to emphasise that the European Union regulation has been taken into account the international standards, especially the Forty Recommendations of the Financial Action Task Force (FATF) and international conventions of the United Nations and the Council of Europe[4] when formulating the obligations from the beginning. Several reports of international organisations and scientific studies pointed to the danger that the Anti-Money Laundering (AML) regime, which was created against the traditional forms of money laundering, was not adequate against money laundering using virtual methods, which in turn made it necessary to modify them and extend their scope to virtual assets (VAs) and virtual assets providers (VASPs).[5] At the 4th Global Conference on Cryptocurrencies and Criminal Finances conference held in November 2020, it was stated that VASPs should be regulated in the same way as other financial services and should also contribute to the fight against global money laundering.[6] An important and necessary first step in the action against virtual assets (cryptocurrency) laundering was the creation of a regulatory framework.[7]

---

[4] See the chapter about "New developments and challenges of the fight against money laundering by the cybercrime – methods and risks".

[5] Z. Céman, M. Hegedűs, *Pénzmosás mint negatív gazdasági tényező az Európai Unióban*, "Belügyi Szemle" 2023, No. 5, p. 885.

[6] See the 5 Recommendation of the Conference which was organised by Interpol, Basel Institute of Governance and Europol, https://baselgovernance.org/sites/default/files/2020-11/Crypto%20Conference%202020%20Recommendations.pdf (accessed on: 05.06.2023).

[7] See Ch. Rückert, *Phänomenologie,* [in:] Ph. Mauma, L. Maute, M. Fromberger, *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020, pp. 527–536; B. Brandl, J. Bülte, *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung – Perspektive Sorgfaltsverpflichtete*, [in:] R. Leitner, R. Brandl (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Vienna 2023, pp. 105–122.

In the first part of the study, we briefly summarise the development at international level with particular regard to the FATF Recommendations, according to which the European Union preventive regulations have also constantly been changed. Among the wide range of preventive instruments against money laundering (cyber laundering), the focus is on the risk-based approach, which is fundamentally of a basic nature, the reporting obligation and the role of the Financial Intelligence Unit (FIU). After this, the latest developments in the EU will be examined and the resulting proposals will also be covered. When outlining development trends, the focus is on the examination of the effectiveness of action against new forms of money laundering, with particular attention to VAs and VASPs.

4.2. Global Standard (FATF Recommendations) in Connection to VAs and VASPs

4.2.1. REGULATORY DEVELOPMENT

The FATF's 40 Recommendations[8] were first published in 1990. FATF has modified and revised the recommendations several times. The FATF Recommendation provides countries with a comprehensive framework to combat illicit financial flows. The document contains the following 7 parts:

1. AML/CFT policies and coordination,
2. money laundering and confiscation,
3. terrorist financing and the financing of proliferation,
4. preventive measures,
5. transparency and beneficial ownership of legal persons and arrangements,
6. power and responsibilities of competent authorities and other institutional measures,
7. international cooperation.

[8] The FATF Recommendations International Standards on Combating Money Laundering and Terrorism & Proliferation, updated February 2023. See: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (accessed on: 3.06.2023).

It should be highlighted that the Recommendations use the risk--based approach (RBA), which means:

> countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively.[9]

Countries must distinguish between high and low risk and adapt the necessary measures accordingly. This basic concept encourages a more efficient allocation of resources.

The FATF recognised that new and innovative payment products and services are developed which have the potential of being used for money laundering or terrorist financing.[10] The FATF has developed guidance for countries and the private sector on how to apply a risk-based approach to implementing AML/CFT measures. With the development of digitalisation, the risk of money laundering increased. Recognising this, the New Payment Products and Services Guidance[11] was published as a first step in 2013. This guidance examines how these payment products and services work, and how to regulate and supervise this activity. It deals with the risks of prepaid cards, mobile payments and internet-based payment. However, the FATF Guidance was not addressed to virtual currencies. It only notes that whereas "some alternative currencies, such as decentralised digital currencies, may fall outside the scope of this guidance, the guidance remains relevant where such currencies are exchanged or redeemed."[12]

---

[9] See FATF Recommendation 1.

[10] See J. Grzywot, *Virtuelle Kryptowährungen und Geldwäsche*, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2019, p. 90.

[11] Guidance for a risk-based approach – prepaid-cards, mobile payments and internet-based payment services, June 2013, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-npps-2013.html (accessed on: 03.07.2023).

[12] Guidance for a risk-based approach – prepaid-cards, mobile payments and internet-based payment services, June 2013, p. 3.

Recognising that virtual currencies would spread in the coming years, and that national policy responses vary considerably, the FATF issued a first report about virtual currencies in 2014.[13] The importance of the report is further enhanced by the fact that it examines the risks associated with crypto-currencies, provides a common definitional vocabulary (virtual currency, digital currency) and classifies the types of virtual currency (convertible/open and non-convertible/closed virtual currency, centralised and non-centralised virtual currency, etc.).[14]

The next step was in June 2015, with the establishment of the "Guidance for a Risk-Based Approach to Virtual Currencies"[15] In October 2018, the FATF Plenary discussed and adopted amendments to the FATF Standards to respond to the increasing use of virtual assets for money laundering and terrorist financing. In 2019, FATF extended the AML/CFT measures to VAs and VASPs to prevent criminal and terrorist misuse of the sector. In 2019, the "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)" was adopted, in order to help the national authorities, supervisory, private sector entities understand their AML/CFT actions and obligations. The VASPs have the same obligations as financial institution (especially KYC).[16] The money laundering offence should extend:

[13] FATF Report Virtual Currencies – Key Definitions and Potential Anti-money Laundering and Counter-terrorist Financing Risks, June 2014, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html (accessed on: 02.08.2023).

[14] See more about the definition in the chapter "New developments and challenges of the fight against money laundering by the cybercrime – methods and risks".

[15] FATF Guidance for a risk-based approach Virtual currencies, June 2015, https://www.fatf-gafi.org/en/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html (accessed on: 06.06.2023).

[16] R. Brandl, J. Bülte, *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung – Perspektive Sorgfaltsverpflichtete*, [in:] R. Leitner, R. Brandl (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Linde Verlag, Vienna 2023, pp. 113–114.

> to any type of property, regardless of its value, that directly represents the proceeds of crime, including in the context of VAs. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence, including in the case of VA-related proceeds. Countries should therefore extend their applicable ML offence measures to proceeds of crime involving VAs.

The same comprehensive approach is applied by the confiscation and provisional measures.

In July 2021, the FATF adopted the report "Opportunities and Challenges of New Technologies for AML/CFT".[17] In October 2021, the "Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Providers" was updated. In June 2023, the "Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs" was adopted.[18] Based on this, we present the following relevant recommendations.

4.2.2. FATF RECOMMENDATION NO. 15 AND FATF RECOMMENDATION NO. 16 (TRAVEL RULE)

The Recommendation No. 15 (Jurisdictions' Implementation of FATF Standards on VAs/VASPs) recognise the dangers associated with new technologies and states that:

> countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including

[17] FATF Opportunities and Challenges of new technologies for AML/CFT, July 2021, https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html (accessed on: 06.06.2023).

[18] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html (accessed on: 03.08.2023).

> new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.

They should take appropriate measures to manage and mitigate those risks in order:

> to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.[19]

The so-called "travel rule" is one of the key AML/CFT measures to combat cyber-laundering. In accordance with the wire transfer requirements, "Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain."[20] The travel rule applies in the VA context. The travel rule requires VASPs and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when transferring VAs. Law enforcement authorities regard the travel rule as very important for the detection, investigation and prosecution of tmoney laundering, and helpful for financial intelligence units to analyse reports of suspected money laundering.[21]

In accordance with the latest report of the FATF in June 2023, the global implementation of Recommendation No. 15 is relatively poor; 75% of jurisdictions assessed against the revised standards are only partially or non-compliant with FATF's requirements

[19] FATF Recommendation No. 15

[20] FATF Recommendation No. 16

[21] FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, Paris 2023, p. 16, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html (accessed on: 03.08.2023).

in this matter.[22] However, the European Union legislator took an important step to protect this sector, and a regulatory framework for VASPs and the travel rule was established.

In summary, it can be concluded that the FATF has responded to the challenges posed by new technologies with phased approach. We can see that it took decisive steps against cyber-laundering with the framework of the preventive measures and laid down global standards in this area as well. In the next point we will research development and regulatory framework of the European Union, which is in line with the FATF's expectations.

4.3. Development of the AML Regulation in the European Union

Money laundering is a major threat to the global financial system and to economies generally, but it is a significant problem at the EU level too, because it damages the integrity, stability and reputation of the financial sector and the internal market and the internal security of the Union.[23] The legislator of the European Union is strongly committed to the fight against money laundering and terrorist financing.

4.3.1. MAIN CHARACTERISTICS OF THE AML REGULATION FRAMEWORK IN THE EU

The most important EU legal acts in connection with the money laundering are found in directive-level rules, which the member states must implement into their own national legal systems. The European Union's anti-money laundering policy can be said to

[22] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html (accessed on: 06.06.2023); FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, Paris 2023, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html (accessed on: 03.08.2023).

[23] Preamble 8 Art. 1 Directive (EU) 2015/849.

be based on two pillars: non-criminal (preventive/administrative) and criminal measures. Measures relating to money laundering compliance can essentially be included among the preventive instruments. The initial sectoral regulation, which imposed obligations only on financial and credit institutions, has now been replaced by a comprehensive concept that entails obligations for almost all economic operators.

There are five AML Directives which regulate the preventive instruments against money laundering:

- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering[24] (I. AML Directive);
- Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering – Commission Declaration[25] (II. AML Directive);
- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[26] (III. AML Directive);
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC[27] (IV. AML Directive);
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system

[24] OJ EU L 166, 28.6.1991, pp. 77–82.
[25] OJ EU L 344, 28.12.2001, pp. 76–82.
[26] OJ EU L 309, 25.11.2005, pp. 15–36.
[27] OJ EU L 141, 5.6.2015, pp. 73–117.

> for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU[28] (V. AML Directive).

Their primary objective is to prevent the financial sector from being used for purposes of money laundering by requiring customer due diligence obligation and reporting obligation.[29] It is important to underline that the EU legislator took into account the FATF's Recommendations for all directives.

In addition, it is also necessary to mention the "Regulation on Transfers of Funds"[30] which serves to comply with the mentioned above FATF Recommendations No. 16. The regulation establishes requirements for financial institutions (banks, payment service providers, e-money issuers, etc.) to include specific information along with electronic money transfers or wire transfers, in order to help prevent, detect and investigate money laundering and terrorist financing.

In line with the FATF's Recommendation, the European Union's regulation uses a risk-based approach, which is implemented on the basis of multi-level regulations. This approach was described by the III. AML Directive, based on the provision of:

> Member States require that institutions and persons covered by this policy shall establish appropriate policies and procedures for customer due diligence, reporting, registration, internal control, risk assessment, risk management,

---

[28] OJ EU L 156, 19.6.2018, pp. 43–74.

[29] See in detail: B. Udvarhelyi, *Pénzmosás elleni küzdelem az Európai Unióban.* [in:] I. Stipta (ed.), *Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai*, Tomus 12., Miskolc 2013, pp. 456–464, 467–469; A. Met-Domestici, *The Reform of the Fight against Money Laundering in the EU*, "Eucrim" 2013, No. 3, pp. 170–179; D. Langlois, *The Revision of the EU Framework on the Prevention of Money Laundering*, "Eucrim" 2013, No. 3, pp. 96–98; A. Met-Domestici, *The Fight against Money Laundering in the EU – The Framework Set by the Fourth Directive and its Proposed Enhancements*, "Eucrim" 2016, No. 4, pp. 170–179.

[30] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006 (OJ EU L 141, 5.6.2015), pp. 1–18.

> compliance management and communication to prevent operations related to money laundering or terrorist financing.[31]

Detecting relevant risks, especially in relation to cyber security and criminal activities, can be quite a challenge for the private sector burdened with the obligation.[32] There are supranational and national risk assessment, sector-specific guidelines for supervisory bodies, and the internal rules of the service provider concerned, including risk-based internal procedures.[33] The implement of the supranational approach to risk identification is the task of the European Union in accordance with the IV. AML Directive.[34] The first Supranational Risk Assessment (SNRA) was adopted in 2017.[35] The aim of the report is to identify, analyse and evaluate the ML and TF risks at Union level. At this time the Commission set up the FinTech[36] Working Group to investigate the dangers of technological development, technology-enabled services and business models (e.g., digital currencies) in order to asset the dangers associated with them. In 2022, the European Commission adopted the third "Supranational Risk Assessment Report" of the risk of money laundering and terrorist financing affecting the internal market and in relation to cross-border activities.[37] The national legal framework will always depend on the development and ecosystem of the country

[31] Art. 35(1) III. AML Directive.

[32] B. Vogel, *Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing*, "Eucrim" 2022, No. 1, pp. 52–60.

[33] Zs. Papp (ed.), *Magyarázat a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról*, Budapest 2019, pp. 134–147.

[34] Art. 6(1) IV. AML Directive.

[35] COM (2017) 340 final.

[36] FinTech refers to technology-enabled and technology-supported financial services. Technology has the potential to facilitate access to financial services and to make the financial system more efficient "Reg Tech" is about adopting new technologies to facilitate the delivery of regulatory requirements.' See the definition in the first SNRA in 2017, COM (2017) 340 final, p. 9.

[37] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM (2022) 554 final, Brussels, 27 October 2022.

concerned. Therefore, countries have to take different approaches in the national risk assessment (NRA), a "one size fits all" solution to assessing money laundering – including cyber-laundering risks – is not feasible.[38]

4.3.2. REQUIREMENT TO REPORT SUSPICIOUS TRANSACTIONS AND THE ROLE OF THE FINANCIAL INTELLIGENCE UNIT (FIU)

The "risk-based approach" to combat money laundering was introduced with the 3rd AML Directive to replace the rules-based approach.[39] In accordance with the new approach, the current trends and typologies of money laundering must be taken into account.

Of central importance among the obligations imposed on actors in the financial and economic spheres is the reporting obligation with which service providers bring valuable information to the attention of the authority operating as a financial intelligence unit (Financial Intelligence Unit, FIU[40]). The reporting obligations means the information of the FIU, including the filing of a report on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases;

[38] See World Bank Group: National Money Laundering and Terrorist Financing Risk Assessment Toolkit, 2022, https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use (accessed on: 13.07.2023). See the FATF National ML/TF risk assessment: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html (accessed on: 13.07.2023).

[39] J. Grzywot, *Virtuelle…*, *op. cit.*, p. 93.

[40] In Hungary is the FIU a department of the National Tax and Customs Administration of Hungary (NTCA), delegated by the relevant legislation. See: https://pei.nav.gov.hu/ (accessed on: 2.08.2023). See: G. Simonka, *A magyar FIU és a pénzmosás elleni intézményrendszer a nemzetközi együttműködés tükrében*, Budapest 2015.

and providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.[41] It is important to underlined that all suspicious transactions, including attempted transactions, shall be reported, regardless of the amount.

The main role of national FIU in the preventive combatting of money laundering must be highlighted. The 1st AML Directive in 1991 only required that credit and financial institutions should cooperate with "the authorities responsible for combating money laundering". This term was used as a generic term, but the Directive didn't contain detailed rules for financial information units. Under an explicit provision of the III. AML Directive in 2005, each Member State is required to establish an FIU in order to combat money laundering and terrorist financing effectively.[42] In accordance with the IV. AML Directive from 2015, each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing.[43] The FIU shall be a central national unit that shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. Each FIU shall be operationally independent and autonomous. It shall be able to obtain additional information from obliged entities. The competent authorities have to provide feedback to the FIU about the use made of the information provided. The Member States shall ensure that their FIUs have access to the financial, administrative and law enforcement information that they require to fulfil their tasks properly. Where there is a suspicion that a transaction is related to money laundering or terrorist financing, the FIU has to

[41] Art. 33 IV. AML Directive.

[42] Art. 21 III. AML Directive.

[43] Art. 32 IV. AML Directive. There are three basic types of financial information units: administrative, investigative or judicial. The FIU could be a hybrid institution too if the characteristics of the three basic types of FIU appear in a somewhat mixed way. See about more: G.A. Simonka: *A pénzügyi információs egység*, [in:] Zs. Papp (ed.), *Magyarázat a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról,* Közigazgatási és Jogi Kiadványok, Budapest 2019, p. 175.

be empowered to take urgent action to suspend or withhold consent to a transaction in order to analyse the transaction and disseminate the results of the analysis to the competent authorities. The FIU can take such action, at the request of an FIU from another Member State. The very important legal background in accordance with the cooperation between the authorities is Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.

4.3.3. THE FIGHT AGAINST MONEY LAUNDERING BY CRIMINAL LAW

As mentioned above the AML measures of the European Union can be divided into two main categories, The other instrument system concerns criminal law. Nowadays, the penal codes of all EU member states regulate the crime of money laundering. It was codified from the beginning of the 1990s, although the EU regulations only required the prohibition of money laundering. The reason for this was the lack of criminal law competence of the European Communities (European Union).[44] The criminalisation obligation came into force only with the issuance of the 6th AML Directive.[45] The provisions of 6th AML Directive complement and reinforce the existing preventive measures. The aim is to enable more efficient and swifter cross-border cooperation between competent authorities.[46] It must be mentioned that the EU legislator recognised the importance

[44] See B. Udvarhelyi, *Az Európai Unió anyagi büntetőjog a Lisszaboni Szerződés után*, Budapest 2019, pp. 97–133; B. Udvarhelyi, *Kézikönyv az Európai Unió pénzügyi érdekeinek védelméről*, Budapest 2022, p. 63; B. Udvarhelyi, *Criminal law competences of the European Union before and after the Treaty of Lisbon*, "European Integration Studies" 2015, Vol. 11, No. 1, pp. 46–59.

[45] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (OJ EU L 284, 12.11.2018), pp. 22–30.

[46] Preamble 1, VI. AML Directive.

of action against cybercrime and therefore identified cybercrime among the list of predicate offences.[47]

The 6th AML Directive contains the repressive measures for combating money laundering and lays down minimum standards for criminal offenses and sanctions.[48] The Directive, which establishes minimum rules for the member states regarding the crime and the legal consequences of money laundering, was a milestone of outstanding importance on the EU scene of the fight against money laundering. This legislative act aims to combat money laundering through criminal law and to facilitate cross-border cooperation between competent authorities and complement the preventive measures regulated in IV. AML/CTF Directive (EU) 2015/849 in force.[49]

4.4. New Developments in the European Union

4.4.1. ACTION PLAN OF THE EUROPEAN COMMISSION 2020 AND LEGISLATIVE PACKAGE 2021

It must be highlighted that the EU's anti-money laundering framework began to develop dynamically following the adoption in 2020 of the "Action Plan for a comprehensive Union policy on preventing

[47] Cybercrime including any offence set out in Directive 2013/40/EU of the European Parliament and of the Council. See the definition of "criminal activity": Art. 2(1) VI AML Directive. It must be mentioned that it was the only crime which is not listed in the categories of offences in the 40 Recommendations of the FATF and the Warsaw Convention of the Council of Europe.

[48] Art. 1(1) VI. AML Directive.

[49] See: J. Jacsó, *Gondolatok az Európai Unió pénzmosás elleni büntetőpolitikájáról a hatodik Pénzmosás elleni uniós irányelv tükrében*, [in:] P. Bárd, A. Borbíró, K. Gönczöl (eds.), *Kriminológia és kriminálpolitika a jogállam szolgálatában. Tanulmányok Lévay Miklós tiszteletére*, Budapest 2019, pp. 401–411; J. Jacsó, B. Udvarhelyi, *The fight against money laundering in Hungary*, [in:] Á. Farkas, G. Dannecker, J. Jacsó (ed.), *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 295–309.

money laundering and terrorism financing".[50] The action plan builds on six pillars, which primarily cover preventive measures, but also affect criminal law.

On 20 July 2021, the Commission presented a package consisting of four legislative proposals to strengthen the EU AML/CFT provisions, as follow:

- AMLA Regulation: Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism;[51]
- New Regulation on AML/CFT: Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;[52]
- New Directive on AML/CFT: Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.[53] It is important

[50] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06, C/2020/2800 (OJ C 164, 13.5.2020), pp. 21–33.

[51] Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No. 1093/2010, (EU) 1094/2010, (EU) 1095/2010, COM (2021) 421 final, Brussels, 20 July 2021. See more about the AMLA: J. Jacsó, *New developments in the fight against money laundering, in particular the Commission's 2021 proposal with special regard to the Anti-money laundering Authority (AMLA)*, [in:] Á. Farkas, G. Dannecker, J. Jacsó (ed.), *External, internal and criminal investigations of criminal offences affecting the financial interests of the European Union,* Budapest 2022, pp. 467–481.

[52] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM (2021) 420 final, Brussels, 20 July 2021.

[53] Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM (2021) 423 final, Brussels, 20 July 2021.

to emphasise that the Directive will replace the 4th AML Directive 2015/849/EU. The new Directive will contain a provision that requires national implementation contrary to the rules in the new *Regulation on AML/CFT* (for example, rules on national supervisions and Financial Intelligence Units of the Member State);

- Reform of the Regulation on Transfers of Funds (Regulation 2015/847):[54] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets (recast).[55] This proposal was the first to be adopted by the EU legislator in 2023.

4.4.2. AMENDMENTS OF THE IV. AML DIRECTIVE TO PREVENT CYBER-LAUNDERING

The EU legislator recognised that it is important to ensure that Union legislative acts on financial services comply with the digital age. The first definition of virtual currency on the level of the EU was established by the 5th AML Directive in 2018. Before the amendment of the 4th AML Directive, providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers, which didn't fall under the Union's obligation to identify suspicious activity. Therefore, criminals were able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. Therefore, it became necessary to extend the scope of the 4th AML Directive so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet

[54] IV. AML Directive.

[55] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) COM (2021) 422 final, Brussels, 20 July 2021.

providers.[56] However, the EU legislator was also aware that "a large part of the virtual currency environment will remain anonymous because users can also transact without such providers".[57] "Virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. We can see that the EU legislator refrained from using the term "crypto" and used the term "virtual currency".

The latest development in the recent past was the amendment of the IV. AML Directive by the Regulation Transfer of Funds (TFR[58]), which extended the scope of the directive to crypto-asset service providers. With this amendment, the EU legislator complies with the FATF Travel Rule (Recommendation No. 15). In addition, in 2023, the European Union adopted for the first time a harmonised regulatory framework for the crypto-asset market (Regulation (EU) 2023/1114 on Markets in Crypto-Assets, (MiCA[59]). The aim of MiCA is the establishment of uniform rules for issuers of crypto-assets that have not been regulated before by other European Union financial services acts[60] and for providers of services in relation to such crypto-assets (crypto-asset service providers).[61] These service

[56] Preamble 8, V. AML Directive.

[57] Preamble 9, V. AML Directive.

[58] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ EU L 150, 9.6.2023, pp. 1–39. (TRF Regulation).

[59] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ EU L 150, 9.6.2023), pp. 40–205 (hereinafter: MiCA Regulation).

[60] One group of crypto assets was classified as a financial institution and was regulated before, see: Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ 173, 12.6.2014), p. 349.

[61] See: summarised about the main regulations of MiCA, https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html (accessed on: 03.06.2023).

providers must comply with a number of obligations. The scope of MiCA "applies to natural and legal persons and certain other undertakings that are engaged in the issuance, offer to the public, and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union."[62] Crypto-assets are one of the main applications of distributed ledger technology (DLT). In accordance with the provision of MiCA, "crypto-asset" means a "digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".[63] It must be underlined that the MiCA regulation applies to any new player in the crypto-ecosystem involved in the issuance.[64]

4.5. Summary and Conclusion

The scope of legal framework of the EU became wider and wider, the latest legal documents even cover the crypto asset service providers and crypto assets. The EU legislator used the term crypto whereas the FATF recommends the term "virtual", but they are synonymous. With the new EU legal framework, every cryptocurrency-related business has to adhere to the same AML/CFT rules as other financial service providers. The traditional strategy to "follow the money" could be changed in the digital age to "follow the virtual asset", which could be a rule of thumb in the effort to combat the new form of money laundering – cyber-laundering.

The cross-border nature of money laundering and cyber-laundering is a significant factor that makes it difficult to combat these crimes and to identify the perpetrators. In the fight against money laundering, the cooperation of several institutions is very important at the national as well as the international level. The proper

[62] Art. 2(1) MiCA Regulation.
[63] Art. 3(1) pt 5 Regulation (EU) 2023/1114.
[64] See: https://www.cssf.lu/en/2023/07/regulation-on-markets-in-crypto-assets-mica-and-regulation-on-information-accompanying-transfers-of-fund-and-certain-crypto-assets/ (accessed on: 03.08.2023).

application of preventive measures in practice can make a major contribution to the investigation and prosecution of money laundering cases. It requires the use of diverse tools of international cooperation and tools to secure and transfer data without delay. The fight against money laundering is characterised by the so-called multi-institutional approach, which could be employed in the fight against cybercrime generally. It is very important to point out that preventive measures are of particular importance in the fight against cyber-laundering, and crypto assets providers could as well play a decisive role.

This proposal package of the European Commission has been an important step in the field of harmonisation of anti-money laundering framework in the EU. With the adoption of the new AML/CFT rulebook, the EU regulatory and enforcement framework will be more uniform. The legal framework of harmonised and comprehensive anti-cyber laundering measures are an indispensable tool for combating cybercrime, in which preventive tools are of decisive importance. However, it is crucial that all actors in the fight against cyber-laundering have sufficient expertise, for which appropriate training is essential.[65]

REFERENCES

Brandl, R., Bülte, J., *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung –Perspektive Sorgfaltsverpflichtete*, [in:] Leitner, R., Brandl, R. (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Vienna 2023, pp. 105–122.

Bussmann, K.-D., Vockrodt, M., *Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie*, "Compliance Berater" 2016, No. 5.

Farkas, Á., Dannecker, G., Jacsó, J., *Conclusion and recommendation of the project*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (eds.), *External, internal and criminal investigations of criminal*

[65] Á Farkas, G. Dannecker, J. Jacsó, *Conclusion and recommendation of the project*, [in:] Á. Farkas, G. Dannecker, J. Jacsó (ed), *External…*, *op. cit.*, p. 498.

offences affecting the financial interests of the European Union, Budapest 2022, pp. 490–502.

Grzywot, J., *Virtuelle Kryptowährungen und Geldwäsche*, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2019.

Jacsó, J., *A pénzmosás*, [in:] Farkas, Á. (ed.), *Fejezetek az európai büntetőjogból*, Miskolc 2017.

Jacsó, J., *Gondolatok az Európai Unió pénzmosás elleni büntetőpolitikájáról a hatodik Pénzmosás elleni uniós irányelv tükrében*, [in:] Bárd, P., Borbíró, A., Gönczöl, K. (eds.), *Kriminológia és kriminálpolitika a jogállam szolgálatában. Tanulmányok Lévay Miklós tiszteletére*, Budapest 2019, pp. 401–411.

Jacsó, J., *New developments in the fight against money laundering, in particular the Commission's 2021 proposal WITH special regard to the Anti-money laundering Authority (AMLA)*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (ed.), *External, internal and criminal investigations of criminal offences affecting the financial interests of the European Union*, Budapest 2022, pp. 467–481.

Jacsó, J., Udvarhelyi, B., *A Bizottság új irányelvjavaslata a pénzmosás elleni büntetőjogi fellépésről az egyes tagállami szabályozások tükrében*, "Miskolci Jogi Szemle" 2017, No. 2, pp. 43–44.

Jacsó, J., Udvarhelyi, B., *The fight against money laundering in Hungary*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (eds.), *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 295–309.

Langlois, D., *The Revision of the EU Framework on the Prevention of Money Laundering*, "Eucrim" 2013, No. 3.

Leslie, D.A., *Legal Principles for Combatting Cyberlaundering*, New York 2014.

Mauma, Ph., Maute, L., Fromberger, M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020.

Met-Domestici, A., *The Fight against Money Laundering in the EU – The Framework Set by the Fourth Directive and its Proposed Enhancements*, "Eucrim" 2016, No. 4.

Met-Domestici, A., *The Reform of the Fight against Money Laundering in the EU*, "Eucrim" 2013, No. 3.

Papp, Zs. (ed.), *Magyarázat a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról*, Budapest 2019.

Rückert, Ch., *Phänomenologie*, [in:] Mauma, Ph., Maute, L., Fromberger, M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020, pp. 527–536.

Simonka, G., *A magyar FIU és a pénzmosás elleni intézményrendszer a nemzetközi együttműködés tükrében*, Budapest 2015.

Udvarhelyi, B., *Az Európai Unió anyagi büntetőjog a Lisszaboni Szerződés után*, Budapest 2019.

Udvarhelyi, B., *Criminal law competences of the European Union before and after the Treaty of Lisbon*, "European Integration Studies" 2015, Vol. 11, No. 1, pp. 46–59.

Udvarhelyi, B., *Kézikönyv az Európai Unió pénzügyi érdekeinek védelméről*, Budapest 2022.

Udvarhelyi, B., *Pénzmosás elleni küzdelem az Európai Unióban*, [in:] *Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai*, Tomus 12., Gazdász-Elasztik Kft., Miskolc 2013, pp. 455–471.

Vogel, B., *Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing*, "Eucrim" 2022, No. 1, pp. 52–60.

Zéman, Z., Hegedűs, M., *Pénzmosás mint negatív gazdasági tényező az Európai Unióban*, "Belügyi Szemle" 2023, No. 5, pp. 885–904.

DR. FERENC SÁNTHA, EGYETEMI DOCENS
University of Miskolc | DOI: 10.32041/9788367149761/5

Chapter 5. Problems of Jurisdiction in Cybercrimes Cases

5.1. Introduction

Until the mid-20th century, crime was largely a local matter. The principles governing the exercise of criminal jurisdiction were based on the axiom that a crime was a phenomenon tied to a specific geographic area.[1] Consequently, the dominant principle among the grounds of jurisdiction was the application of the territorial principle, since it was obvious that jurisdiction should be exercised by the State in whose territory the offence was committed. However, even before the appearance of cybercrimes, there was an increasing number of criminal offences which, due to the place of commission, the nationality of the perpetrator or the nature of the act, violated or threatened the legal order of two or more states at the same time.[2] Cybercrime has multiplied this trend and has fundamentally changed the nature of crime, making it transnational and borderless.[3] The development of cyberspace and info-communication is an important dimension of the dynamic changes of the 21st century.[4] In this context, cyberspace almost epitomises the phenomenon

[1] D. Tóth, Zs. Gáspár, *Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés terén*, "Belügyi Szemle" 2020, No. 2, p. 140.

[2] P.M. Nyitrai, *Nemzetközi és európai büntetőjog*, Budapest 2006, p. 207.

[3] D. Tóth, Zs. Gáspár, *Nemzetközi…*, *op. cit*., p. 140.

[4] Á.Farkas, *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapjai*, "Jog-Állam-Politika" 2019, No. 2, p. 63.

of deterritorialisation, as it allows for the rapid transfer of digital data between users and devices around the world.[5] Deterritorialisation, as the globalisation of social processes and the move away from individual and isolated locations, is a major challenge for the current jurisdictional system, which is still based on the primacy of the territorial principle.[6] The communication space of the web operates on the principle of non-locality. The communication universe is a linguistic, social and political space to which the jurisdiction and sovereignty of individual states cannot easily be extended. States, however, do not want to accept the restriction or even the erosion of their territorial jurisdiction and sovereignty in cyberspace, and therefore try to prevent it in various ways.[7] Since the countries exercising criminal jurisdiction coexist, the permeability of borders, which is also a feature of criminality, raises jurisdictional problems.[8]

In this paper, I define the concept of jurisdiction and then analyse the principles underlying criminal jurisdiction in the first and in the second chapter. In doing so, I draw on the legal literature, the rules of the Budapest Convention,[9] and the provisions of the Hungarian Criminal Code (HCC) and Polish Criminal Code (PCC) on jurisdiction. The latter aspect is also important because one of the questions to be answered is: In which cases do the HCC and the PCC apply to the commission of a cybercrime? The third chapter is devoted to jurisdictional conflicts, and finally I outline three hypothetical practical cases in which jurisdictional problems and institutions of international cooperation in criminal matters

[5] C. Ryngaert, *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, "German Law Journal" 2023, Vol. 24, Issue 4, p. 537.

[6] D.B. Jakab, *Területiség és deterritorializáció. A terület mint a társadalomelmélet vezérfonala*, "Replika" 2009, No. 5, p. 164.

[7] L. Fekete, *Szabadság, jog és szabályozás a kibertérben*, "Replika" 2001, No. 9, p. 219. Clough also notes that "early scholarship postulated cyberspace as a distinct place, beyond traditional rules based on geographical location." However, states do not share this view, and consistently apply the principle of territoriality to cybercrime and refuse to treat the Internet as an area outside their jurisdiction. J. Clough, *Principles of cybercrime*, Cambridge 2010, p. 405.

[8] L.A. Wiener, *A büntető joghatóság és gyakorlása, kivált az Európai Unióban*, "Állam és Jogtudomány" 2002, No. 3–4, p. 177.

[9] The Council of Europe's Convention on Cybercrime, Budapest, 23 November 2001.

can be analysed. The aim of my research is to confirm or refute a hypothesis I have put forward, which is the following: Traditional jurisdictional principles in domestic and international criminal law are not able to respond to the challenges posed by cybercrime, in particular positive jurisdictional conflicts.

5.2. The Concept of Jurisdiction

Jurisdiction, in the most general sense, is the set of rules that make the law a functioning, accessible body of law, and the most important prerequisite for its application.[10] One aspect of the concept, criminal jurisdiction, refers to the right of the state to legislate and enforce criminal law. In a narrower sense, it has a twofold meaning: firstly, the applicability of the rules of national criminal law and, secondly, the scope of the authorities' competence in criminal matters.[11]

The three-level understanding of the concept of jurisdiction is an indispensable issue in the international and especially in the Anglo-Saxon literature, and this paper also refers to it. According to this concept, jurisdiction is the basis for the future exercise of the state's criminal claim (*jurisdiction to prescribe* or *legislative jurisdiction*), which means the state's power to regulate human behaviour: to require the exercise of certain conduct or, as is typical in criminal law, to prohibit certain acts. Another meaning of jurisdiction is the *jurisdiction to enforce*, which is the actual exercise of existing jurisdiction: the ability of a State to validly enforce its law through the exercise of executive and judicial power. Finally, the third level of interpretation of jurisdiction is the *jurisdiction to adjudicate*, which means the power of a state to try a criminal case and to determine whether the accused person has committed a crime.[12]

---

[10] Jurisdiction is essentially a term of international law that refers to the right of a state to make and enforce its law and to exercise justice. P.M. Nyitrai, *Nemzetközi és…*, *op. cit*., p. 208.

[11] P.M. Nyitrai, *Nemzetközi és…*, *op. cit*., p. 209.

[12] See in detail: S.W. Brenner, B.-J. Koops, *Approaches to Cybercrime Jurisdiction*, "Journal of High Technology Law" 2004, Vol. 4, No. 1, pp. 5–6; D. Tóth, Zs. Gáspár, *Nemzetközi…*, *op. cit*., p. 141.

Although several international legal instruments, including the Budapest Convention, contain provisions on jurisdiction, it is not a purely international legal category: the rules of jurisdiction and their content are given substance by domestic criminal law provisions. As a concept of domestic criminal law, *scope* defines the different aspects of the application of the criminal law of a given State (temporal, territorial and or personal scope). Therefore, in this paper, the concept of jurisdiction is used in the following sense: *jurisdiction means the power of the state to make and apply the rules of criminal law. The provisions on jurisdiction regulate when, where and to whom the criminal law (the Criminal Code) is to be applied when adjudicating a criminal offence.* Provisions on criminal jurisdiction can be found in the General Part of the Criminal Code in most countries – including Hungarian and Polish criminal law. The principles underlying criminal jurisdiction have been developed by jurisprudence, but these principles are always reflected in the provisions of the Criminal Code on jurisdiction.

5.3. The Principles of Jurisdiction

States traditionally base criminal jurisdiction on five aspects: territoriality, the active and passive aspects of citizenship (active and passive personality principle), state self-defence and the principle of universality.[13]

1. *The territoriality principle* is the most common basis for the exercise of criminal jurisdiction, according to which the criminal law of a State applies to all offences committed on its territory, irrespective of the nationality of the perpetrator. The Budapest Convention regulates the territoriality principle in the first place[14] and, unlike the other grounds

[13] P.M. Nyitrai, *Nemzetközi és…*, *op. cit.*, p. 213.

[14] See Art. 22(1) of the BC: "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established under Articles 2 through 11 of this Convention, when the offence is committed: a) in its territory (…)".

of jurisdiction, its adoption and application in domestic law is binding on the States Parties.[15] The territoriality principle is also included in the Hungarian Criminal Code (HCC)[16] and in the Polish Criminal Code (PCC).[17] According to this rules, HCC applies in the case of cybercrime committed on the territory of Hungary and the PCC if the crime is committed on Polish territory. Here I mention the *quasi-territorial principle*, which extends the concept of domestic territory to offences committed on board a ship or registered aircraft flying the flag of a given country. The quasi-territoriality principle is included in the Budapest Convention[18] as well as in the HCC[19] and PCC.[20]

2. The second most frequent basis of jurisdiction is the *personality principle* (nationality principle or *active personality principle*), according to which the jurisdiction of the state extends to the offence committed by its citizen abroad. The active personality principle is also regulated both by the Budapest Convention and by the HCC and the PCC.

---

[15] See Art. 22(2) of the BC: "Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down paragraphs 1 b) through 1 d) of this article or any part thereof."

[16] See Art. 3(1) of the HCC: "Hungarian criminal law shall apply: a) to criminal offenses committed in Hungary (…)".

[17] See Art. 5 of the PCC: "Polish criminal law shall be applied to the perpetrator who committed a prohibited act within the territory of the Republic of Poland (…)".

[18] See Art. 22(1)(b)(c) of the BC: "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established under Articles 2 through 11 of this Convention, when the offence is committed: (…) (b) on board a ship flying the flag of that Party; or (c) on board an aircraft registered under the laws of that Party".

[19] See Art. 3(1) of the HCC: "(1) Hungarian criminal law shall apply: (…) (b) to criminal offenses committed on commercial ships or watercraft sailing, or aircraft flying under Hungarian flag outside the territory of Hungary."

[20] See Art. 5 of the PCC: "Polish criminal law shall be applied to the perpetrator who committed a prohibited act (…) on a Polish vessel or aircraft, unless an international agreement to which the Republic of Poland is a party stipulates otherwise."

It is important to note that, according to the Convention[21] and the PCC,[22] a further condition for the application of the principle is that the act is also considered a criminal offence and punishable under the law of the place where it is committed. This is called the *double incrimination requirement* or the principle of *double criminality*. In contrast, the active personality principle plays a much broader role in Hungarian criminal law: the additional condition is not that the act should be a criminal offence under the law of the place of the commission, but only that it should be a criminal offence under the Hungarian Criminal Code.[23] Here I mention that whereas the Convention does not, the Hungarian[24] and Polish Criminal Codes[25] do also regulate the *passive personality principle*, which is also one of the grounds for extraterritorial jurisdiction. The principle protects the state's own citizen (or its own legal person or other organisation) in the event of an offence committed abroad by a foreigner.[26]

[21] See Art. 22(1)(d) of the BC: "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established under Articles 2 through 11 of this Convention, when the offence is committed: (…) (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."

[22] See Art. 109 of the PCC: "Polish criminal law shall be applied to Polish citizens who have committed an offence abroad". See also the Art. 111 § (1): "The liability for an act committed abroad is, however, subject to the condition that the liability for such an act is likewise recognised as an offence, by a law in force in the place of its commission."

[23] See Art. 3(1) of the HCC: "Hungarian criminal law shall apply: (…) (c) to any act of Hungarian citizens committed abroad, which is punishable by Hungarian law."

[24] See Art. 3(2)(d) of the HCC: "Hungarian criminal law shall apply: (…) (b) to any act committed by non-Hungarian citizens abroad against a Hungarian national or against a legal person or unincorporated business association established under Hungarian law, which is punishable under Hungarian law."

[25] See Art. 110(1) of the PCC: "Polish criminal law shall be applied to foreigners who have committed abroad an offence against the interests of the Republic of Poland, a Polish citizen, a Polish legal person or a Polish organisational unit not having the status of a legal person".

[26] T. Horváth, M. Lévay, *Magyar büntetőjog általános rész*, Budapest 2014, p. 102.

The following jurisdictional principles already apply in cases where the offence is committed *abroad* by a person who is *not a national* of the State (foreign national or stateless person). It should be noted that the Convention does not contain such principles but allows States Parties to regulate and apply them.[27]

3. Under the *principle of state self-defence* or the *protective principle,* a State has jurisdiction to criminalise extra-territorial conduct, regardless of the nationality of the offender, where that conduct is against the fundamental interest of the state, for example crimes against the security, territorial integrity or political independence of the state. The protective principle is included in both the PCC[28] and the HCC.[29] It should be noted that in Polish criminal law, the double incrimination requirement is not necessary in this case and the scope of the relevant offences is quite broad. Double incrimination is not a precondition in Hungarian criminal law either, but the relevant criminal offences are narrower, namely the offences against the state regulated by the Criminal Code. Based on this provision, a cyber-attack launched against Hungary from abroad with the aim of obtaining data that can be used to the detriment of the country ("conducting intelligence activities" against Hungary) may

[27] According to the Art. 22(4) of the BC: "This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law."

[28] See Art. 112 of the PCC: "Regardless of the provisions in force in the place of the commission of the offence, Polish criminal law shall be applied to a Polish national, or to a foreigner in case of the commission of:
1) an offence against the internal or external security of the Republic of Poland,
2) an offence against Polish offices or public officials,
3) an offence against essential economic interests of Poland,
4) an offence of false deposition made before a Polish office,
5) from which a material benefit was gained, even if indirectly, in the Republic of Poland".

[29] See Art. 3(2)(b) of the HCC: "Hungarian criminal law shall apply (a) to any act committed by non-Hungarian citizens abroad, if it is recognized as an offense against the State (…) regardless of whether or not it is punishable in accordance with the law of the country where committed."

constitute the crime of espionage (Art. 261 of the HCC), in which case the Hungarian Criminal Code applies.

4. The *principle of universality* requires a State to prosecute certain crimes, regardless of the place it was committed or the nationality of the perpetrator. These are typically the so-called crimes under international law (genocide, crimes against humanity, war crimes and crime of aggression) and the so-called transnational crimes, namely crimes punishable under an international treaty. Both the HCC[30] and the PCC[31] regulate the principle of universality, and it is important that double incrimination is not a condition here, either.
5. Until now, Polish and Hungarian rules on criminal jurisdiction have been very similar, but there is a difference about *offences committed abroad by foreigners*. In addition to the cases mentioned above, the Polish legislator provides for the application of the PCC for offences punishable by imprisonment for more than 2 years if the perpetrator is in Poland, and for terrorist offences.[32] The HCC also contains an additional provision on the offence committed by a non-Hungarian citizen abroad. Under *the representational principle* (the vicarious administration of justice), it is possible to prosecute and hold liable a non-Hungarian perpetrator

[30] See Art. 3(2)(b) of the HCC: "Hungarian criminal law shall apply (a) to any act committed by non-Hungarian citizens abroad, if it constitutes a criminal act under Chapter XIII or XIV (crimes against humanity and war crimes), or any other criminal offenses which are to be prosecuted under an international treaty ratified by an act of Parliament."

[31] See Art. 113 of the PCC: "Regardless of regulations in force in the place of commission of the offence, Polish criminal law shall be applied to a Polish national, or to a foreigner, concerning to whom no decision on extradition has been taken, in the case of the commission abroad of an offence which the Republic of Poland is obligated to prosecute under international agreements, or in case of offences prescribed in the Rome Statute of the ICC."

[32] See Art. 110(2)(3) of the PCC: "1. Polish criminal law shall be applied to foreigners in the case of the commission abroad of an offence other than listed in § 1, if, 2. under Polish criminal law, such an offence is subject to a penalty exceeding 2 years of deprivation of liberty, and the perpetrator remains within the territory of the Republic of Poland and where no decision on his extradition has been taken. 3. an act must be considered terrorism".

> not only for the aforementioned serious international crimes but also for other offences committed abroad, if the double incrimination requirement is met.[33]

Based on the principles and rules of jurisdiction in Polish and Hungarian criminal law, it can be concluded that, in addition to the primary application of the territorial principle, the relevant regulations extend the traditional territorial jurisdiction and provide for almost unlimited extraterritorial jurisdiction. Consequently, *when a cybercrime is committed, Hungarian and Polish criminal law apply in almost every possible situation, regardless of the place of the commission and the nationality of the perpetrator*. The only limitation[34] appears to be the double incrimination requirement, but since cybercrimes are punishable under international treaties, the principle of universality applies in theory, and there is no obstacle to applying Hungarian and Polish criminal law to cybercrimes committed by non-citizens abroad. However, such a *broad and almost catch-all regulation of jurisdictional provisions inevitably generates conflicts of jurisdiction*.

5.4. Conflicts of Jurisdictions

There are two types of jurisdictional conflicts, negative and positive. In the first case, either no state has potential jurisdiction over the case (this is almost impossible in practice), or no state intends to exercise its actual jurisdiction. The latter situation is very rare, but it can happen. An example from the literature maintains that when there occurs cybercrime concerning viruses, or Web sites showing hate speech, single countries may feel they are insufficiently harmed for

[33] See Art. 3(2)(aa) of the HCC: "Hungarian criminal law shall apply to any act committed by non-Hungarian citizens abroad, if it is punishable as a criminal offence under Hungarian law and in accordance with the laws of the country where committed."

[34] However, it should be stressed that in the case of offences committed abroad by non-Hungarians, the provision requiring the decision of the Prosecutor General to initiate criminal proceedings constitutes a (self-)limitation on the exercise of Hungarian criminal jurisdiction.

them to claim jurisdiction, perhaps also because they may think that some other country will surely claim jurisdiction.[35]

Much more common is the positive conflict of jurisdiction, where two or more states claim and intend to exercise jurisdiction in the same criminal case. For instance, if a Hungarian national uses a computer in Poland to hack into a computer in Austria, at the very least, Hungary, Poland, and Austria will be able to claim jurisdiction.[36]

Since cybercrime in many cases falls within the scope of transnational criminality, it can often be difficult to determine in which country the crime has been committed; the perpetrator and the victim may be in different countries, and the information asset or data involved in the crime may be located in a third country. Consequently, *in cybercrime cases, it is a very realistic and almost necessarily occurring situation that numerous countries have jurisdiction to prosecute*. In this situation, problems may arise in making decisions about which state should prosecute.[37]

Resolving conflicts of jurisdiction is a fundamental interest to avoid duplication of proceedings and to ensure efficient, timely and cost-effective prosecution.[38] Two basic methods for resolving positive conflicts of jurisdiction are the hierarchy of jurisdictional principles and the consultation between the States concerned.

The hierarchy of jurisdictional principles is exemplified by the Council of Europe Recommendation 420 (1965) on the Settlements of conflicts of jurisdiction in criminal matters, according to which the State in whose territory the offence was committed shall have the primary right to exercise jurisdiction. The primacy

[35] S.W. Brenner, B.-J. Koops, *Approaches…*, *op. cit*., p. 41.

[36] Similar examples are mentioned by Mezei and Brenner, Koops. See K. Mezei, *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, Pécs 2019, p. 195 and S.W. Brenner, B.-J. Koops, *Approaches…*, *op. cit*., p. 41.

[37] L. Dornfeld, *Az elektronikus bizonyítékszerzés aktuális kérdései*, "Kriminológiai Közlemények" 2017, No. 77, p. 243.

[38] Further risks of jurisdictional conflicts are the duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the states concerned. See point 239 of the Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b (accessed on: 15.07.2023).

of the territorial principle can only be overridden by the protection principle, because if the act threatens the security or credit of the state, the threatened state has the primary criminal claim. The territorial principle is followed by the active personality principle, and finally the jurisdiction of the state in whose territory the perpetrator is found.[39] Furthermore, Article 10 of Council Framework Decision 2005/222/JHA[40] on attacks against information systems established the grounds of jurisdiction for the offences it covers. Proceedings may therefore be initiated if the offence has been committed in whole or in part within its territory, or by one of its nationals or the benefit of a legal person that has its head office in the territory of that member state. Based on paragraph 4, this ranking also constitutes a hierarchy in deciding which State should prosecute if two or more states have and intend to exercise jurisdiction in the same criminal case. However, Directive 2013/40/EU on attacks against information systems and replacing the Framework Decision no longer establishes a hierarchy between these jurisdictional grounds.[41] Ideas on the jurisdictional hierarchy have also been formulated in the relevant literature. Bassiouni, the famous international criminal lawyer, argued that the primacy of the territorial principle must prevail, followed by the active and passive personality principles, and only then can jurisdiction be exercised based on other principles, provided that the accused is in the territory of the state claiming jurisdiction.[42]

At first sight, the primacy of the territorial principle seems acceptable. For example, in principle, territoriality better guarantees due process and compliance with the principle of legality, which

[39] Recommendation 420 on the settlement of conflicts of jurisdiction in criminal matters adopted by the Consultative Assembly of the Council of Europe on 29 January 1965.

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

[41] L. Dornfeld, *Az elektronikus…*, *op. cit.*, p. 244.

[42] M.C. Bassiouni, *International Criminal Law. A Draft International Criminal Code and a Draft Statute for an International Criminal Tribunal*, Hingham 1987, p. 191.

requires individuals to be aware that a certain act is punishable.[43] Moreover, the majority of the evidence necessary for the investigation of a crime is usually located at the place where it was committed and there is reason to be optimistic about a quick and efficient completion of the criminal proceedings. However, it must be emphasised that currently there is *no international treaty that establishes a hierarchy of jurisdictional principles* and provides a general primacy of the territorial principle. Nor does customary international law allow such a conclusion to be drawn. On the other hand, in the case of cybercrime, *the place of commission is often uncertain*. Different countries have different rules on what should be considered the place of the commission in case of content-related cybercrimes, such as child pornography.[44] This can be the place where the data or content is uploaded or downloaded, or – as in Hungary[45] – the place where the server hosting the website is located. The identification of the perpetrator's location is further hampered by software and methods whose specific purpose is to hide the perpetrator's location (and identity) so that they cannot be identified geographically.[46]

Another way of solving the positive jurisdictional conflicts is *consultation* between states having and claiming jurisdiction. According to the Article 22(5) of the Budapest Convention, "When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."

It can be seen that, under the Convention, consultation is only an "appropriate" option and not a real obligation,[47] and the laconic

[43] J.-B. Maillard, *The limits of subjective territorial jurisdiction in the context of cybercrime*, "ERA Forum" 2018, Vol. 19, Issue 3, p. 3.

[44] S.W. Brenner, B.-J. Koops, *Approaches…*, *op. cit*., pp. 15–16.

[45] See the Decision BH2022.65 of the Hungarian Supreme Court.

[46] These methods include IP address modification and hiding (spoofing) and the use of proxy servers, VPN (Virtual Private Networks) or botnet infrastructure (zombie machines). See in details: J.-B. Maillard, *The limits…*, *op. cit*., pp. 4–6, and K. Mezei, *A kiberbűnözés…*, *op. cit*., pp. 195–196.

[47] According to the Explanatory Report of the Convention, "(…) the obligation to consult is not absolute, but is to take place „where appropriate". "Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it

provision does not provide guidance on the ranking of jurisdictional claims. Moreover, the Convention does not regulate the criteria[48] which, considered together, can be used to decide which country is clearly most closely linked to the crime committed. Finally, the Convention does not provide an answer to the question of what to do if the consultation fails.[49]

5.5. Conflicts of Jurisdiction and the Institutions of International Cooperation in Criminal Matters[50]

In the following, I outline three hypothetical cases with a common characteristic: a *cybercrime* – a cyberattack – *is committed against a Hungarian victim* (a Hungarian citizen natural person or a Hungarian resident legal person, or other organisation). The three models were set up based on the place of the commission, giving importance to the perpetrator's nationality and the perpetrator's detected location after initiating the criminal proceedings. In

has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation." See point 239 of the Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b (accessed on: 15.07.2023).

[48] The factors need to be examined and taken into account in the consultation to resolve the jurisdictional conflict may include the place of the commission of the crime; the nationality of the perpetrator; the location of the perpetrator and the victim(s); the place where the majority of the crime was committed or where most of the victims are located; the place where the damage is significant; the possibilities of transfer or extradition to other countries; the interests of the perpetrator, in particular his or her resocialisation, etc. See: Z.A. Nagy, *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in:] K. Karsai, Zs. Fantoly, Zs. Juhász, Zs. Szomora, A. Gál (eds.), *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, Szeged 2018, p. 761.

[49] If the consultation is unsuccessful, recourse to an intergovernmental organisation or (arbitration) tribunal can be an option, but this would certainly lead to a prolongation of the procedure and call into question the timeliness of the subsequent criminal proceedings.

[50] This chapter is made by using the following source R. Bartkó, F. Sántha, *A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre*, (manuscript, under publication).

the first case, the detected location of the cyberattack is Hungary, in the second case the starting point of the attack is a member state of the European Union (EU), and in the third, the place of the commission is on the territory of a third state outside the EU.

5.5.1. THE DETECTED LOCATION OF THE CYBER-ATTACK IS HUNGARY

When the perpetrator – whether a Hungarian citizen or a foreigner – commits cybercrime on the territory of Hungary, there is no jurisdictional problem, as the Hungarian state, and therefore the competent Hungarian criminal authorities have clear jurisdiction based on the territorial principle. In this case, the perpetrator located in Hungary can, as a main rule, be prosecuted without any particular difficulty.

From the perspective of jurisdiction, the situation becomes more complex and the instruments of international cooperation in criminal matters will play a role when the detected offender has left Hungary and is staying in a member state of the EU at the time of the initiation of the criminal proceedings. In this situation, if the national arrest warrant is unsuccessful, the Hungarian criminal court will issue a *European arrest warrant*, which, if successful, will allow the perpetrator to be *surrendered* in accordance with the procedural rules laid down in the Act CLXXX of 2012 on the cooperation with the member states of the European union in criminal matters.[51]

Two scenarios are possible from this point. If the perpetrator is a Hungarian national who is residing in a member state of the EU,

[51] This Act is the implementing law of the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. The European arrest warrant is a simplified cross-border judicial surrender procedure for the purpose of prosecuting or executing a prison sentence or detention order. A warrant issued by one EU country's judicial authority is valid in the entire territory of the EU. It has replaced the cumbersome in many cases lengthy extradition procedures that used to exist between EU countries. Here it should be noted that all cybercrimes in Hungary meet the condition that a European arrest warrant can only be issued if the crime is punishable by a minimum of 1 year imprisonment.

Hungary will have exclusive jurisdiction based on the territoriality principle and the suspect will most likely be surrendered to Hungary under the arrest warrant. By contrast, if the perpetrator is not a Hungarian, the EU member state of which he or she is a national may also establish jurisdiction based on the active personality principle which is included in the Budapest Convention, as analysed earlier.[52] However, in my view, if the cyberattack takes place in Hungary against a Hungarian victim, the aspects of the evidentiary procedure, and, consequently, the success of the procedure will shift the balance towards the territorial principle. In this case, the surrender based on the European arrest warrant ensures the presence of the Hungarian perpetrator in the domestic criminal proceedings.

The situation is even more complicated if the location of the suspect, based on the international arrest warrant issued by the Hungarian Court, is detected in a third country, namely outside the European Union. In this case, surrender based on the European arrest warrant cannot be invoked, but the provisions on *extradition* under Article 24 of the Budapest Convention and the Hungarian Act XXXVIII of 1996 on international mutual legal assistance in criminal matters will apply. According to Article 31 of the Hungarian Act, Hungary is entitled to submit a request for extradition for the purpose of prosecuting to the third state where the perpetrator is staying. The previously mentioned conflict of jurisdiction may of course arise in this case as well, but the spirit of the Budapest Convention justifies the preference for conducting criminal proceedings under Hungarian rules in this case as well, therefore extradition may be a viable legal institution.[53]

[52] If this state and Hungary reach an agreement in the consultation, this state may prosecute the perpetrator.

[53] If the perpetrator is located in a non-EU member state that has not ratified the Budapest Convention, the provisions of the European Convention on Extradition (1957) will apply. (All countries that are members of the Council of Europe are parties to the European Convention on Extradition.) In the case of a non-European country, the rules of the international treaty concluded with the state concerned, or, in the absence of a treaty, the rules of reciprocity, and the Hungarian Act XXXVIII of 1996 will apply.

5.5.2. THE DETECTED LOCATION OF THE CYBER-ATTACK IS A MEMBER STATE OF THE EUROPEAN UNION

The second case of my model analysis is when the cyberattack affects a Hungarian victim, but the location and starting point of the attack is not Hungary, but another member state of the EU.

In this situation, *one possible scenario* is if the perpetrator is a Hungarian national who is staying in another EU country.[54] As a result, there are essentially two competing grounds of jurisdiction. The first is the Hungarian nationality of the perpetrator, which is the factor underlying the active personality principle. The other is the territoriality principle, since the offence was committed from the territory of another member state. The fact in which state the criminal proceedings were initiated will be relevant to the solving of this jurisdictional problem.

a) *If the proceedings have been initiated only in Hungary*, the presence of the perpetrator in the domestic criminal proceedings can be provided along the previously mentioned forms of cooperation in criminal matters.
b) *If the offender perpetrator has been prosecuted only in the member state where the offence was committed*, that state, since the perpetrator is a Hungarian national, shall provide information to Hungary on the proceedings within the framework of the exchange of information,[55] resulting in two further possible cases: (i) member state where the offence was committed conducts its own criminal proceedings, and then, after taking into account the foreign judgment, the final decision can be enforced in Hungary; or (ii) the Hungarian authorities initiate the surrender of the Hungarian national for the purpose of prosecuting based on an European arrest warrant issued after the initiation of the criminal proceedings.

[54] If the Hungarian national perpetrator is staying in a non member state of the EU after the criminal proceedings have been initiated, the provisions on extradition previously mentioned may be applied.

[55] On the provisions on the exchange of information between Member States, see Articles 104–105 of the Act CLXXX of 2012.

c) In the third case, *criminal proceedings have been initiated both in Hungary and in the member state where the offence was committed*. In the case of *parallel proceedings*, namely where two member states are simultaneously conducting criminal proceedings against the same offender for the same cybercrime, the Act provides for a *consultation procedure,*[56] the outcome of which will determine which Member State will actually prosecute the offender.

The other possible scenario in my second model is when the cybercrime causing harm in Hungary is committed by a person of non-Hungarian nationality in another EU member state. In this case, apart from the passive personality principle, there is no other ground for conducting criminal proceedings in Hungary, and the jurisdiction of Hungary cannot be justified based on the interest of evidence and the nationality of the perpetrator. I think that, in such a scenario, the Hungarian authorities may provide procedural legal assistance for criminal proceedings conducted by a foreign state, but there is no reasonable justification either for conducting the proceedings domestically or for enforcing any criminal sanction in Hungary.

5.5.3. THE DETECTED LOCATION OF THE CYBER-ATTACK IS A THIRD COUNTRY OUTSIDE THE EUROPEAN UNION

In my third hypothetical situation, the cybercrime directed against the Hungarian victim is committed in the territory of a state that is not a member state of the EU. If the perpetrator is a Hungarian citizen and staying in Hungary, Hungary has jurisdiction on

[56] See Articles 106–107 of the Act CLXXX of 2012. According to the Act, the parties shall take into account all relevant factors to decide which member state will prosecute the case. Such relevant factors include the place of the commission of the crime, the nationality of accused and the victim(s), the place of detention of the accused, the state of the criminal proceedings in the member states, the fact in which member state more evidence is available, and whether the criminal proceedings in the member states are related to other criminal proceedings in that member state. If the consultation is unsuccessful, the Prosecutor General may refer the matter to Eurojust to decide.

the basis of the active personality principle and there is no particular problem in prosecuting the perpetrator. However, if the Hungarian perpetrator is located in a non-EU country, extradition under Article 24 of the Budapest Convention or, if the Convention cannot be invoked, extradition rules based on the European Convention on Extradition (1957)[57] may apply.[58] And if the Hungarian offender is staying in a country that is not party to the previously mentioned conventions, the rules of the international treaty concluded with the state concerned, or, in the absence of a treaty, the rules of reciprocity, and the Hungarian Act XXXVIII of 1996 will apply. Finally, the last possible scenario for my third situation is when the offender is not a Hungarian citizen. In this case, the jurisdiction of Hungary could only be established on the basis of the passive personality principle, which presupposes the principle of double criminality. However, based on the place where the offence was committed and the nationality of the perpetrator, the states concerned are much more likely to claim jurisdiction under the Budapest Convention. In this scenario – as we have also discussed in the second model – Hungarian authorities may only provide procedural legal assistance for criminal proceedings conducted by the foreign state.

5.6. Conclusion

The hypothesis I put forward at the beginning of this study has been proven to be true: traditional jurisdictional principles in domestic and international criminal law are not able to respond to the challenges posed by cybercrime, in particular positive jurisdictional

[57] Since the Budapest Convention, based on the purposes set out its preamble, is a lex specialis compared to the European Convention on Extradition, the applicability of the Convention should be examined first, and the European Convention on Extradition is secondary.

[58] It is not excluded, of course, that the state concerned, either on based on the Article 24(6) of the Budapest Convention or Articles 7 and 8 of the European Convention on Extradition, may refuse extradition because it has already initiated criminal proceedings under the territoriality principle. In this case, following the criminal proceedings, the foreign judgment can be enforced in Hungary.

conflicts. Possible solutions to the problems outlined could be the creation of a global international treaty[59] to regulate jurisdictional issues and the procedure to be followed in the event of a conflict of jurisdiction. Consultation between the States concerned is a necessary element, but it is advisable to set a reasonably short deadline for such consultation. And if the consultation fails, a mandatory hierarchy of jurisdictional principles need to be established, otherwise we risk the effective prosecuting the perpetrators of cybercrime. Finally, it should be emphasised that the successful determination of the state that has actual jurisdiction in the case is only the first step in holding the perpetrator accountable, since jurisdiction can only be effectively exercised and proceedings carried out if the perpetrator is available to the authorities of the state that has jurisdiction, for example if he or she is in the custody of that state. Otherwise, the institutions of international or European mutual legal assistance in criminal matters, such as extradition or surrender based on the European arrest warrant, should be used.

REFERENCES

Bartkó, R., Sántha, F., *A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre*, (manuscript, under publication).

Bassiouni, M.C., *International Criminal Law. A Draft International Criminal Code and a Draft Statute for an International Criminal Tribunal*, Hingham 1987.

Brenner, S.W., Koops B.-J., *Approaches to Cybercrime Jurisdiction*, "Journal of High Technology Law" 2004, Vol. 4, No. 1.

Clough, J., *Principles of cybercrime*, Cambridge 2010.

Dornfeld, L., *Az elektronikus bizonyítékszerzés aktuális kérdései*, "Kriminológiai Közlemények" 2017, No. 77.

[59] Note that a new convention on cybercrime – the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes – is being drawn up within the framework of the United Nations.

Farkas, Á., *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapjai*, "Jog-Állam-Politika" 2019, No. 2.

Fekete, L., *Szabadság, jog és szabályozás a kibertérben*, "Replika" 2001, No. 9.

Horváth, T., Lévay, M., *Magyar büntetőjog általános rész*, Budapest 2014.

Jakab, D.B., *Területiség és deterritorializáció. A terület mint a társadalomelmélet vezérfonala*, "Replika" 2009, No. 5.

Maillard, J.-B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, "ERA Forum" 2018, Vol. 19, Issue 3.

Mezei, K., *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*, Pécs 2019.

Nagy, Z.A., *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in:] Karsai, K., Fantoly, Zs., Juhász, Zs., Szomora, Zs., Gál, A. (eds.), *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, Szeged 2018.

Nyitrai, P.M., *Nemzetközi* és *európai büntetőjog*, Budapest 2006.

Ryngaert, C., *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*, "German Law Journal" 2023, Vol. 24, Issue 4.

Tóth, D., Gáspár, Zs., *Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés terén*, "Belügyi Szemle" 2020, No. 2.

Wiener, I.A., *A büntető joghatóság és gyakorlása, kivált az Európai Unióban*, "Állam és Jogtudomány" 2002, No. 3–4.

DR PIOTR BURCZANIUK
Cardinal Stefan Wyszyński University in Warsaw | DOI: 10.32041/9788367149761/6

Chapter 6. Pre-Trial Activities of Intelligence Service and Law Enforcement Agencies

6.1. Introduction

This chapter will analyse the pre-trial activities directed at the acquisition of information, relevant from the perspective of criminal law enforcement authorities to carry out activities in the identification and detection of cybercrimes and the prosecution of their perpetrators. The considerations focus on two essential types of these activities. First, security activities related to the functioning of the European and national cybersecurity system and, in particular, the proper cooperation of the participants in this system with law enforcement agencies. Secondly, intelligence gathering activities that national services are authorised to carry out, in the context of the possibility and scope of their use in the fight against cybercrime. A complementary element of the considerations in question will be the analysis of international cooperation in both areas indicated above, conducted between services, in particular within the European Union, which is of fundamental importance in the context of combating cybercrime, which is characterised by its cross-border nature.

The main objective of this analysis is to answer the question of whether the scope of activities belonging to both groups and the international cooperation conducted is sufficient given the nature of the current types of cybercrimes and what are the most significant challenges requiring legislative intervention. In addition to

the main objective indicated in the first paragraph, each part of this analysis sets specific objectives related to the specificity of the issue under consideration.

6.2. Impact of the Cybersecurity System on the Fight Against Cybercrime

This section discusses the relevance of the security measures associated with the functioning of the European and national cybersecurity system for the fight against cybercrime. The starting point for these considerations must be the answer to the question of the interplay and impact of these two, theoretically separate, aspects of cybernetic security, i.e., cybersecurity and cybercrime.

Starting with very general definitions of both terms, it should be pointed out that cybersecurity is fundamentally focused on threat prevention. It refers to actions and measures taken by a broad spectrum of individuals, especially owners and users, to protect ICT[1] from digital threats. Combating cybercrime, on the other hand, focuses on the detection and prosecution, of illegal incidents occurring with or against ICTs by authorised state services and authorities.

Identifying the relationship and mutual interdependencies between these two aspects of cybernetic security seems crucial to ensure the effectiveness of efforts in both areas. This is because it is impossible to effectively identify and combat cybercrimes without the necessary level of expertise in the area of the cybersecurity prevention system. At the same time, it is also impossible to carry out this prevention effectively without knowing the actual methods of the perpetrators of cybercrimes. Cybersecurity and the fight against cybercrime are thus still two different but increasingly interlinked aspects of a single cybernetic security, the protection of which requires coordinated actions and increasingly far-reaching cooperation between those responsible for both areas.

[1] Information and Communication Technology, covering a wide range of technologies including computers, software, networks, the internet and mobile devices.

Starting a legal reflection on the cybersecurity system and its impact on the fight against cybercrime, it should be noted that to date, it has not become the subject of a binding and universally applied normative act. Although numerous activation policies in this area have been put in place by the United Nations, in the end, mainly due to diverging interests, they only led to the creation of soft law standards in the form of resolutions and declarations containing only recommendations addressed to Member States. Also regionally, including within the European Union, a similar regulatory approach prevailed. The situation was only fundamentally changed by the adoption of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,[2] referred to as the "NIS Directive".

The NIS Directive, as indicated in its Article 1, set as a fundamental objective the achievement of a high common level of security of network and information systems in the European Union to improve the functioning of the internal market. This was to be achieved by taking action in three dimensions: firstly, the introduction of network and information security obligations; secondly, the creation of responsible institutions in all Member States; and thirdly, the definition of rules for cooperation between these institutions at the European level.

In the first aspect, the NIS Directive assumed the introduction of security obligations for two groups of entities. The first included Operators of Essential Services (OES), identified at Member State level, i.e., services essential for the maintenance of critical societal and economic activities, operating in one of the sectors listed in Annex II to the Directive, i.e., energy, transport, banking, financial market infrastructures, healthcare, water supply and digital infrastructures. The second includes the genre-identifiable large Digital Service Providers (DSPs) listed in Annex III, i.e., online trading platforms, search engines and cloud computing services. The obligations imposed on them were essentially based on proper risk management, which is based on conducting an assessment

[2] OJ EU L 2016, No. 194, p. 1.

of the risk and implementing security measures appropriate to its type.[3] The NIS Directive established a lower degree of tolerable risk and thus broader obligations for key service providers, who are to be guided primarily by ensuring the continuity of these services. The means of implementing risk management became the identification, prevention, detection and handling of all incident risks and the mitigation of their impact.[4] One of the primary responsibilities of key service operators and digital service providers was to ensure the security of the networks and information systems they use. The requirements imposed by the Member States in this regard were to be proportionate to the risks associated with the network and information system concerned and were to take into account the state of the art of such measures,[5] with a view to eliminating an excessive financial and administrative burden imposed on such operators. The NIS Directive assumed ex ante measures for key service providers, linked to the certification process, while the requirements were considerably relaxed for digital service providers, with only ex post supervisory measures.

The second aspect is that the NIS Directive imposed obligations on each Member State to set up competent national cybersecurity authorities, covering at least the sectors and services designated by the Directive.[6] The Directive established Two levels of cooperation between these authorities: technical and political/strategic. The first level concerns the establishment of the so-called CSIRT teams,[7] which are responsible for dealing with risks and for undertaking incident-response measures. In accordance with the Directive, such teams shall be established at least in the sectors and services designated by the Directive. The national CSIRTs of the Member States and CSERT-EU were to form a CSIRT network to develop confidence and trust between Member States and to promote rapid and effective

[3] Cf. Recital 44.
[4] Cf. Recital 46.
[5] Cf. Recital 54.
[6] In Poland, the uKSC distinguishes several sectors that are key to the functioning of the State, which are supervised by the competent authorities, i.e. the ministers responsible for individual sectors of the economy.
[7] Computer Security Incident Response Teams.

cooperation. In establishing a system of these teams and entrusting them with the task of reporting serious security incidents, the authors of the Directive saw an opportunity for effective prevention and response. Within the framework of political and strategic cooperation, each Member State was to designate a single point of contact for cybersecurity, responsible for cooperation with other coordination bodies in the EU and with the European Commission,[8] in particular within the so-called Cooperation Group, thus laying the foundation for European cooperation on cybersecurity. In addition, the NIS Directive envisaged the creation of national incident strategies and plans[9] and the established requirements for regular security audits.

The deadline for the implementation of the NIS Directive was 9 May 2018. Poland fulfilled this obligation belatedly by adopting the Act on the National Cybersecurity System on 5 July 2018,[10] which entered into force on 28 August 2018, hereinafter referred to as the "uKSC".

In the context of the main thesis presented in this paper, it should be noted that the NIS Directive does not regulate the substantial aspects of the fight against cybercrime in substance. This aspect of cybernetic security has been referred to in a rather concise manner. Indeed, according to recital 8 of the NIS Directive (and its Article 1(6)), it is without prejudice to the possibility for each Member State to take measures necessary, inter alia, to enable the investigation, detection and prosecution of criminal offences. Its Recital 62 also notes that incidents may result from criminal offences the prevention, investigation and prosecution of which is supported by coordination and cooperation between key service operators, digital service providers, competent authorities and law enforcement authorities. Where it is suspected that an incident is related to serious criminal offences under Union or national law, Member States should encourage key service operators and

[8] In Poland, according to the uKSC, it is run by the minister responsible for cybersecurity.

[9] In Poland, the Resolution No. 125 of the Council of Ministers of 22 October 2019, which was adopted, remains valid. Cybersecurity Strategy of the Republic of Poland for 2019-2024 (M.P. of 2019, item 1037).

[10] Journal of Laws 2022, item 1863.

digital service providers to report serious criminal incidents to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities from different Member States be facilitated through the European Cybercrime Centre (EC3) and through ENISA, as described further below.

The assumptions of the NIS Directive mentioned above are reflected in the uKSC. The provision of Article 40(2) of the SCC is of fundamental importance in this context, according to which CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity teams provide information constituting legally protected secrets, including those constituting company secrets, to law enforcement authorities in connection with an incident that fulfils the constitutive elements of a crime. As pointed out in the Polish legal doctrine:

> Article 40(2) complements Article 34 of the KSC Act, allowing criminal proceedings to be conducted in a situation where an incident is found to constitute a criminal act. The legislator has regulated both the cooperation with law enforcement authorities and the rules of exchange of information with them separately, as Article 2(10) narrowly defines the concept of handling an incident. According to the statutory definition, these are activities that make it possible to detect, classify, analyse, prioritise, take corrective action and limit the effects of an incident. Undoubtedly, this definition does not include notifying law enforcement authorities of an incident or securing digital evidence for ongoing criminal proceedings. By contrast, Article 4(8) of the NIS Directive appears to introduce a broader definition of incident handling, which shall be understood as covering all procedures aimed at detection, analysis, mitigation and response to an incident. The response element may therefore include the notification of a crime and the collection of evidence for subsequent investigation. For this reason, the legislator has imposed an obligation on the CSIRT MON, CSIRT NASK, CSIRT GOV and sectoral cybersecurity

> teams to provide information which is a legally protected secret to law enforcement authorities in connection with an incident which fulfils the constitutive elements of a crime. In turn, these authorities in such situations act on the basis of general provisions.[11]

At the same time, in accordance with Article 38 of the SCS, information processed under the Act shall not be made available if its disclosure would, inter alia, adversely affect the investigation, detection and prosecution of criminal offences.

Thus, on the basis of the regulations cited above, it is evident that both the European and the Polish legislator, while creating the rules of cybersecurity management, assumed an immanent necessity of correlation between two aspects of cybernetic security – cybersecurity and combating cybercrime. This conclusion is also confirmed by an analysis of the content of the Cybersecurity Strategy of the Republic of Poland for the period 2019–2024, issued on the basis of Article 68 of the uKSC, which sets out five specific objectives of the Polish government's policy to strengthen and develop the national cybersecurity system. Under the first specific objective on the development of the national cybersecurity system, it was that the capacity to combat cybercrime, including cyber espionage and terrorist incidents should be increased.

A review of the NIS Directive in the EU, after six years in force, has shown that the wide discretion left to Member States in its implementation has led to significant variation in the types and levels of detail in the obligations imposed on service providers, which had a significant impact on their cross-border activities and thus led to fragmentation of the EU internal market and disrupted its functioning. To address this issue, Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, referred to as "NIS Directive 2", was adopted

[11] P. Drobek, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, Article 40.

on 14 December 2022. It entered into force on 16 January 2023 and the deadline for its implementation is 17 October 2024. The primary objective of the NIS 2 Directive is, as highlighted in its Recital 5, to eliminate divergences between Member States, in particular by defining minimum rules for the operation of a coordinated regulatory framework, establishing mechanisms for effective cooperation between the responsible authorities in the different Member States, updating the list of sectors and activities subject to cybersecurity obligations and introducing effective remedies and enforcement measures, which are key to the effective enforcement of these obligations.

An analysis of both the recitals of this directive and its individual provisions leads to the general reflection that a significant part of its provisions are the result of practical problems encountered by the cybersecurity system shaped by the NIS Directive. Indeed, NIS 2 implies a number of security solutions directed at threats identified in the cybersecurity system in recent years. Hence, its provisions directly refer to specific types of such threats, which either result from a specific methodology of action of the perpetrators, such as, inter alia, ransomware attacks,[12] or are related to the use of specific types of technological solutions, including, inter alia, the Internet of Things[13] and identifiable solutions, e.g., end-to-end encryption.[14]

The NIS 2 Directive abolishes the existing entity-based distinction between key service operators and digital service providers. Instead, a uniform size criterion will be introduced to include even medium-sized enterprises (in some cases also small and micro enterprises) operating in the sectors or providing the types of services covered by the Directive. These entities will be divided into new categories, i.e., key actors (Annex I sectors: energy, transport, banking, financial market infrastructures, healthcare, drinking water, waste water, digital infrastructures, ICT service management, public administration entities, space) and important actors (Annex II sectors) and qualified according to their size, and importance of their respective sectors or the type of services they provide. As can be seen from the above,

[12] Cf. Recital 54.
[13] Cf. Recital 53.
[14] Cf. Recital 98.

the NIS 2 Directive imposes cybersecurity compliance obligations on entirely new entities, significantly broadening the cybersecurity regime. At the same time, the new regulation emphasises the need for a sectoral approach to cybersecurity, assuming and announcing the introduction of sectoral regulations that take into account the specificity and complexity of a particular sector, shaping tailored risk management measures, incident reporting obligations and oversight and enforcement rules. In this context, it should be noted that the Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector,[15] directly targeted at the financial sector, was adopted at the same time as the NIS 2 Directive.

As far as the area of risk management is concerned, the NIS Directive implies the need to balance the measures applied with the degree of dependence of the entity on networks and information systems, the degree of exposure of the entity to risk and the social and economic impact that a potential incident would have. Such measures are aimed at identifying the risk of incidents (including a special assessment of the security of the supply chain of products[16] and services[17]), preventing, detecting, responding to and recovering from incidents and mitigating their impact.[18] The security of the physical environment of networks and systems must also be considered in the new risk management approach. Therefore, an important methodological basis for the measures to be introduced is to be good market practice, based mainly on the standardisation process, with particular reference to the standards contained in the ISO/IEC 27000 series.[19] The whole risk management process is also to take into account the minimisation of excessive financial and administrative burdens.

The NIS 2 Directive emphasises the importance of so-called cyber hygiene, a set of good practices aimed at ensuring overall safety

[15] OJ EU L 2022, No. 333, p. 1.
[16] Cf. Recital 85.
[17] Cf. Recital 86.
[18] Cf. Recital 78.
[19] Cf. Recital 79.

and security in the event of incidents.[20] At the same time, it draws attention to the NIS 2 Directive's move away from purely reactive measures, based on a system of incident reporting and identification, towards active cyber defence, defined as proactively preventing, detecting, monitoring, analysing and mitigating network security breaches, combined with the use of capabilities deployed within and outside the network under attack. Furthermore, the identification and neutralisation of vulnerabilities in networks and information systems, in particular by their manufacturers or solution providers, is to become the key to the new system. Among other things, civil and criminal liability exemptions of the individuals carrying out vulnerability and information security tests enhance the process of identification of vulnerabilities.

The changes introduced by the EU legislator are part of a new approach to cybersecurity policy, which places the user of the system, regardless of his or her role in the system, rather than the information system (hardware and software), at the centre. In a nutshell, this approach assumes that a system is only as secure as its users are aware of the risks and follow certain procedures. This change in approach is the result of analyses of the scale and types of reported significant and critical incidents, which show that most of them have their origin in human activity, which turns out to be the weakest link in the entire cybersecurity system. This new policy therefore breaks with the original assumption of striving for "perfection" of information systems, focusing instead on the activities of people, organisations and states in cyberspace, aiming to steer them towards behaviour that is considered safe.

Interestingly, the need to change the optics of cybersecurity policy was recognised by the Polish legislator even before the adoption of the NIS 2 Directive, proposing as early as January 2021[21] to replace the existing definition of the term "cybersecurity" covered by the PSC, derived from the NIS Directive, focused on the resilience of the information system and its protection, in favour of a definition covering

[20] Cf. Recital 49 and 89.

[21] Article 1(2)(b) of the Bill of 20 January 2021 amending the Act on the National Cybersecurity System and the Act – Telecommunications Law.

activities necessary to protect information systems, users of such systems and other entities, from cyber threats. He also points out that some of the directional changes currently covered by the NIS 2 Directive were introduced into the Polish legal order even before the implementation of the NIS Directive, e.g., by the Act of 10 June 2016. on anti-terrorist activities,[22] which gave the Internal Security Agency, hereinafter referred to as the "ABW", the tasks of identifying, preventing and detecting threats to the security of the public administration's ICT systems and critical infrastructure, to be carried out through powers to: assess the security of these ICT systems, providing, at the request of the Head of the ABW, information on the construction, functioning and principles of operation of these ICT systems, blocking the availability in an ICT system of specific IT data or ICT services related to a terrorist event, keeping a register of events violating the security of these ICT systems, issuing recommendations to the Head of the ABW with a view to improving the security level of ICT systems. In turn, the PCA itself enabled the ABW to implement the ARAKIS-GOV early warning system for Internet-based threats.

In the context of the main thesis presented in this paper, it should be added that the NIS Directive 2, like the NIS Directive, does not regulate the fight against cybercrime in substance, but the extent of its correlation with this aspect of cybernetic security is much clearer than in the case of the previous Directive. In accordance with recital 107, where it is suspected that an incident is related to serious criminal offences under Union or national law, Member States should encourage key and important players, on the basis of the applicable rules of criminal procedure under Union law, to report serious criminal incidents to the appropriate law enforcement authorities. Where appropriate, and without prejudice to the data protection rules applicable to Europol, it is desirable that coordination between competent authorities and law enforcement agencies from different Member States be facilitated by the European Cybercrime Centre and ENISA. In addition, the NIS Directive 2 notes the need to give

[22] Journal of Laws 2022, item 2632.

law enforcement authorities access to information including, inter alia, domain name registration data.[23]

As can be seen from the analysis of the provisions of the NIS Directive and NIS 2, the EU legislator sees the functional relationship between the cybersecurity system and the issue of combating cybercrime as two pillars of cybernetic security. Indeed, there is a strong logical link between securing ITC systems, and thus the services provided by means of such systems and the information stored in them, and the issue of combating cybercrime, which is often a direct consequence of gaps or deficiencies identified in the security policies of these systems or errors associated with their use. The security of information systems is therefore crucial at the prevention stage, as a mechanism to prevent cyber attacks. An analysis of the statistics[24] of the scope of incidents reported within the cybersecurity system leads to the conclusion that most of them aim to exploit vulnerabilities in the security of information systems, with the consequence of acquiring protected information or infecting the system with malware, which constitutes a criminal offence. Therefore, ensuring the security of information systems is one of the primary measures to prevent cybercrime. The NIS Directive and NIS 2 and the entire system established on their basis, are therefore aimed at enhancing the security of information systems in strategic sectors, which indirectly contributes to reducing the possibility of cyber attacks and thus preventively combating cybercrime.

Undoubtedly, the cybersecurity system, based on the prevention, detection and response to various types of cyber threats, plays a key role in the fight against cybercrime. This role is outlined in two key aspects. First, when the cybersecurity system supports the process of identifying and prosecuting cyber criminals. Secondly, when it neutralises opportunities for perpetrators by eliminating system vulnerabilities previously identified in specific criminal activities. Thus, it can be said that, on the one hand, the cybersecurity system,

[23] Cf. Recital 110.

[24] Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2021 r., Warszawa 2022; Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2020 r., Warszawa 2021.

by carrying out monitoring, acquires information on specific incidents and secures the evidence necessary to identify the perpetrator; on the other hand, law enforcement findings on the specific modus operandi of the perpetrators, help to neutralise vulnerabilities in ITC systems and thus act as a preventive measure.

The developments in cybersecurity policy indicated above, focusing on the role and importance of the user of an ITC system and therefore also the potential victim or perpetrator of a crime, lead to the conclusion of an even greater need for convergence between these two aspects of cybernetic security in the near term.

However, it should be borne in mind that this rapprochement may face significant legal and practical problems. The most significant of these seem to relate to the different perspectives of the regulators and the main participants in both aspects on privacy and data protection issues. For, on the one hand, there is a great deal of pressure from law enforcement authorities for companies and institutions, which are also participants in the cybersecurity system, to collect and share more and more of such information with them, justifying this by the need to effectively combat cybercrime, while on the other hand, these companies, often inspired by the fears of their own users regarding the threat to their privacy and freedom, implement far-reaching restrictive measures in this regard. The second aspect is the concern about the use of various modern technologies, such as facial recognition systems, online behaviour monitoring or artificial intelligence algorithms, among others, which, on the one hand, may have a high level of effectiveness in the fight against cybercriminals, but, on the other hand, the mechanism of their operation is based on the collection and aggregation of large amounts of personal data, including sensitive data. It seems that both the EU and national legislators will soon be faced with the need to determine the balance between the needs of law enforcement and fundamental personal rights, led by the right to privacy. The Polish legislator will also face these challenges, inter alia, by undertaking the implementation of the NIS 2 Directive in the near future.

Attention should also be drawn to the challenge of the lack of consistency and harmonisation between different countries and regions in terms of both cybersecurity and cybercrime regulation. Many

companies operate globally, in multiple markets and face the need to comply with different standards and regulations, which can lead to complex and costly compliance processes and often, in situations of apparent contradiction, a lack of implementation. The lack of uniform regulations can therefore clearly hinder cooperation between countries and regions in the fight against cybercrime and in cybersecurity emergencies. The challenges described, therefore, do not take a domestic perspective, but clearly demonstrate, firstly, the need for regional and even global cooperation in the creation of an effective cybersecurity system; secondly, they make its emergence dependent on cooperation with ITC solution providers.

6.3. Types and Scope of Law Enforcement Intelligence Gathering Activities to Combat Cybercrime – Current Status and Challenges

The considerations set out in this part are devoted to intelligence gathering activities carried out by national services, in the context of the possibility of their use in order to obtain information relevant from the perspective of combating cybercrime.

The first element of these considerations is the analysis of the term intelligence gathering (the literal translation of the term used in the Polish legal acts is 'operational and reconnaissance activities') used in the Polish legal acts governing the scope of competence of services to define one of the types of activities they are authorised to perform. The analysis of these acts leads to the conclusion that at present[25] – to a different extent – eleven services are authorised to perform them, including six law enforcement services, i.e., the Police, the Military Police and the Border Guards, the State Protection Service, the National Fiscal Administration, the Prison Service (they have, in principle, investigative and administrative powers); and five services defined as special services, i.e., the Internal Security Agency, the Foreign Intelligence Service, the Military Counterintelligence Service, the Military Intelligence Service and

[25] Status as of 29 May 2023.

the Central Anti-Corruption Bureau (they have in principle, analytical and informative powers. The exceptions are the ABW and the CBA, which also have investigative powers). The indicated types of activities reflect the scope of responsibilities of these services – in the case of law enforcement services, their tasks are focused on preventing crimes and prosecuting their perpetrators, whereas, as far as the in intelligence and security services are concerned, their essential tasks include obtaining and transmitting information.

The introduction of a legal definition of the notion of "operational and reconnaissance activities" was assumed in 2008 by the draft act on intelligence gathering activities, defining them such activities as a set of undertakings, overt and covert, conducted for the three purposes indicated in the draft, which consist, in particular, in obtaining, collecting, processing and checking in an overt and covert manner information about crimes and obtaining documentation, samples and comparative materials in order to reveal or secure evidence of a crime.[26] The works on the draft have not been completed. However, discussion about the need for statutory regulation of these activities has been ongoing, including the presentation of a draft Operational Work Code at a Senate hearing in January 2023, which is "intended to be a kind of instruction manual for the operation of the services".[27] However, incomplete legislative activities on the indicated drafts resulted in a lack of the legal definition of the notion of "intelligence gathering activities" in the Polish legal system. What is more, the other types of activities – investigative, administrative or analytical – do not have such a definition either. This implies the necessity to systematically separate and qualify them on the level of legal doctrine.

The literature on the subject emphasises that intelligence gathering shall be understood as activities of competent state authorities which essentially consist of secret and confidential, extra-procedural

[26] Article 2(1) and (2) of the draft law on operational and reconnaissance activities, online: https://orka.sejm.gov.pl/proc6.nsf/projekty/353_p.htm (accessed on: 29.05.2023).

[27] P. Śmiłowicz, *Kodeks pracy operacyjnej dla służb*, "Gazeta Prawna online", 26 January 2023, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8646248, kodeks-pracy-operacyjnej-dla-sluzb-ko.html (accessed on: 01.06.2023).

activities of such services, directed at the performance of their tasks related to the prevention of crime and other negative social phenomena and their combating. Moreover, these activities are generally performed outside the framework of criminal proceedings, although they often serve to fulfil the tasks of ongoing or future criminal proceedings.[28] The extra-procedural mode in which such activities are being carried out also translates into the problem of using such material as evidence in a criminal case.[29] It is clearly emphasised that:

> the results and the course of the activities in question do not have a direct evidentiary effect and, therefore, cannot be directly used in the course of criminal proceedings. However, these activities may determine the areas in which evidence needs to be gathered and may also serve to check evidence that has already been gathered. Mostly these activities serve specific ongoing or future criminal proceedings, often initiated on the basis of their results. They may also be carried out without a direct link to a specific criminal case.[30]

The features indicated above – secrecy, "extra-procedurality", deception – as an acceptable and inherent element of such actions, or their informative role, are the most frequently indicated distinctive features of these actions in the legal literature.[31] In addition, the possibility of interchangeably use of such terms as: "operational work, operational activities, operational activities".[32]

---

[28] Cf. Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Toruń 1996, p. 67; J. Widacki (red.), *Kryminalistyka*, Warszawa 1999, p. 110; B. Hołyst, *Kryminalistyka*, Warszawa 2016, p. 47.

[29] Cf. P. Czarnecki, *Czynności operacyjno-rozpoznawcze a postępowanie karne*, "Palestra" 2014, nr 7–8.

[30] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, https://wspia.eu/media/oojnsacq/44-w%C3%B3jcik.pdf (accessed on: 01.06.2023).

[31] Cf. T. Hanusek, *Kryminalistyka. Zarys wykładu*, Kraków 1996, p. 96.

[32] N. Nowicki, *Normatywne ujęcie czynności operacyjno-rozpoznawczych w aspekcie dowodu nielegalnego*, "Przegląd Bezpieczeństwa Wewnętrznego" 2021, t. 13, nr 24, p. 333.

In the context of the correlation between the different types of activities, in accordance with the doctrine of administrative law, intelligence gathering activities are considered to be activities in carried out in the sphere of administrative law, while investigative activities are, on the other hand, an element of procedural activities that are carried out in the domain of criminal proceedings.[33] Moreover, intelligence gathering activities are not followed by any coercive measures translating into a legal obligation to take part in such activities (or to provide information), which is an immanent feature of investigative activities. Finally, as far as the legislative aspects are concerned, investigative activities are governed by the provisions of the Code of Criminal Proceedings while the intelligence gathering activities stem from the legal provisions defining the powers and scope of competence of the respective services. These distinctions thus make it quite easy to separate intelligence gathering activities from investigative activities.

On the other hand:

> the scope of the concept of administrative activities has not been regulated by the Act of 6 April 1990 on the Police[34] but, contrary to the name, other tasks of law enforcement bodies, apart from purely administrative ones, are also performed within their framework. Undoubtedly, administrative activities include explanatory activities in misdemeanour cases, which perform the detection and evidential function.[35]

Thus, the borderline between intelligence gathering activities and administrative-order activities must be analysed each time, taking into account the manner in which a given – specific – activity is performed.

---

[33] Cf. M. Rudnicka, *Ogólna charakterystyka policji jako formacji uzbrojonej i umundurowanej oraz jej wielowymiarowość*, "De Securitate et Defensione. On Security and Defence" 2016, t. 2, nr 2, p. 169.

[34] Journal of Laws 2023, item 171.

[35] A. Taracha, *Kontrola osobista i przeglądanie zawartości bagażu (art. 15 ust. 1 pkt 5 ustawy o Policji) a ochrona konstytucyjnych praw człowieka*, "Prawo w Działaniu. Sprawy Karne" 2020, t. 41, p. 68.

It should also be emphasised that there is no exhaustive catalogue of intelligence gathering activities. Only the most complex types of them, which entail the most far-reaching interference in the sphere of constitutional rights and freedoms, have been regulated in legal statues. These include, inter alia, operational control, controlled purchase, controlled acceptance or presentation of a material benefit, collection and processing of telecommunications data or HUMINT-related activities (cooperation with natural persons providing intelligence to the services). Other types of intelligence gathering activities are regulated by secret internal regulations of individual services, which specify the ways, methods and forms of their performance.[36] In view of the above, only the activities regulated at the statutory level will be subject to further analysis.

In the context of the above observations, turning to the main thread of the considerations concerning the types and scope intelligence gathering activities carried out by law enforcement agencies in the area of combating cybercrime, their delineation must be done, firstly, by specifying the law enforcement agencies responsible for the fight against cybercrime; and secondly, the specific intelligence gathering powers vested in these agencies, the use of which is linked to the fight against cybercrime.

In the first aspect, an analysis of the statutory competence of the Polish law enforcement authorities leads to the conclusion that the key authorities responsible for combating cybercrime in Poland are the Police and the Internal Security Agency (ABW) and, to a lesser extent, the Military Counterintelligence Service. It should be noted that, as far as the abovementioned services are concerned, only the Police is a service of the so-called law enforcement character (whose tasks relate directly to combating crime), while the remaining services belong to the group of intelligence and security services (which primarily gather the information relevant for the neutralisation of potential threats). Hence, the problem of combating cybercrime remains primarily the domain of the Police, and only then the ABW (in the military area the SKW).

[36] Cf. R. Brzozowski, *Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), p. 157.

This inference is underlined by the fact that, according to the Police Act, its basic tasks include, inter alia, initiating and organising activities aimed at preventing the commission of crimes and offences (preventive function), detecting crimes and offences and prosecuting their perpetrators (investigative function). The tasks of the Police, formulated in this way, establish a presumption of its competence in combating crime, including cybercrime – to the exclusion of possible – defined in an enumerative fashion – jurisdiction of other services. The primary role of the Police in combating cybercrime is reinforced by its organisational structure, in which, since 2022 there is the Central Bureau for Combating Cybercrime (CBZC), which is an organisational unit of the Police, responsible for the performing, at the national level, tasks in the field of identifying and combating crimes committed with the use of an IT system, an ICT system or an ICT network, as well as preventing these crimes, as well as detecting and prosecuting the perpetrators of these crimes and supporting, to the necessary extent, the organisational units of the Police in identifying, preventing and combating these crimes.

In turn, the tasks of the ABW are mainly related to the functioning of the national cybersecurity system and tasks in the area of identification, prevention and detection of threats to the security of information and communication systems of public administration bodies or elements of critical infrastructure, which are significant from the point of view of ensuring continuity of the state's functioning. Taking into account its investigative powers, this organ also remains an important element of the system of combating cybercrime, both when the committed offence is related to a breach of the elements of the indicated cybersecurity system, and when the offence is related to offences against state security remaining within its jurisdiction, in particular espionage, terrorism or unlawful disclosure or use of classified information.

Within the framework of intelligence gathering activities, the Commander of the CBZC, under the Act, is vested with powers identical to those of the Commander-in-Chief of the Police or the Commander of the Central Bureau of Investigation of the Police, including: operational control (Article 19 of the Act on the Police), controlled purchase (Article 19a of the Act on the Police), secret

surveillance of production, movement, storage and turnover of objects of crime (Article 19b of the Police Act), obtaining and using information constituting legally protected secrets (Article 20 of the Police Act) and obtaining data not constituting the content of a telecommunication transmission, postal consignment or transmission within the framework of a service provided electronically (Article 20c of the Police Act). The same powers, although different in their scope, correlated with the ABW, are vested in the Head of the ABW (Articles 27–30 and Article 34 of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency).[37]

Turning to the first of these activities, one should start by emphasising that the current regulatory shape of both operational control and the power to obtain telecommunication data is structurally identical for all authorised services, which is a consequence of the uniform implementation in 2016[38] of the Constitutional Court's judgment of 30 July 2014 (ref. K 23/11), which outlined the minimum standards for the statutory regulation of the secret acquisition of information about individuals by public authorities.

Pursuant to this regulation, the operational control is initiated, in the formal sense, by virtue of a decision of a competent district court, upon a written application of a competent Police Commander (including the Commander of the CBZC) or the Head of the ABW, submitted after obtaining a written consent of the Public Prosecutor General. The condition for granting such consent is: firstly, submission of a request concerning one of the enumerated offences (different for the Police and the Internal Security Agency), and secondly, facts and circumstances explaining why other operational measures would prove ineffective or would be useless (which emphasises that the operational control is the measure of last resort as an activity having a strong and far-reaching impact on constitutional rights and civil liberties).

In the case of the Police, the operational control may be ordered, inter alia, in order to prevent, detect and identify perpetrators, as well

[37] Journal of Laws 2023, item 1136.

[38] As of 7 February 2016, by virtue of the Act of 15 January 2016 amending the Police Act and certain other acts (Journal of Laws 2016, item 147).

as obtain and record evidence of intentional criminal offences, prosecuted by public prosecution referred to:

1. in Chapter XXV of the Criminal Code, referred to as "CC" (offences against sexual freedom and morality):
   - Article 200a CC (establishing contact with a minor for the purpose of committing a sexual offence),
   - Article 200b CC (propagation of paedophilic behaviour),
   - the entire catalogue of crimes when the victim is a minor or when the pornographic content referred to in Article 202 CC involves the participation of a minor;
2. in Chapter XXIX of the CC (offences against the activities of state institutions and local self-government) – Article 224a of the CC (false alarm);
3. in Chapter XXXIII of the CC (offences against the protection of information):
   - Article 267 § 1–4 CC (both § 1 concerning unlawful acquisition of information, so-called "computer hacking", and § 2 concerning computer eavesdropping, so-called "sniffing"),
   - Article 268a § 1 and 2 CC (thwarting access to computer data),
   - Article 269 KK (damage to computer data; so-called computer sabotage),
   - Article 269a CC (interference with computer system),
   - Article 269b § 1 KK (manufacture of hacking tools);
4. in Chapter XXXV of the CC (offences against property).
   - Article 279(1) CC (burglary, particularly in the context of cash held in bank accounts).
   - Article 285 § 1 CC (activation of telephone impulses).
   - Article 287 § 1 KK (computer fraud; so-called phishing);
5. in Chapter XXXVI of the CC (offences against economic turnover and property interests in civil law transactions) – Article 299 of the CC (money laundering).

In this context, the scope of application of operational control carried out by the ABW, includes, as regards offences which may be committed with the use of ICT methods and means, the offence of unlawful disclosure or use of classified information (Article 265 KK

and Article 266 KK), espionage (Article 130 KK), terrorism (Article 115 § 20 of the CC) and the catalogue of offences covered by Chapters XXXV of the CC (offences against property), XXXVI of the CC (offences against economic turnover and property interests in civil law transactions – including, inter alia, Article 270 of the CC, i.e., theft of funds, or Article 287 of the CC, i.e., computer fraud) and XXXVII of the CC (offences against trading in money and securities) – with the express proviso that they must harm the economic foundations of the state.

Pursuant to Article 19(3) of the Police Act (Article 27(6) of the ABW and AW Act), the operational control is conducted in secret and consists of:

1. obtaining and recording the content of conversations conducted by technical means, including through telecommunications networks,
2. obtaining and recording images or sound of persons from premises, transportation means or places other than public places,
3. obtaining and recording the content of correspondence, including electronic correspondence,
4. obtaining and recording data contained in computer storage media, telecommunications terminal equipment, information and communication technology systems,
5. gaining access to and controlling the contents of deliveries.

The right to carry out the operational control is mutually correlated with the obligation on the part of a telecommunications entrepreneur, postal operator and service provider providing electronic services to ensure, at their own expense, technical and organisational conditions allowing for carrying out such control (Article 19(12) of the Police Act and Article 27(12) of the ABW and AW Act). Importantly, these obligations are further specified, with regard to the telecommunications entrepreneur in Article 179 of the Act of 16 July 2004. Telecommunications Law[39] and the postal operator in Article 82 of the Act of 23 November 2012 Postal Law.[40] However,

[39] Journal of Laws 2022, item 1648.
[40] Journal of Laws 2022, item 896.

such obligations are not specified with regard to a service provider providing services by electronic means, in the Act of 18 July 2002 on the provision of services by electronic means.[41]

The indicated provisions do not specify the technical aspects of the application of the operational control, which seems to be a conscious will of the legislator, leaving this issue to the services, ensuring the flexibility of their actions in conditions of technological variability. On the other hand, the services are under a legal obligation to protect the means, forms and methods of their operations (Article 20a(1) of the Police Act, Article 35(1) of the ABW and AW Act), "therefore the technical issues related to the implementation of eavesdropping are not the subject of the application for ordering operational control".[42] Therefore, in the Polish legal system, it is not required to directly grant the services the right to use, for example, software called "state trojans" to break through the security of telephones and computers and read the contents of devices used by persons, as is the case, in inter alia, Germany.[43]

The scope of activities falling under the operational control, in particular including the so-called electronic surveillance, undoubtedly remains the most important and effective tool in the hands of law enforcement agencies aimed at combating cybercrime. Indeed, the detection and prosecution of many types of cybercrime is only possible thanks to the ability of authorised services to monitor electronic means of communication, content delivered electronically or, finally, electronic data itself. These activities may include various levels of "depth" of interference in the rights and freedoms of citizens, including in particular the secrecy of correspondence, ranging from the analysis of messages transmitted via e-mail, instant messaging or by internet chats, to the examination of user activity on social networking platforms or information on the websites followed by the user.

---

[41] Journal of Laws 2020, item 344.

[42] P. Opitek, *Kontrola telefonu za pomocą Pegasusa*, "Legalis online", 21 January 2022, https://legalis.pl/kontrola-telefonu-za-pomoca-pegasusa/ (accessed on: 04.06.2023).

[43] Ibid.

It should be added that the effective application of this activity, mainly due to technological development, encounters numerous difficulties. One of the most frequently mentioned issues in the literature on the subject is, in particular, the problem of cooperation, in the course of carrying out operational control, with foreign (not based in Poland) providers of electronic means of communication. While, they are obliged to provide, at their own expense, technical and organisational conditions enabling operational control on the basis of the aforementioned regulations, in practice cooperation with such providers, in particular those based outside the EU, may be illusory and de facto dependent on their good will (and often their own privacy policies). Access to the content of the communication itself, which is currently encrypted for most communicators, remains a separate issue. As emphasised in the literature, on the one hand, the providers themselves do not have the possibility to decrypt the transmitted messages, on the other hand, the possible imposition of such access by legal regulations would entail the necessity to build into these services the so-called backdoors available to the services, which in turn would undermine the sense of the services provided.[44] Finally, the last problem concerns anonymous activities of web users, mainly in the area of the so-called "Darknet" (also known as the "Dark Web"). It is a hidden area of the World Wide Web, not indexed by standard search engines and requiring access through special tools and software, such as anonymous networks and darknet browsers. It appears that the use of other types of operational and exploratory activities, discussed below, would be appropriate to explore and investigate this area of the web. Access to data itself, increasingly processed in the so-called cloud, also remains an important issue. On the one hand, this data is physically located in different parts of the world, while on the other, it remains secured by extensive encryption technology.

[44] Cf. S. Wikariak, *Coraz więcej inwigilacji ze strony służb? Projektowane przepisy budzą kontrowersje*, "Gazeta Prawna online", 24 January 2023, https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8644248,policja-sluzby-kontrola-operacyjna-inwigilacja-dostep-do-danych-komunikatory.html (accessed on: 04.06.2023).

Incidentally, it should be pointed out that the operational control discussed above (which is one of the intelligence gathering activities) should be distinguished from the so-called procedural surveillance, specified in Article 237 of the Code of Criminal Procedure (which is one of the investigative activities), i.e., control and recording of telephone conversations ordered by the court at the prosecutor's request, after the commencement of criminal proceedings, with the aim of detecting and obtaining evidence for the ongoing proceedings or preventing the commission of a new offence.

One of the intelligent gathering activities different from operational control remains the so-called controlled purchase. Pursuant to Article 19a of the Police Act (Article 29 of the ABW and AW Act), the Police Commissioner (in the case of the ABW – the Head of the ABW), after obtaining a written consent of the competent regional public prosecutor (in the case of the ABW – the Public Prosecutor General) may order, for a specified period of time, that activities aimed at verifying previously obtained reliable information on a crime and establishing perpetrators and obtaining evidence of a crime, consisting in the secret acquisition, disposal or seizure of objects originating from a criminal offence, subject to forfeiture, or the manufacture, possession, transportation or circulation of which is prohibited, as well as the acceptance or presentation of a material benefit and the submission of an offer in the indicated scope, be carried out. This activity is referred to as "the controlled purchase" or police provocation. Although the original purpose of this activity was to infiltrate criminal gangs dealing in illegal goods, in particular drugs, alcohol, cigarettes, but also firearms or explosives, there would be no obstacle to its current use to combat cybercrime through, for example, the controlled purchase of copyright-infringing digital goods in the form of illegal software, films, music or e-books, but also stolen confidential data or hacking tools, or even "services" related to cyber attacks. However, while, in the current state of the law, the use of operational control and controlled purchase is possible against the offences specified in Article 267 § 1 KK (computer hacking) or Article 269b § 1 KK (production of hacking tools), these tools may not be used with regard to crimes under Articles 115–117 of the Act of 4 February

1994 on copyright and related rights,[45] i.e., crimes of intellectual theft, due to the fact that they have not been entered into the catalogue specified in Article 19, paragraph 1 of the Police Act. It is reasonable to consider the appropriate amendments in this respect.

Another statutory intelligence gathering activity is the so-called controlled delivery. Pursuant to Article 19b of the Police Act (Article 30 of the ABW and AW Act), the relevant Police Commander (in the case of the ABW – the Head of the ABW), may order secret surveillance of the production, movement, storage and trade in objects of an offence, if this does not create a threat to human life or health. The competent prosecutor (in the case of the ABW – the Prosecutor General) shall be notified immediately that such activities have been initiated. The ABW and AW Act emphasises that this activity, which is always ordered prior to the initiation of criminal proceedings, is intended to document offences falling within the scope of competence of the ABW or to establish the identity of persons participating in them or to seize objects of offences. In practice, this activity consists of deliberately failing to intervene or refraining from immediately arresting a suspect in order to allow further collection of information on criminal activities and identification of other persons related to the crime. Through this activity, a law enforcement agency can supervise or observe criminal suspects, acting in an undercover manner, in order to gain more information and collect evidence of their activities. Covert surveillance may include tracking the movement of criminal items, such as tracking shipments, cars or containers to identify individuals and groups associated with the crime. It may also include the observation of places where items of crime are stored, produced or traded in order to identify suspects and collect evidence of their activities. If carried out effectively, these activities make it possible to identify entire criminal networks and apprehend key individuals responsible for the crime. Traditionally, therefore, this activity has been used to combat traditional forms of crime, mainly organised crime such as drug trafficking. Its use against cybercrime is a more complex issue and, as it seems, practically limited, due to the specific nature

[45] Journal of Laws 2022, item 2509.

of criminal activities in the online environment. This is because, for the most part, cybercriminals, using technological safeguards such as VPNs, operate anonymously, effectively concealing their identities. Moreover, some forms of cybercrime, such as hacking attacks, among others, can be difficult to monitor in real time. However, despite these difficulties, its application in some aspects of fighting cybercrime seems possible, e.g., by creating an appearance that an undercover operative or officer is interested in purchasing certain digital goods on online forums or darknets, in order to gain information on the trafficking of illegal software, data theft or hacking tools. Such activities could also include monitoring criminal activities in cyberspace, such as harassment or blackmail, in order to identify their perpetrators. Despite the actual possibilities, the technical side of these activities will remain a challenge, related not only to having the right skills and tools, but also to working with digital service providers to obtain the necessary information and technical support.

Based on Article 20c of the Police Act (Article 28 of the ABW and AW Act), both the Police and the ABW are entitled to obtain and process data, without the knowledge and consent of the data subject, not constituting the content of, respectively, a telecommunication transmission, a postal consignment or a transmission within an electronically provided service, as defined in:

1. Article 180c and Article 180d of the Telecommunications Act, referred to as "telecommunications data", comprising:
   a) the so-called billing records, i.e. data identifying the network termination point, the telecommunications terminal equipment and the end user originating the call and to whom the call is directed (identifying the date and time of the call, its duration, type of call, location of the telecommunications terminal equipment),
   b) other telecommunications data:
      - covered by telecommunications secrecy in terms of: user data, transmission data, location data, data on attempts to connect between network terminations;
      - processed with the consent of the user who is an individual, other data of that user in connection with

the service provided, in particular bank account or payment card numbers, as well as contact telephone numbers,
- a list of subscribers, users or network termination points, taking into account the data obtained at the conclusion of the contract;

2. Article 82 item 1 point 1 of the Postal Law Act, referred to as "postal data", including data on postal operator, provided postal services and information enabling identification of users of these services;
3. Article 18(1) to (5) of the Provision of Services by Electronic Means Act referred to as "online data", including the surname and forename of the service recipient, PESEL number (or other identity document), permanent residence address, correspondence address and data used to verify the service recipient's electronic signature.

The analysed activity, along with the operational control, is a key tool used to combat cybercrime. Moreover, due to the simplified – in comparison to the operational control – mode of obtaining telecommunication, postal and Internet data, it makes it an essential tool in this area. In particular, is an effective tool in the domain of identifying suspicious activity, enabling the linkage of the individual digital traces provided by such data, leading to the identification of cybercrime perpetrators. In addition, a broader analysis of this data, identifying patterns and anomalies in the use of telecommunications services, can raise suspicion that a cybercrime of particular type has been committed, essentially computer fraud (e.g., a large number of calls or messages may indicate use of bots or other automated tools used by fraudsters) or sexual fraud (e.g., the identification of specific communication patterns may lead to the identification of sexual offenders, in particular grooming or the distribution of child pornography).

It should also be borne in mind that the activities discussed above, consisting in obtaining data at the pre-trial stage, should be distinguished from the instrument of obtaining and securing computer data at the pre-trial stage, as an investigative power provided for in Article 217 of the Code of Criminal Procedure

in conjunction with Article 236a of the Code of Criminal Procedure or 218a of the Code of Criminal Procedure.

It should also be noted that a fundamental political and legal debate is currently taking place around this activity, specifically the scope of telecommunications data collected by operators, at both the European Union and national level. On the one hand, the Court of Justice of the European Union, in a number of rulings questioned the universal, generalised and undifferentiated obligation to retain all traffic and location data of all subscribers and registered users, of all means of electronic communication. Furthermore, in the CJEU's view, access by the competent authorities to the stored data should be subject to prior control by a court or an independent administrative authority. On the other hand, it is pointed out that currently retention obligations are not covered by electronic communication providers (e.g., providers of e-mail and instant messaging services), which creates a significant information gap in this respect. Amendments in this respect were proposed by the Polish legislator in the draft Law on Electronic Communications, which was met with a negative reaction of both public administration bodies (e.g., the Minister for European Union Affairs) and publicists and representatives of social organisations.[46]

In the context of these considerations, it should be added that according to Article 20 of the Police Act (Article 34 of the ABW and AW Act), the Police may process information, including personal data, to the extent necessary for the performance of its statutory tasks. The personal data processed in accordance with this provision may also include information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and include genetic and biometric data for the purpose of uniquely identifying a natural person or data concerning a person's health, sexuality or sexual orientation.

[46] Cf. A. Obem, *Polski rząd wdraża prawo unijne… niezgodnie z prawem unijnym. Służby dostaną więcej danych*, Panoptykon Foundation website, https://panoptykon.org/wiadomosc/pke-prawo-komunikacji-elektronicznej-sluzby-retencja-danych (accessed on: 05.06.2023).

The so-called camouflage, set out in Article 20a of the Police Act (Article 35 of the ABW and AW Act), on the basis of which the Police officers (or, respectively, the ABW officers), while performing intelligence gathering activities, may use public documents or other documents which make it impossible to establish the identification data of a police officer and the means he/she uses to perform the official tasks, constitutes an important instrument supporting the intelligence gathering activities analysed above.

6.4. International Information and Operational Cooperation in the Fight Against Cybercrime

This section considers international cooperation between services, particularly within the European Union, when carrying out pre-trial activities. This cooperation is of fundamental importance in the case of the fight against cyber threats and cybercrime, which are characterised by their cross-border nature.[47]

In this respect, both the Police and the Internal Security Agency are entitled to conduct such cooperation, while its character, resulting from the legal construction, is shaped differently in both services. Pursuant to Article 1(2)(7) of the Police Act, one of the tasks of this service is cooperation with the police of other countries and their international organisations, as well as with bodies and institutions of the European Union on the basis of international agreements and arrangements and separate regulations. In turn, in accordance with Article 8 of the Act on the ABW and AW, the service may undertake cooperation with competent authorities and services of other states, which may take place after obtaining the consent of the Prime Minister.[48] The regulation of the powers of international cooperation of the Police and the ABW, different

[47] The considerations do not include the issue of international procedural cooperation, regulated, inter alia, by the Council of Europe Convention on Cybercrime (OJ EU L 2015, No. 728).

[48] The MP's bill to amend the Act - Criminal Code and certain other acts (print No. 3232) envisages extending the cooperation in question to include an 'international organisation'.

in mode and scope, results from two basic assumptions. In the case of law enforcement services, the need for international cooperation is obvious from the perspective of tasks related to combating crime and results from international obligations. Moreover, it takes place openly and in an institutionalised manner, as exemplified by police cooperation within organisations such as Interpol or Europol. This is not the case, however, with the intelligence and security services, which, as state bodies carrying out information-oriented, and thus by definition secret, activities aimed at protecting the interests of the state, including against the actions of other states. This necessitates a cautious and formalised approach to international cooperation. As it seems, these factors provided the rationale for the introduction of an additional supervisory measure in the form of a consent of the political level conditioning the undertaking of such cooperation by the ABW.[49]

The international cooperation, from the perspective of the many actors involved in this process, can take the form of multilateral (multilateral) or bilateral (bilateral) cooperation.

Multilateral cooperation is mainly conducted under multilateral international treaties, mainly by international organisations, with a clear formal definition of the mandate, objectives and principles of operation, organisational structures and sources of funding. In this context, from the perspective of obtaining information on cyber threats and cybercrime, cooperation within the European Cybercrime Centre (EC3) and within ENISA becomes particularly important for the Polish services. Importantly, as indicated earlier, both the NIS Directive[50] and the NIS Directive 2,[51] explicitly assumed the necessity of the coordination of activities between competent authorities and law enforcement agencies from various EU Member States, using the organisations mentioned above.

[49] Cf. M. Kamiński, *Prawne aspekty współpracy międzynarodowej służb specjalnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, P. Burczaniuk (red.), Warszawa 2021, pp. 182–183 and 194.

[50] Cf. Recital 62.

[51] Cf. Recital 110.

EC3 was established by the European Union in 2013 as part of the structures of the European Union Agency for Law Enforcement Cooperation (Europol),[52] to coordinate the fight against cybercrime in the EU, as well as to develop cybercrime tools and training and training materials. The Centre offers operational, strategic, analytical and forensic support to investigations carried out by Member States. In this way, the EC3 has four core functions:

1. serves as the European contact point for information on cybercrime,
2. brings together the expertise on cybercrime available in Europe to build the capacity of Member States to combat this phenomenon,
3. supports national cybercrime investigations,
4. provides law enforcement and judicial services with a collective voice in cybercrime investigations carried out in Europe.

As far as organisational details are concerned, EC3 comprises two divisions:

1. Operations (EC3-Operations), which includes task forces focused on detecting and monitoring criminal activities in areas such as online child sexual abuse, online fraud and cybercrimes against critical infrastructure and key information systems within the EU.
2. management (EC3-Management), which is responsible for the administration of the centre, external contacts and operational support, the development of an operational strategy, as well as the development of investigative skills.[53]

The quality of the EC3's operational activities is directly conditioned by the direct involvement of the Member States and the extent of the data they provide.

As regards strategic aspects, a key role is played by a report entitled EU Serious and Organised Crime Threat Assessment (SOCTA),

[52] Communication from the Commission to the Council and the European Parliament tackling crime in our digital age: establishing a European Cybercrime Centre (COM (2012) 0140 final).

[53] Cf. T. Safjański, *Taktyczno-kryminalistyczne aspekty działania Europejskiego Centrum ds. Walki z Cyberprzestępczością*, "Przegląd Policyjny" 2016, nr 2(122), p. 118.

which is prepared on the basis of national risk assessments that are forwarded to Europol by the Member States.

As far as the exchange of information on cybercrime is concerned, the EC3 uses a dedicated online cybercrime reporting system for this purpose as well as collects information on cybercrime from a wide variety of sources, both public and private. The centre collects information on the activities of cybercriminals, the methods they use, as well as on people suspected of cybercrime. The centre facilitates networking between law enforcement agencies, Computer Emergency Response Teams (CERTs) and private sector ICT security professionals. Importantly, the EC3 provides a focal point for the exchange of information not only between member states, but also with third countries (it has, among other things, a well-developed cooperation with the FBI).

It should be added that in 2014, the EC3 established the Joint Cybercrime Action Taskforce (J-CAT), consisting of a permanent operational team of cyber liaison officers from several EU Member States (including the Polish Police) and non-EU partners.[54] The team conducts intelligence-driven coordinated action against key cybercrime threats and targets by facilitating joint identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by partners. J-CAT's jurisdiction includes cybernetic crime (understood as crimes that use electronic and digital technology to attack computers or computer networks), international payment fraud, online child sexual exploitation and aiding and abetting cybercrime (bulletproof hosting, anti-virus services, criminal use of the darknet, etc.).

In conclusion, it can be pointed out that the EC3 acts as a kind of European "back office" coordinating and supporting national police authorities in their tasks of fighting cybercrime.

In contrast, the European Union Agency for Cybersecurity (ENISA) has a different role as the core element of the European cybersecurity system. It was established in 2004 as the European Network and Information Security Agency (ENISA) under Regulation

[54] As of 20 June 2023, it includes 12 EU Member States and 7 non-EU partner countries.

(EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004,[55] with its headquarters in Athens. The latest reorganisation of ENISA, including the change of its name to its current name, took place in 2019 on the basis of the Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019.[56] Article 3 of this Regulation equipped ENISA with a mandate to carry out tasks with a view to achieving a high common level of cybersecurity across the Union, including by actively supporting the Union's Member States, institutions, bodies, authorities and entities in improving cybersecurity. This objective is to be achieved mainly through the provision of expertise, technical support and coordination between Member States. According to the fifth objective, covered by Article 4 of the said Regulation, ENISA promotes cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies and relevant public and private sector stakeholders on issues related to cybersecurity. In this way, it effectively acts as a platform for information sharing and coordination between EU Member States in the event of major cyber incidents. On 27 June 2019, ENISA's statutory body became the Network of National Liaison Officers (NLOs), whose role is to facilitate the exchange of information between ENISA and Member States and to support ENISA in disseminating its activities, findings and recommendations to relevant stakeholders across the Union. With respect to the Polish institutional architecture, the role of the contact point is performed by the director of the CSIRT division of NASK. Importantly, ENISA's new task, in line with the NIS 2 directive, will be to prepare a publicly available database of publicly known vulnerabilities.

As far as the exchange of information within the cybersecurity system is concerned, in addition to ENISA, whose role in this regard is paramount, it is also important to remember:

[55] Its mandate was successively renewed by EU regulations in 2008, 2011 and 2013.

[56] OJ EU L 2019, No. 151, p. 15.

1. The Horizontal Working Party on Cyber Issues (HWPCI), which provides strategic coordination of cybersecurity issues in the EU Council.
2. The NIS Cooperation Group, established by the European Commission's Executive Decision of 1 February 2017 in relation to the implementation of the NIS Directive, whose mission is to support efforts to achieve a high common level of network and information security within the EU. The group consists of representatives of EU Member States, the European Commission and ENISA. Poland is represented by the minister responsible for information technology.
3. The CSIRT network, established under the provisions of the NIS Directive, is responsible for international cooperation at the operational level. The network consists of national CSIRT units. Poland is represented in it by CERT Polska.
4. The European Cyber Security Organisation (ECSO), established in June 2016 to facilitate contractual public-private partnerships in cyberspace between the private sector, the European Commission and the public administrations of the Member States.
5. The Central European Platform for Cybersecurity (CECSP), a regional forum which includes representatives from the Visegrad Group (V4) countries and Austria; the CECSP is where, among other things, cybersecurity strategies are reviewed and the current implementation of the NIS Directive is discussed.

With regard to bilateral cooperation, it should be pointed out that it is mainly based on bilateral international agreements. In accordance with the legal doctrine, such agreements make it possible to regulate in detail the cooperation of authorities and institutions of two countries that have common interests in a given area. In the context of the considerations covered in this chapter, agreements on cooperation in combating crime are of particular importance. They regulate the cooperation of authorities at the pre-trial stage (procedural cooperation is regulated by separate agreements on mutual assistance in criminal matters). An essential element of such agreements is the specification of the catalogue of crimes,

in combating which, the parties to the agreement plan to cooperate In turn, the purpose of these agreements is usually to enable the exchange of information between the authorities of both parties, authorised to combat such offences, indicated in the agreement. However, they often also regulate various forms of operational cooperation, such as covert surveillance or undercover operations. Currently, Poland has concluded 41 such agreements.[57]

An important area of bilateral international cooperation is direct operational and information cooperation between the services, based mainly on mutual trust and common interests.

6.5. Conclusions

The considerations presented in this chapter lead to the fundamental conclusion of the need to consolidate, both at the legislative and practical level, activities aimed at securing cyberspace. It is evident that, both at the level of European and national legislation and at the level of the tasks of services and entities responsible for such security, there is a line of demarcation separating preventive activities (the area of cybersecurity) from information activities aimed at combating threats, to procedural activities strictly related to the fight against cybercrime. This boundary exists not only in the area of doctrinal considerations, but translates directly into the tasks and powers granted to the services in individual areas and entities responsible for them. These tasks and powers are not accompanied by clearly defined coordination rules and cooperation mechanisms. This is all the more incomprehensible in view of the fact that these entities serve to ensure a single cybernetic security, with the only distinction being that their tasks concentrate on its individual phases.

This comprehensive view should be adopted, by both the European and national legislator, in the numerous drafts of normative acts aimed at raising the level of cybersecurity currently under way. An essential part of these considerations should be to coordinate

[57] Internetowa Baza Traktatowa Ministerstwa Spraw Zagranicznych, https://traktaty.msz.gov.pl/umowa-1 (accessed on: 22.06.2023).

the actions of those responsible for these various phases and to implement elements to facilitate cooperation, including in particular cross-border information exchange and actual cooperation in the case where specific security incidents occur.

REFERENCES

Act of 6 April 1990 on the Police (Journal of Laws 2023, item 171).

Act of 4 February 1994 on copyright and related rights (Journal of Laws 2022, item 2509).

Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (Journal of Laws 2023, item 1136).

Act of 18 July 2002 on the provision of services by electronic means (Journal of Laws 2020, item 344).

Act of 16 July 2004. Telecommunications Law (Journal of Laws 2022, item 1648).

Act of 23 November 2012. Postal Law (Journal of Laws 2022, item 896).

Act of 10 June 2016 on anti-terrorist activities (Journal of Laws 2022, item 2632).

Brzozowski, R., *Czynności wykonywane przez funkcjonariuszy ABW na tle zadań ABW*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, Burczaniuk, P. (red.), Warszawa 2021.

Communication from the Commission to the Council and the European Parliament tackling crime in our digital age: establishing a European Cybercrime Centre (COM (2012) 0140 final).

Czarnecki, P., *Czynności operacyjno-rozpoznawcze a postępowanie karne*, "Palestra" 2014 nr 7–8.

Czeczot, Z., Tomaszewski, T., *Kryminalistyka ogólna*, Toruń 1996.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ EU L 2016, No. 194, p. 1).

Directive (EU) 2016/1148 (OJ EU L 2022, No. 333, p. 80).

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing

Drobek, P., [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Czaplicki, K., Gryszczyńska, A., Szpor, G. (red.), Warszawa 2019, Article 40.

Hanusek, T., *Kryminalistyka. Zarys wykładu*, Kraków 1996.

Hołyst, B., *Kryminalistyka*, Warszawa 2016.

Kamiński, M., *Prawne aspekty współpracy międzynarodowej służb specjalnych*, [in:] *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego*, Burczaniuk, P. (red.), Warszawa 2021.

Nowicki, N., *Normatywne ujęcie czynności operacyjno-rozpoznawczych w aspekcie dowodu nielegalnego*, "Przegląd Bezpieczeństwa Wewnętrznego" 2021, t. 13, nr 24.

Obem, A., *Polski rząd wdraża prawo unijne... niezgodnie z prawem unijnym. Służby dostaną więcej danych*, Panoptykon Foundation website, https://panoptykon.org/wiadomosc/pke-prawo-komunikacji-elektronicznej-sluzby-retencja-danych (accessed on: 05.06.2023).

Opitek, P., *Kontrola telefonu za pomocą Pegasusa*, "Legalis online", 21 January 2022, https://legalis.pl/kontrola-telefonu-za-pomoca-pegasusa/ (accessed on: 04.06.2023).

Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2020 r., Warszawa 2021.

Raport roczny z działalności CERT Polska – Krajobraz bezpieczeństwa polskiego Internetu w 2021 r., Warszawa 2022.

Regulation (EU) No. 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (OJ EU L 2019, No. 151, p. 15).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (OJ EU L 2022, No. 333, p. 1).

Resolution No. 125 of the Council of Ministers of 22 October 2019, which was adopted, remains valid. Cybersecurity Strategy of the Republic of Poland for 2019–2024 (M.P. of 2019, item 1037).

Rudnicka, M., *Ogólna charakterystyka policji jako formacji uzbrojonej i umundurowanej oraz jej wielowymiarowość*, "De Securitate et Defensione. On Security and Defence" 2016, t. 2, nr 2, p. 169.

Safjański, T., *Taktyczno-kryminalistyczne aspekty działania europejskiego centrum ds. Walki z Cyberprzestępczością*, "Przegląd Policyjny" 2016, nr 2(122), p. 118.

Śmiłowicz, P., *Kodeks pracy operacyjnej dla służb*, "Gazeta Prawna online", 26 January 2023, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8646248,kodeks-pracy-operacyjnej-dla-sluzb-ko.html (accessed on: 01.06.2023).

Taracha, A., *Kontrola osobista i przeglądanie zawartości bagażu (art. 15 ust. 1 pkt 5 ustawy o Policji) a ochrona konstytucyjnych praw człowieka*, „Prawo w Działaniu. Sprawy Karne" 2020, t. 41.

Widacki, J. (red.), *Kryminalistyka*, Warszawa 1999.

Wikariak, S., *Coraz więcej inwigilacji ze strony służb? Projektowane przepisy budzą kontrowersje*, "Gazeta Prawna online", 24 January 2023, https://www.gazeta prawna.pl/firma-i-prawo/artykuly/8644248,policja-sluzby-kontrola-operacyjna-inwigilacja-dostep-do-danych-komunikatory.html (accessed on: 04.06.2023).

Wójcik, E., *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, https://wspia.eu/media/oojnsacq/44-w%C3%B3jcik.pdf (acessed on: 01.06.2023).

PROF. DR. ERIKA RÓTH, EGYETEMI TANÁR
University of Miskolc | DOI: 10.32041/9788367149761/7

Chapter 7. Application of Coercive Measures in Cybercrime Cases

7.1. Introduction

A delicate balance must prevail in criminal proceedings. On one side of the scale is the interest in the effectiveness of criminal proceedings, while on the other are the rights of the participants of the procedure. These rights may be limited in order to ensure the effectiveness of the proceedings, but only if the conditions prescribed by law are met.

The fundamental rights of the suspect/accused can be restricted in several forms in order to ensure the effective completion of investigation and if neccessary that of the court procedure. The most serious limitations are coercive measures, in particular measures restricting personal liberty. A common feature of coercive measures that can be used in criminal proceedings is that they restrict fundamental civil rights, the exercise of rights that are guaranteed by international human rights conventions and the constitutions of individual states. While coercive measures affecting personal liberty may only restrict the rights of the suspect/accused, coercive measures affecting assets may be imposed not only against the suspect, other participants of the proceedings may also be affected.

The rules of coercive measures in the Act XC of 2017 on Code of Criminal Procedure (hereinafter: HCCP) have no difference according to whether they are applied in cases of cybercrime and other criminal cases. The Code distinguishes between coercive

measures affecting personal liberty and assets (property). While in the case of coercive measures affecting personal liberty there are no or only few peculiarities in the area of cybercrime, several specific features can be identified in the case of coercive measures affecting assets. The author of the chapter intends to deal with the latter in detail, especially with the search, seizure and rendering of electronic data temporarily inaccessible. It should be noted here, that in some countries search, seizure and other measures are not part of coercive measures but regulated as security measures or measures connected with evidence.[1]

However, we must also mention briefly the coercive measures affecting personal liberty, since coercive measures restricting right to liberty can play an important role in cybercrime cases as well.

When applying coercive measures, the criteria of necessity, proportionality and gradation must be taken into account. The requirement of gradation is served, for example, by the fact, that coercive measures affecting personal liberty make it possible to achieve the same procedural purpose with different restrictive measures. We can say that these measures are built on each other, since, for example, if the suspect/accused violates the relatively lenient rules of conduct imposed in the framework of criminal supervision, stricter rules of conduct can be imposed on him, or even his detention can be ordered.

According to the HCCP, in Hungarian criminal proceedings coercive measures may be ordered by the court/judge, the public prosecutor and investigating authorities to compel participants of the criminal proceeding to perform their obligations or to refrain from doing something. However, there are some coercive measures that only the court is authorised to order, e.g., pre-trial detention, criminal supervision, rendering electronic data temporarily inaccessible etc.

Coercive measures affecting personal liberty in the Hungarian Code of Criminal Procedure are:

[1] This is the case, for example, in Poland where we can find regulation of search and seizure in the Section V. (Evidence) of the Code of Criminal Procedure, while coercive measures are regulated in Section VI.

a) custody,
b) restraining order,
c) criminal supervision,
d) pre-trial detention, and
e) preliminary compulsory psychiatric treatment.

It is important to mention that custody can be ordered by the court, the public prosecutor and the investigating authority, but the ordering and maintaining of the other coercive measures listed above falls under the jurisdiction of the court, therefore these are called "coercive measures affecting personal liberty subject to judicial permission".

Coercive measures affecting assets are the following:

a) search,
b) body search,
c) seizure,
d) sequestration, and
e) rendering electronic data temporarily inaccessible.

7.2. General Rules for the Application of Coercive Measures

The common feature of coercive measures is that their application means a greater or lesser restriction of fundamental rights of citizens. Therefore, efforts should be made that the use of coercive measures result in a restriction of the fundamental rights of the person concerned only to the extent and for the period of time that is strictly necessary (HCCP 271. § (1) para.). In the case when coercive measures are applied, the principles of gradation and proportionality prevail, which means that a coercive measure with more severe restriction may be ordered, if the purpose of the coercive measure cannot be achieved by a less restrictive coercive measure or other procedural act (HCCP 271. § (2) para.). The coercive measure must be carried out with respect for the fundamental rights of the person concerned, and unnecessary damage should be avoided (HCCP 271. § (3) and (6) para.).

7.3. Coercive Measures Affecting Personal Liberty

Without discussing coercive measures affecting personal liberty in detail, it is necessary to mention their possible inclusion, importance, and role in the fight against cybercrime.

Coercive measures affecting personal liberty subject to judicial permission may be ordered:

a) to ensure the presence of the defendant (to prevent him from escaping or hiding from the authorities),
b) in order to avoid the complication and obstruction of evidence (e.g., if the defendant destroyed, falsified, or hid any physical evidence or electronic data, or there are reasonable grounds to assume that he will do so),
c) to prevent the possibility of reoffending.

In cybercrime cases, where electronic evidence can be very easily modified, deleted or hidden, it is extremely important to prevent the suspect for doing so. Another purpose of ordering a coercive measure may be to prevent reoffending. The suspect may purchase a new device and continue the criminal activity even if the device originally used to commit criminal offence has been seized.

Two coercive measures are appropriate to achieve this aim: pre-trial detention and criminal supervision. If the offence was committed by harassing the person in question on social networking sites, via email messages, SMS or by other similar ways, even the restraining order may be a suitable instrument. When a restraining order is applied, the court shall impose as a rule of conduct that the defendant may not contact, directly or indirectly, and is to stay away from, a person protected by the restraining order (HCCP 280. § (2) para.).

A restraining order may be issued to avoid the complication or obstruction of the taking of evidence, or to eliminate the possibility of reoffending with regard to the victim. Criminal supervision and pre-trial detention may be ordered for all three procedural purposes mentioned above.

7.4. Coercive Measures Affecting Assets

Coercive measures affecting assets may restrict or limit the rights of the person concerned to possess, dispose and use the property its entirety, but may only affect certain elements of the property right (ownership). Thus, if the affected thing remains in the possession of the owner or processor after the compulsory measure has been ordered, he may still be able to use it.

7.4.1. SEARCH

The search restricts the so-called right to a house, the right to inviolability of the private home. Not only the suspect could be the person affected by the search. This coercive measure means a searching of a dwelling, other premises, fenced area or vehicle in order to conduct the criminal proceeding successfully. The search may also include the inspection of an information system or data medium (HCCP 302. § (1) para.). A search may be ordered if it can be reasonable to assume that it leads to:

a) the apprehension of a perpetrator of a criminal offence,
b) the detection of traces of a criminal offence,
c) the discovery of a means of evidence,
d) the discovery of a thing that may be subject to confiscation or forfeiture of assets,
e) the examination of an information system or data medium (HCCP 302. § (1) and (2) para.).

The search may be ordered by the court, public prosecutor or investigating authority except for the case when a search is to be conducted in the offices of a notary public, or in a law office, for the purpose of gaining access to protected data related to the activities of a notary public or a lawyer. This kind of search shall be ordered by a court. In any search conducted in the offices of a notary public, or in a law office, the presence of a prosecutor is obligatory. With his presence the public prosecutor ensures that the coercive measure is lawfully carried out by the investigating authority

within the framework of the court decision (Order of the Prosecutor General No. 9/2018 (VI.29.) 28 § (1) para.).

But even in this case, the search is allowed to be carried out without the court decision if decision-making by the court would cause a delay that would significantly jeopardise the purpose of the search. In such a case the decision of the court must be obtained afterwards without delay. If the search is not ordered by the court, its result cannot be used as evidence.

Special regulations concerning the office of the lawyer are becoming more and more important. With the spread of electronic administration, a significant part of the information related to individual cases is available in electronic form (or in electronic form as well). In addition, communication with clients and other persons involved in a case is increasingly done using IT devices.

If possible, the decision ordering a search shall specify the person, means of evidence, thing that may be subject to confiscation or forfeiture of assets, information system, or data medium to be found during the search (HCCP 304. § (2) para.). The precise, prior definition of the subject of the coercive measure is a guarantee and is of fundamental importance.[2]

If the purpose of the search is to find a specific person, a means of evidence, a thing, an information system or a data medium, the owner, possessor, user of the real estate or vehicle concerned, or the person authorised by that person shall be called upon to disclose the whereabouts of the physical evidence or person sought or to make available the electronic data sought. If the request is complied with, the search may only be continued if it is reasonable to assume that any other means of evidence, thing, information system or data medium may also be found.

Since not all police stations have the necessary means to carry out coercive measures and police staff lack the necessary knowledge on a certain special issue, they often have recourse to external assistance. The external help, the expert or specialist consultant is the person

[2] E. Belovics, M. Tóth, *Büntető eljárásjog*, Budapest 2017, p. 221.

who carries out the tasks on the spot and has the tools that are essential for the successfully executed procedural act.[3]

It is difficult to separate problems of involving expert and coercive measures because in these cases even the execution of coercive measures – such as search and seizure – affecting assets may require special knowledge in the field of informatics. In the HCCP there is no special rule concerning the seizure of electronic devices. This measure can be source of many errors, and improper execution can even lead to the destruction of evidence.

The Government Order containing detailed rules of the investigation prescribes, that during the examination of the information system, it is necessary to ensure that data accessible through the information system – without bypassing or evading protection devices or IT solutions – is also known and recorded, regardless of the location of the data (Government Order No. 100/2018 (VI.8.). According to László Dornfeld, during the search:

> in the information system, examinations are carried out which may not be possible later. For example, if a data is stored in a cloud service and accessible from the system during the search, it is worthwhile to perform the analysis at that time, as later access to the internet may jeopardise the integrity of the data on the data medium.[4]

During the search of IT system, it must be ensured that data accessible through the system remain unchanged during the inspection and recording. "Crucial is the ability to prove that the content presented in court is exactly the same as the one captured during the investigation."[5]

---

[3] B. Simon, R. Gyaraki, *A kiberbűncselekmények felderítése* és *nyomozása*, [in:] T. Kiss (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020, p. 134.

[4] L. Dornfeld, *A kibertérben elkövetett bűncselekményekkel* összefüggésben *alkalmazható kényszerintézkedések*, "Belügyi Szemle" 2018, No. 2, pp. 119–120.

[5] P. Lewulis, *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, p. 42, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

7.4.2. BODY SEARCH

Body search is the search and examination of the clothing and body of a person subject to body search for the purpose of finding a means of evidence or a thing that may be subject to confiscation or forfeiture of assets. In the course of a body search, things found on the searched person may also be inspected. A body search may be ordered against a suspect, a person reasonably suspected of having committed a criminal offence or a person who can reasonably be assumed to be in possession of a means of evidence or a thing that may be subject to confiscation or forfeiture of assets (HCCP 306. § (1)–(2) para.). Of course, the body search can also be aimed at finding cybercrime-related evidence or thing subject to confiscation or forfeiture.

Voluntary performance is also important in the body search. If the body search is aimed at finding a specific thing, the person subject to the body search must be called upon to hand over the thing sought. If the request is fulfilled, body search cannot be continued (HCCP 307. § (1) para.).

7.4.3. SEIZURE

Although the seizure of electronic data is of particular importance from the point of view of cybercrime, we must also deal with the general rules of seizure. We do so because the seizure of electronic data is a special case of seizure and thus the general rules apply even if the seizure of electronic data is necessary in the criminal proceeding.

Seizure is a coercive measure affecting assets that are regulated in very detailed form in the HCCP. This time we limit ourselves to the introduction of the most essential provisions that can be considered fundamental. We must mention that the Code also includes, for example the list of things that cannot be seized, the detailed rules of execution of the seizure, etc. It deals with the special rules of seizure of documents and electronic data and preservation of electronic data, which we will discuss in detail. Finally, the Code also stipulates what can happen to the seized item.

7.4.3.1. *General Rules of Seizure*

As is mentioned above, seizure is one of the coercive measures affecting assets. Seizure restricts the right to a property of a person who suffered it, especially the right to possession. Thus, not only the owner of the thing but also the possessor may be affected.

According to the relevant provisions of the HCCP, the purpose of seizure may be to secure evidence or a thing or asset that may be subject to confiscation or forfeiture in order to ensure the successful conduct of the criminal proceeding (HCCP 308. § (1) para.). A movable thing, money in an account, electronic money, or electronic data may be seized (HCCP 308. § (3) para.).

Although seizure can usually be ordered by the investigating authority and the public prosecutor, only the court can order the seizure of evidence held in a notary public's or lawyer's office containing protected data related to the activities of the notary public or lawyer, similar to what was written concerning the search. However, if the delay resulting from obtaining the court decision would significantly jeopardise the purpose of the seizure, the investigating authority or prosecutor may execute the seizure, but the decision of the court must be obtained without delay. If the court does not order the seizure, the seized evidence must be returned to the person concerned.

The seizure may be carried out by taking possession, by other means securing preservation, by leaving the thing in the possession of the person concerned, but in the case of electronic data, the special method of seizure is defined by the HCCP. In order to execute the seizure, the holder or the handler of the thing or electronic data shall be called upon to disclose the whereabouts of the object or make the electronic data available. If he refuses to comply with the request, the thing or the electronic data can be detected by search or body search (HCCP 312. § (1) para.).

7.4.3.2. *Seizure of Electronic Data and Ordering the Preservation of Electronic Data*

In accordance with the requirements of the Budapest Convention,[6] the Hungarian CCP regulates the seizure of electronic data as a special type of seizure and the ordering of preservation of electronic data (HCCP 315–317). It has to be mentioned that these rules are only relatively new. The seizure of electronic data and ordering to preserve them was also regulated in the former Code of Criminal procedure.[7] The new Code only refined the former rules, but these changes were important.

However, in connection with criminal offences it may be necessary to seize not only the data, but seizure of the device also (laptop, flash drive, mobile phone, etc.) may become necessary. They are seized as physical evidence according to the practise established in relation to "traditional" offences.

Let us review what special rules apply to the seizure of electronic data, in particular the method of seizure. According to the 315. § (1) para. of the HCCP, seizure of electronic data may be carried out by making a copy of the electronic data, by transferring the electronic data, by making a copy of the entire content of the information system or data medium containing it, by seizing the information system or data medium containing it or by any other means provided for by law. The above-mentioned order of methods of seizure means the order of their application:

> If the seizure of electronic data is necessary for the purposes of criminal proceedings, it is not usually necessary to seize the information system (computer, server) or data medium containing the electronic data. The reason for this is that from the point of view of evidence the data itself is relevant, which can be obtained from the information

[6] Convention on Cybercrime (2001, ETS No. 185) adopted by the Committee of Ministers of the Council of Europe at its 109th Session, 8 November 2001 (hereinafter: Convention or Budapest Convention).

[7] See 151 § (2) and 158/A § of the Act XIX of 1998.

> system or data medium containing electronic data in a number of other ways (copying, data transfer).[8]

In some cases, it is not possible to seize the complete computer system due to the nature of the computer system under investigation (e.g., bookkeeper's office) or its technical characteristic (e.g., server room of an internet service provider). In this case the aim may be to obtain targeted data extraction for a specific set of data, which usually takes place in the context of the search of a dwelling or other premises. This may require the involvement of several experts and special equipment.[9]

The special method of seizing electronic data used for payment was first defined in the HCCP currently in force. According to it, the seizure of this special electronic data can also be carried out by performing an operation on the electronic data that prevents the person concerned from disposing of material (property) value expressed by the electronic data (HCCP 315. § (2) para.).

At the beginning of the codification of the current code on Criminal Procedure, Zoltán Szathmáry suggested that a procedural code could be developed that could provide flexible responses to the challenges of the future. To this end, "for the time being, it would be sufficient to lay down basic rules in the Act which could provide basis for regulation adapted to future needs".[10] As we can see, the legislator accepted this solution, and the Code contains only a short, one-sentence provision that does not deal with technical details.

In the case of Bitcoin – as one of the most widespread cryptocurrencies – no other measure than seizure makes sense, because there is no body to enforce the decision of the authorities. The only way to suspend the right to dispose of Bitcoin is to take a coercive measure applied directly against the owner by means of a forced transaction, whereby the Bitcoin to be seized is transferred from the owner's

---

[8] P. Polt (ed.), *Nagykommentár a büntetőeljárásról szóló 2017*, évi XC. törvényhez, Budapest 2018.

[9] See I.Zs. Máté, *A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban,* "Magyar Rendészet" 2014, No. 2, p. 33.

[10] Z. Szathmáry, *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban*, "Magyar Jog" 2015, No. 11, p. 645.

address to the address of the authority.[11] This solution has been introduced in the current rules of criminal procedure. Regarding the seizure of Bitcoin, Viktor Halász notes that to appropriate storage of Bitcoin requires a centralised action by the investigating authority, specifically, the creation of a properly configured official wallet. Thus, the Bitcoin seized during the investigation would be placed is this central wallet.[12]

> In the case of electronic data used for payment, it may be sufficient to prevent the person subject to seizure from using this data for payment. Therefore, in such cases, it is also possible to block the use of electronic data used for payment (either by locking it by entering wrong codes, or by transferring the content of the data to a third-party account, etc.).[13]

Seizure of the information system or data medium containing electronic data may be carried out if:

a) it may be subject to confiscation or forfeiture of assets,
b) it is significant as a means of physical evidence, or
c) it contains a significant volume of electronic data that needs to be examined for the purpose of taking evidence, or the volume of such data cannot be determined in advance (HCCP 315. § (5) para.).

> It is also possible, that there is a suspicion that the data medium also contains data (for example data that has already been deleted) that cannot be seized by simple copying. In such cases the information system (data medium) containing the electronic data may

[11] V. Halász, *A bitcoin mûködése* és *lefoglalása a büntetõeljárásban,* "Belügyi Szemle" 2018, No. 7–8, p. 128.
[12] Ibidem, p. 128.
[13] P. Polt (ed.), *Nagykommentár…*, *op. cit.*

> be seized, as the expert can also extract these deleted (possible encrypted) data from the original device.[14]

The seizure of electronic data shall be carried out in a manner ensuring, if possible, that the electronic data not necessary for the criminal proceeding are not affected by it, or such data are only affected by the seizure for the shortest period possible (HCCP 315. § (4) para.). This rule meets the general requirement of ordering and implementing coercive measures, which means that efforts shall be made to ensure that the application of the coercive measures results in restriction of the fundamental rights of the person concerned only to the extent and for the time strictly necessary (HCCP 271. § (1) para.).

The electronic devices are seized in increasing number and their content is examined by an IT expert. It cannot be said that the seizure of such devices is only recommended for certain types of offence, for example, consider that a mobile phone may contain recordings of relevant events in the form of video or photographs.[15] When electronic devices are seized, their careful packaging and transport are also important from the point of view of the subsequent examination of data, and consequently, the effectiveness of the evidence.[16] When found, if the computer is on, files must not be opened, and the computer must not be turned off without the help of an expert. If the computer is on and the screen is also on, a picture of it must be taken. If it is detected that a deletion program is running, the power must be disconnected immediately.[17] Devices containing digital data must be protected from physical impact and from electric and magnetic fields.[18] The involvement of an expert during a search is not mandatory, the HCCP only makes provision for it. However,

---

[14] Ibidem.

[15] Z. Benedek, *Digitális adatok a helyszínen*, "Belügyi Szemle" 2018, No. 7–8, p. 147.

[16] See Z. Benedek, *Digitális…*, *op. cit*., pp. 149–150. T. Gaál and I.Zs. Máté also draw attention to the importance of packaging. T. Gaál, *A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban*, "Belügyi Szemle" 2018, No. 7–8, p. 30, I.Zs. Máté, *A bizonyítékok…*, *op. cit*., pp. 34–35.

[17] Z. Benedek, *Digitális…*, *op. cit.*, p. 149.

[18] Ibidem, p. 150.

it is useful if an expert is present, as the expert can examine the data medium and electronic devices on the spot. He can also help to decide whether something needs to be seized or not.[19]

7.4.3.3. *Ordering the Preservation of Electronic Data*

The predecessor of the current coercive measure can be found in the Hungarian Code of Criminal Procedure since 1 January 2003. It was incorporated into provisions of the Act XIX of 1998 (the old code of criminal procedure) by the Act I of 2002. Its name was the obligation to preserve data recorded by means of a computer system. It transposed the requirements set out by the Article 16 of the Budapest Convention into domestic legislation. Later the name of the measure was modified (data stored in the information system which means a broader category), but the substance remained unchanged.

The Budapest Convention expressly requires appropriate measures to be taken in order to preserve computer data. In Article 16 it obliges parties to the Convention to adopt measures (legislative or other) to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification (Article 16 para 1. of the Convention). "The measures described in the articles operate only where computer data already exists and is currently being stored."[20]

The preservation of electronic data could be the part of seizure of electronic data. In order to detect or prove a criminal offence, an obligation to preserve electronic data may be ordered. It limits the right of disposal of the electronic data owner, processor and operator. (HCCP 316. § (1) para.):

---

[19] Ibidem, p. 151.

[20] Explanatory Report to the Convention on Cybercrime, point 150.

> Obligation to preserve data can be beneficial to the investigating authority because it does not have to seize information and data medium that are not of interest to it, and also to the subject of the coercive measure, because he can continue to use the data medium and programs (with the exception of the data concerned).[21]

The investigating authority, the public prosecutor or the court may order the preservation of electronic data if it is necessary to:

a) detect a means of evidence,
b) secure a means of evidence, or
c) determine the identity or actual place of residence of a suspect (HCCP 316. § (3) para.).

The person obliged to preserve electronic data is obliged to keep the electronic data specified in the decision unchanged and provide secure storage for these data separately from other data files if necessary; to prevent the modification, deletion, destruction, transfer, unauthorised copying of electronic data and unauthorised access to it. In other words, it means, that after the decision has been delivered, the person obliged to preserve the data must ensure that neither he nor anyone else changes the data (HCCP 316. § (4) para.).

The preservation of electronic data in the original location can significantly hinder the data subject's activities related to the possessing, handling, storage or transmission of electronic data. In this case the HCCP 316. § (6) para. provides another possibility:

> At the request of the person obliged to preserve data, it can also be ordered that he does not have to physically store the given electronic data where the authority found it, but to make a copy of the electronic data and keep it. In such cases the person obliged to preserve the electronic data can even change the original data (if the decision so allows).[22]

[21] F. Tóth, *Az informatikai bűnözéshez kapcsolódó kényszerintézkedések*, "Büntetőjogi Szemle" 2017, No. 1, p. 79.
[22] P. Polt (ed.), *Nagykommentár…*, *op. cit.*

If, despite the best efforts of the person obliged to preserve electronic data, the data are assessed (modified, deleted, destroyed, transferred, copied, accessed without authorisation, or any attempt to do so is detected), he must immediately inform the authority ordering the preservation of electronic data (HCCP 316. § (8) para.).

Since the purpose of the ordering this measure is to preserve data that may be important from the point of view of the detection or evidence in an unchanged state, after the order is issued, the authority that ordered it shall start the examination of electronic data. As the result of such examination, the authority shall decide whether to order the seizure to be enforced in another way or terminates the preservation.

The fundamental difference between a seizure and the obligation to preserve electronic data is correctly summarised by Fanni Tóth: While in the case of the preservation order the investigating authority can only examine the data, the seizure is used to secure the evidence.[23]

The preservation obligation lasts for a maximum of three months.

7.4.4. SEQUESTRATION

On the one hand, the sequestration serves the interest of the state, which manifests itself in the confiscation of assets, and on the other hand serves the private party's claims for the compensation.[24] While seizure limits the right to possession, the sequestration restricts the right to dispose of the property.

Sequestration means the suspension of a right of disposal over the sequestrated thing for the purpose of securing the confiscation of assets or a civil claim (HCCP 324. § (1) para.).

In general, we can say that in the field of cybercrime, seizures ordered for the purpose of finding and preserving evidence are much more important and much more frequent. There are two cases

[23] F. Tóth, *Az informatikai…*, *op. cit.,* p. 78.
[24] E. Belovics, M. Tóth, *Büntető…*, *op. cit*., p. 230.

when the legislator allows the sequestration to be ordered: when it is necessary for the forfeiture of property or to satisfy a civil claim.

The Code allows ordering sequestration regarding assets, providing a detailed list of items of property concerned, e.g., thing, money in an account, electronic money, right of pecuniary nature, claim of pecuniary nature, etc. (HCCP 324. § (2) para.).

Sequestration may be ordered if:

a) a proceeding is conducted because of a criminal offence with regard to which the forfeiture of assets may be ordered, or
b) its purpose is to secure a civil claim,

and it is reasonable to assume that enforcing the forfeiture of assets, or satisfying the civil claim, would be frustrated (HCCP 324. § (3) para.).

Sequestration may be ordered by the court, the prosecution service, or the investigating authority, but in some cases defined by the Code only the court is authorised to order it even before the indictment (HCCP 327. § (1)–(2) para.). If the obtaining the decision of the court would significantly jeopardise the purpose of sequestration, the prosecution service or an investigating authority may order the sequestration until the court decision is adopted. In such a situation, the permission of the court shall be obtained ex-post without delay (HCCP 327. § (5) para.).

7.4.5. RENDERING ELECTRONIC DATA TEMPORARILY INACCESSIBLE

The introduction of the measure called "rendering electronic data irreversibly inaccessible" into the Criminal Code and the insertion of coercive measure enabling the temporarily inaccessibility of electronic data into the Code of Criminal Procedure – as it was already analysed by several authors[25] dealing with the topic and

[25] See, for example, F. Tóth, *Az informatikai…*, *op. cit*., pp. 80–81.; T. Gaiderné Hartmann, *Elektronikus adatok ideiglenes* és *végleges hozzáférhetetlenné tétele – egy* új *intézmény első* évei, "Magyar Jog" 2015, No. 2, pp. 106–107; L. Dornfeld, *A kibertérben…*, *op. cit*., pp. 129–130.

as it is written in the reasoning of the given acts – was primarily required by the obligation stemming from the Directive 2011/93/EU.

The coercive measure was introduced in the Code of Criminal Procedure in connection with the entry into force of the Criminal Code. It was a logical legislative step to have a procedural counterpart of the criminal measure to prevent access to illegal content. At the same time, it raised a number of problems in practice, which were also pointed out by László Dornfeld in his study.[26]

In order to understand the purpose of this coercive measure, we need to have a look at the parallel measure of the Criminal Code. According to the 77. § (1) para. of the Criminal Code, data disclosed through an electronic communications network shall be rendered irreversibly inaccessible:

a) if the publication or disclosure of which constitutes a criminal offence,
b) if said data are actually used as an instrument for the commission of a criminal act, or
c) if said data are created by way of a criminal act.

The conditions for the application of the given coercive measure in the HCCP are thus aligned with the applicability of the measure prescribed in the Criminal Code. In addition, however, two further criteria can be derived from the provision of the HCCP. Rendering electronic data temporarily inaccessible may be ordered where a proceeding is conducted regarding a criminal offence subject to public prosecution, in connection with which rendering electronic data permanently inaccessible may be ordered, and doing so is necessary to interrupt the criminal offence.

Rendering electronic data temporarily inaccessible restricts the right to dispose of data published via an electronic communications network.

It may be ordered in the form of:

a) temporarily removing the electronic data concerned, or
b) temporarily preventing access to the electronic data concerned.

[26] See L. Dornfeld, *A kibertérben…*, *op. cit.*, pp. 130–133.

Removing electronic data temporarily means that service provider that processes the electronic data concerned shall be ordered to temporarily remove the electronic data (HCCP 336. § (1) para.). In the second case (point b) the court may order an electronic communications service provider to prevent access to electronic data temporarily (HCCP 337. § (2) para.). The enforcement of this coercive measure is organized and controlled by the National Media and Communications Authority (HCCP 337. § (3) para.).

The temporarily removing the electronic data is the primary solution, in the event of its ineffectiveness, access may be temporarily blocked, provided that the procedure is in progress due to the crimes listed in the HCCP.

In addition, the legislator also created the possibility for the prosecutor or the investigating authority to call on the service provider capable of preventing access to electronic data to voluntarily remove electronic data, provided that this doesn't harm the interests of the criminal proceeding. The purpose of this provision is to ensure that the content that violates criminal law is only available for the shortest possible time.[27]

7.5. *The Lege Ferenda* Proposals

We do not wish for, and cannot formulate, proposals for specific legislative amendments, since to formulate it we would need to have a much better understanding of Polish procedural rules and law enforcement practice.

In relation to cybercrime, it can be said in general, that due to rapid technical development, substantive and procedural rules that should be timeless quickly become out-of-date. Frequent amendments of rules can cause a breakdown in coherence.

The task of the legislator is to remedy the problems arising in the application of the law if the applicability of the rules is called into question. In doing so it is necessary to cooperate with practitioners, and where appropriate, not only with lawyers.

[27] I. Lajtár, *A kíberbűnözésről*, "Ügyészek Lapja" 2019, No. 1, p. 50.

The full implementation of EU legislation is extremely important in the fight against cybercrime.

The legislator must also be open to adopting solutions and good practices already tried and tested in other countries.

7.6. Conclusion

Rules of criminal procedural codes and law enforcement practice must meet double requirement: to ensure effectiveness of criminal justice and to protect and respect human rights of participants, among others fundamental rights of the suspect/accused.

In the proceedings due to cybercrimes, law enforcement authorities, in particular the investigating authorities, have to deal with particular difficulties. The easy alteration of data, the possibility of encryption and the difficulty of identifying the perpetrator can easily encourage the authorities to circumvent the legal rules to a certain extent and try to obtain evidence. Thus, the requirement of efficiency could precede the respect for fundamental rights. However, this should not be allowed to happen.

Successful execution of search or seizure in the case of cybercrimes requires special expertise. Therefore, it is very important to involve IT experts in the performance of these procedural acts. It is almost impossible to correct errors or shortcomings in this area at a later stage. "(…) even the best legislation on coercive measures is not enough if the investigatory authorities lack the competence, tool, methods, and resources needed to investigate cybercrime and to collect relevant evidence."[28]

Although certain coercive measures affecting assets (e.g., search, seizure) are of paramount importance in the case of cybercrimes, it should not be forgotten that other coercive measures can also play a role in ensuring the effectiveness of evidence or preventing reoffending (e.g., pre-trial detention, criminal supervision or restraining order).

[28] J. Riekkinen, *Evidence of cybercrime and coercive measures in Finland*, p. 16, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

REFERENCES

Belovics, E., Tóth, M., *Büntető eljárásjog*, Budapest 2017.

Benedek, Z., *Digitális adatok a helyszínen*, "Belügyi Szemle" 2018, No. 7–8.

Dornfeld, L., *A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések*, "Belügyi Szemle" 2018, No. 2.

Gaál, T., *A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban*, "Belügyi Szemle" 2018, No. 7–8.

Gaiderné Hartmann, T., *Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei*, "Magyar Jog" 2015, No. 2.

Halász, V., *A bitcoin mûködése és lefoglalása a büntetõeljárásban*, "Belügyi Szemle" 2018, No. 7–8.

Lajtár, I., *A kíberbűnözésről*, "Ügyészek Lapja" 2019, No. 1.

Lewulis, P., *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

Máté, I.Zs., *A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban*, "Magyar Rendészet" 2014, No. 2.

Polt, P. (ed.), *Nagykommentár a büntetőeljárásról szóló 2017. évi XC. törvényhez*, Budapest 2018.

Riekkinen, J., *Evidence of cybercrime and coercive measures in Finland*, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

Simon, B., Gyaraki, R., *A kiberbűncselekmények felderítése és nyomozása*, [in]: Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020.

Szathmáry, Z., *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban*, "Magyar Jog" 2015, No. 11.

Tóth, F., *Az informatikai bűnözéshez kapcsolódó kényszerintézkedések*, "Büntetőjogi Szemle" 2017, No. 1.

Basic Hungarian legal sources

1998. évi XIX. törvény a büntetőeljárásról (the old Code of Criminal Procedure).

2017. évi XC. törvény a büntetőeljárásról.

9/2018. (VI. 29.) LÜ utasítás az előkészítő eljárással, a nyomozás felügyeletével és irányításával, valamint a befejező intézkedésekkel kapcsolatos ügyészi feladatokról.

100/2018. (VI. 8.) Korm. rendelet – a nyomozás és az előkészítő eljárás részletes szabályairól.

PROF. DR. ERIKA RÓTH, EGYETEMI TANÁR
University of Miskolc | DOI: 10.32041/9788367149761/8

Chapter 8. Particulars of Evidence in Cybercrime Cases

8.1. Introduction

Introduction and analysis of the rules of evidence are very important if we deal with a special field of crime such as cybercrime. Before starting a detailed discussion of the topic, it should be noted, that there is no special procedural provision in this area regarding cybercrime in Hungary. The rules governing proceedings for all criminal cases must also be applied to cybercrime cases.

The other side of the phenomenon is, the "Evidence of cybercrime (…) differs from evidence of traditional crime. Accordingly, novel coercive measures, other investigatory powers, tactics, and technical methods are needed in order to secure evidence of cybercrime."[1] It follows from the nature of these offences, that certain means of evidence play significant role in this field such as physical evidence and electronic data. Employing a specialised expert is also often required in these cases.

But it is not only the specific means of evidence that need to be introduced. We have to speak about the method of obtaining it, since some of these means of evidence can be obtained by using covert means, e.g., secret surveillance of an information system. Due to the often cross-border nature of cybercrime, another important

[1] J. Riekkinen, *Evidence of cybercrime and coercive measures in Finland*, p. 1, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

issue is the acquisition of evidence in another country and the use of the obtained evidence. In this respect, judicial cooperation in criminal matters is of great importance.

In the beginning of this chapter, we intend to examine the general rules of evidence such as the lawfulness of evidence, evaluation of evidence etc. After that we will take a look at the means of evidence that can be used in Hungarian criminal proceedings. In the next part of the chapter specialities of evidence used in cybercrime cases and the specific problems of obtaining evidence will be discussed.

8.2. General Rules of Evidence

The effective Code of criminal procedure is Act XC of 2017 (hereinafter: HCCP) which entered into force on 1 July 2018. Regulation governing the use and evaluation of evidence in the Hungarian code on criminal procedure is based on the rules of the *free system of evidence*, since any means of evidence or evidentiary act specified in the Code may be used or applied freely in the criminal proceeding. The value of evidence is not determined in advance by law. The court, the prosecution service, and the investigating authority shall evaluate pieces of evidence freely both individually and in their totality, and it shall determine the result of the evidence according to its conviction thus formed. The only but very important limit is, that a fact originating from a means of evidence may not be taken into account as evidence if the court, the prosecution service, the investigating authority, or another authority acquired the given means of evidence by way of a criminal offence, a material violation of the procedural rights of a person participating in the criminal proceeding, or in any other prohibited manner (HCCP 167. §). But, in some respects, the Hungarian system of evidence is a so-called "mixed system"[2] as the law may order the use of certain means of evi-

[2] As Á. Farkas writes, this provision indicates the survival of certain elements of the legally bound system of evidence. Á. Farkas, E. Róth, *A büntetőeljárás*, Budapest 2018, p. 200. According to Mihály Tóth the current law is closer to the free evidentiary system, but its evidential system can actually be considered "mixed". E. Belovics, M. Tóth, *Büntető eljárásjog*, Budapest 2017, p. 146.

dence (HCCP 167. § (1) para.) and the manner of performing and conducting evidentiary acts, and examining and recording means of evidence may be specified by law (HCCP 166. § (2) para.).

With respect to the separation of procedural functions and the biding nature of the charge, it is very important that the prosecutor is responsible for discovering all facts required to prove the charge, and providing the evidence supporting them and making a motion to collect them. In the course of clarifying the facts of the case a court shall obtain evidence on the basis of motions. In the absence of a motion, the court is not obliged to obtain or examine any pieces of evidence (HCCP 164. §).

8.3. Means of Gathering Evidence

As it was mentioned earlier, the Hungarian system of evidence is (basically) free, but the HCCP provides a list of means of evidence and evidentiary acts. The free system of evidence means that any means of evidence or evidentiary act specified in the HCCP may be used or applied freely in the criminal proceeding. Means of evidence are the following:

a) witness testimony,
b) defendant testimony,
c) expert opinion,
d) opinion of a probation officer,
e) means of physical evidence, including documents and deeds, and
f) electronic data.

Although the enumerations of means of evidence is closed, the list is exhaustive, the enumeration of evidentiary acts in the HCCP appears to be exemplary (it is indicated by the term "in particular"), although we cannot mention any additional act that might be used in criminal proceedings. These acts are the following:

a) inspection,
b) on-site interrogation,
c) reconstruction of a criminal offence,

d) presentation for identification, confrontation,
e) and instrumental examination of a testimony.

In this subchapter we deal with means of evidence – except for expert opinion and electronic data which will be discussed in the next point – and with evidentiary acts, especially with rules of inspection, as it can be used in cybercrime cases quite frequently.

8.3.1. MEANS OF EVIDENCE

It is beyond dispute, that usually witness testimony and testimony of the accused could be a very important and frequently used means of evidence in criminal proceedings, in cybercrime cases the electronic data and expert opinion (of informatics/data science specialists) are of particular importance. Before dealing with these two means of evidence in details, we outline briefly the specific feature of other means of evidence.

Witness testimony is the most frequent evidence in criminal proceedings but in cybercrime cases it is less significant. Cybercrimes typically have no eyewitnesses,[3] but of course, the victim and anybody else who has knowledge of facts relevant to the offence can be interrogated as a witness. It is a civic duty to testify as a witness unless the HCCP makes an exception. These exceptions are regulated by the HCCP as the two main categories of obstacles to testifying: prohibition of giving testimony[4] and reasons of refusal to give testimony.

The *testimony of defendants*, especially if there is admission of guilt, may support the detection of an offence and the establishment of facts. In the Hungarian criminal procedure, the defendant is not obliged to testify and to tell the truth if he testifies, but he may not accuse falsely another person of having committed a criminal

[3] "Eyewitness and eyewitness testimonies and traditional physical evidence are rarely available." J. Riekkinen, *Evidence…*, *op. cit.*, p. 5.

[4] The name of this category is misleading, because these persons shall not be interrogated, the addressees of the prohibition are authorities acting in the criminal proceedings.

offence, and he may not violate the right to respect for the deceased by stating any false fact (HCCP 185. § (1) para. d) point).[5]

It needs be said that the accused's confession can be the basis of several prosecutorial measures and decisions that can bring the proceeding to a conclusion favourable for the accused, such as mediation, conditional suspension of the proceeding, plea agreement, or in the case of accusation, the taking of measures necessary for quicker and simpler special procedures, such as (immediate) summary procedure or procedure for passing a penal order.

Physical evidence and *electronic data* are in very close connection with each other. In the former Code of criminal procedure, electronic data was one form of physical evidence. It was only created as a special means of evidence by the new Code. Even nowadays we can discover a connection among the rules concerning physical evidence when the legislator determines the definition of "document": a "document" is any physical evidence that records data by technical, chemical, or any other method, including, in particular, texts, drawings, and illustrations recorded in a paper-based form or as electronic data (HCCP 204. § (2) para.).

The *opinion of a probation officer* has a lesser importance in cybercrime cases. The opinion prepared by the probation officer describes the facts and circumstances characterising the personality and living conditions of the defendant, in particular his family situation, health, any addiction, housing situation, education, qualification, workplace or, in the absence of a workplace, data on

[5] Defendant shall be informed about his right concerning his testimony according to the 185. § (1) para. of the HCCP. Information concerns the following issues:

- he is not obliged to give a testimony; he may refuse to testify and to answer any question at any time during the interrogation; but he may decide to testify at any time, even if he refused to do so earlier,
- refusing to testify does not hinder the continuation of the proceeding or affect the right of the defendant to ask questions, make observations, or file motions,
- if he testifies, anything he says or makes available may be used as evidence,
- he may not accuse falsely another person of having committed a criminal offence, and he may not violate any right to respect for the deceased by stating any false fact.

his occupation, financial situation and assets; it shall also present any relationship between the discovered facts, circumstances, and the commission of the criminal offence, as well as the risk of reoffending, and the needs of the defendant. In the opinion, the probation officer provides information on employment possibilities that would be suitable for the defendant considering his skills, as well as healthcare and social care options available to him; he may suggest individual rules of behaviour or obligations to be imposed on a defendant, as well as interventions to be taken to mitigate the risk of reoffending (HCCP 203. § (1)–(2) para.). The probation officer's opinion can be helpful in determining the sanction by the court or discretionary measures taken by the public prosecutor, such as conditional suspension of the proceeding or referral of the case to a mediation procedure.

8.3.2. EVIDENTIARY ACTS

8.3.2.1. *Inspection*

The court, the prosecution service, or the investigating authority may order and carry out an inspection if a person, object, or site needs to be inspected, or an object or site needs to be observed to discover or establish a fact to be proven (HCCP 207. § (1) para.). During the inspection, means of physical evidence shall be sought and collected, and arrangements shall be made for the proper preservation of them.

In the course of an inspection, circumstances that are relevant to evidence shall be recorded in detail, in particular, the course, method, location, and condition of finding and collecting the inspection object. During the search for, recording, and securing of physical evidence, it is necessary to proceed in such a way that compliance with the rules of procedure can be verified subsequently. If possible and necessary, a visual, sound, or audio-visual recording, drawing or sketch shall be made of the object of the inspection, and it shall be attached to the minutes (HCCP 207. § (2) para.).

The HCCP allows the involvement of the expert during the inspection in all cases (HCCP 207. § (4) para.). This can be very important, since improper collection and recording of evidence can affect the success of the evidence. The participation of an *IT expert* in the inspection – similarly to search and seizure – can guarantee professionalism, credibility and unchangingness of the evidence. In the proceedings where electronic data are concerned, the involvement of an IT expert could be important if the inspection of the information system or data medium requires special knowledge, while in order to collect electronic evidence a *specialist consultant* can be used.[6] The specialist consultant is not an expert, but is a person with expertise on a specific issue not specifically defined by law. He assists the authorities by providing expertise where specific knowledge is required to detect, search for, acquire, collect or record evidence. He provides information of a specific nature to supplement the expertise of the authorities. A specialist consultant may be interrogated as a witness regarding a procedural act carried out with his involvement (HCCP 270. § (1) and (5) and the justification for the given article of the Act).

Evidence found on the internet is usually saved as part of the online inspection. In data saving, the acting investigators search and record relevant data such as internet searches and downloaded files.[7]

On-site interrogation, reconstruction of a criminal offence, presentation for identification and confrontation have little if any significance in cybercrime cases, so we will only briefly describe their essence.

8.3.2.2. *On-Site Interrogation*

On-site interrogation gives the court, the prosecution service, or the investigating authority an opportunity to interrogate the defendant and the witness on the site. This is done if it is necessary

[6] See B. Simon, R. Gyaraki, *A kiberbűncselekmények felderítése* és *nyomozása*, [in:] T. Kiss (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020, p. 138.
[7] Ibidem.

that they give testimony at the scene of the criminal offence or at another place related to the criminal offence or to show the place where the criminal offence was committed, another place related to the criminal offence, to show physical evidence or the course of the criminal offence (HCCP 208. § (1) para.).

8.3.2.3. *Reconstruction of a Criminal Offence*

Reconstruction of a criminal offence may be ordered and held by the court, the prosecution service or the investigating authority if it is necessary to establish or verify whether an event or phenomenon could have occurred at a specific place, time, in a specific manner or under specific circumstances. It shall, as far as it possible, be held under the same conditions as the event or phenomenon under investigation occurred or could have occurred (HCCP 209. § (1) para.).

8.3.2.4. *Presentation for Identification*

Presentation for identification can be ordered and held by the court, the prosecution service or the investigating authority if doing so is necessary for the identification of a person or object. A least three persons or objects must be presented to the defendant or the witness for identification. This usually means the physical presentation of a person or an object, but in the case when no other option is available, they can be presented by visual or audio or audio-visual recording (HCCP 210. § (1) para.).

8.3.2.5. *Confrontation*

Confrontation may be necessary when the testimony of the defendants, witnesses or the defendant and the witness contradict each other. In such a case the court, the prosecution service and the investigating authority can order a confrontation in order to resolve the contradiction (HCCP 211. § (1) para.).

8.3.3. OBTAINING THE EVIDENCE

Authorities acting in criminal cases can use open and covert means to obtain the evidence necessary to establish the facts of a case. It is not possible to outline in a few sentences all that is important to know about the use of covert means in criminal proceedings in Hungary, so we only try to provide a brief overview of the most important features of these instruments.

The use of *covert means* raises several constitutional problems, because fundamental rights of citizens – even those of outsiders, who have no connection with the offence subject of the investigation – might be violated. Therefore, it is of utmost importance that the use of covert methods should be permitted only in exceptional cases, in accordance with the principles of *necessity* and *proportionality*. In order to meet these requirements, the HCCP allows the use of covert means if:

a) it can be reasonably assumed that the information or evidence to be obtained is essential for achieving the purpose of a criminal proceeding, and it cannot be obtained by other means,
b) its use does not result in a disproportionate restriction of the fundamental right of the person concerned, or of another person in relation to the attainment of the law enforcement goal and
c) it is likely that information or evidence relating to a criminal offence may be obtained by its use (HCCP 214. (5) para.).

The HCCP allows the use of several covert means in criminal proceedings.[8] It classifies covert means into *three categories* according to the permission (authorisation) they are subject to. These categories are the following:

a) not subject to permission of a judge or a prosecutor,
b) subject to permission of a prosecutor, or
c) subject to permission of a judge (HCCP 214. § (4) para.).

[8] In Poland "secret or remote searches are not allowed on the grounds of criminal procedure". P. Lewulis, *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, p. 47, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

The first group includes for example the use of a trap or covert surveillance. The surveillance of payment transactions, simulated purchases, use of an undercover investigator and some other means are allowed only with *permission of the public prosecutor*, but covert means representing the most serious restriction of fundamental right may only be used with the permission of judicial authority.

According to the HCCP the following covert means may be used only *with judicial permission*: secret surveillance of an information system, secret search, secret surveillance of a locality, secret interception of a consignment, interception of communications.

The last group of covert means play a most important role in cybercrime cases, as they might be decisive for identifying the perpetrator or to obtain access to information necessary to detect the offence. The court decides on granting permission to use any covert means subject to permission of a judge upon a motion submitted by the prosecution service. Since covert means may only be used during the investigation (or to the limited extent in the preparatory procedure) the tasks of a court of first instance are performed by a district court judge appointed as *investigating judge* by the president of the respective regional court. We intend to describe covert means typically appropriate to use in cybercrime cases in the next subchapter.

8.4. Particulars of Evidence Used in Cybercrime Cases

What is special about the evidence process in cybercrime cases? First of all, the main difficulty is how to prove the commission of such offences, to detect the identity and location of the perpetrator. Regarding crimes committed in the cyber environment, the preponderance of evidence is based on *digital data*. "The evidence of cybercrime offences exists nearly exclusively in electronic form.[9]" Many authors emphasise, that is more difficult to collect evidence and establish facts in cybercrime cases than in other cases.[10] While that may be true, it should be added that this statement is justified not

[9] J. Riekkinen, *Evidence…*, *op. cit.*, p. 5.

[10] For example, I. Lajtár, *A kiberbűnözésről,* "Ügyészek Lapja" 2019, No. 1, p. 50.

only in cybercrime cases, but in other procedures where electronic data must be used as a means of evidence. Electronic data can be changed and deleted quickly and thus evidence can be destroyed or falsified. Determining the *place* where the digital data was created or/and uploaded sometimes means insurmountable tasks for law enforcement agencies. The IT service providers often lack the will to cooperate, but without their help, collection of evidence is a difficult or impossible task.

Similarly, *pinpointing the user's identity* can be extremely difficult, taking into account that the same system is frequently used by several people.[11]

Another challenge of digital investigation is *encryption*. Several forms of encryption are described by Kökényesi-Bartos, who summarises the consequence of encrypted communication as follows:

> It is not easy to observe such communication on the internet, not even by the authorities, even if the user's Internet service provider or messaging service company providing the messaging service was approached by law enforcement to provide legal assistance.[12]

Encryption is no longer a magic thing, cybercriminals have easy access to encryption solutions and software, "(…) they are available in online commerce together with software designed to remove digital evidence".[13] At the same time, unblocking the increasingly widespread and sophisticated encryption technology is also a serious challenge.[14]

---

[11] See: Ibidem.

[12] A. Kökényesi-Bartos, *The functioning of internet communication and the challenges of online digital investigation*, [in:] G. Virág (ed.), *Combating cybercrime, corruption and money laundering*, "Studies on Criminology" 2022, Vol. 59, Special Issue 2, p. 90. In his study, the author writes about solutions that hide the user's IP address, thus making it impossible to identify the user.

[13] B. Grund, *A kibertér bűncselekményeiről* és *a kiberbűnözés hazai gyakorlatáról,* p. 5, https://jog.tk.mta.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol (accessed on: 18.07.2023).

[14] I. Lajtár, *A kiberbűnözésről*, *op. cit*., p. 50.

8.4.1. ELECTRONIC DATA AS A MEANS OF EVIDENCE

As Zoltán Nagy wrote, "the range of crime that cannot be committed by computer is getting narrower".[15] Criminals use tech services and tools to plan and commit crimes more frequently. "As a result, e-evidence is becoming essential to fighting crime: currently, 85% of criminal investigations involve digital data."[16] We agree with Lewulis, who states that "The importance of digital evidence extends to the prosecution of all types of crimes in all jurisdictions."[17]

What is e-evidence? Electronic evidence, or "e-evidence", refers to *digital data* that is used to investigate and prosecute criminal offences. As Tibor Peszleg states, digital evidence is data, so it is not a tangible thing. Data does not exist in itself, it is only recorded by some data medium.[18]

Among electronic data, a distinction can be made between electronic data carrying content, traffic data or other electronic data and traces.[19] Such data can be used to identify a person or obtain more information about their activities. Electronic data includes, among others: emails, text messages or content from messaging apps, audiovisual content information about a user's online account, etc.

---

[15] Z. Nagy, *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in]: *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, "Acta Universitatis Szegediensis, Acta Juridica et Politica" 2018, Vol. 81, p. 755.

[16] European Council, *Better access to e-evidence to fight crime,* https://www.consilium.europa.eu/en/policies/e-evidence/#:~:text=The%20regulation%20on%20production%20and%20preservation%20orders%20for,provider%20established%20or%20represented%20in%20another%20member%20state (accessed on: 26.07.2023).

[17] P. Lewulis, *Collecting…*, *op. cit.*, p. 39.

[18] T. Peszleg, *A digitális bizonyítási eszközök megszerzésének elvei* és *gyakorlati érvényesülésük,* "Ügyészek Lapja" 2010, No. 2, p. 26.

[19] See more about the classification in: Z. Nagy, *A joghatóság…*, *op. cit.*, p. 758. Claudia Warken states, that "The common distinction of communication data, generally resulting in a classification of content data and non-content data or content data, traffic data and user data, does not meet the requirements of modern legistics. (…) The required classification has to reflect the sensitivity of specific types of electronic data." In her study she provides a comprehensive data classification for criminal law purposes. C. Warken, *Classification of Electronic Data for Criminal Law Purposes*, "Eucrim" 2018, No. 4, p. 226.

When using the internet, the user leaves traces, which in the event of committing a criminal offence can help identify the perpetrator and clarify circumstances of the offence.[20] If the subscriber is the same as the user, the investigating authorities has an easier task. However, if the given subscription is used more than one person, identifying the alleged perpetrator is much more difficult, and the fact that a subscriber's IP address is not permanent also causes problem. In the case of dynamic IP address allocation based on the given IP address alone, it is not possible to determine which internet subscriber used it, only if we know the exact time of use. The service provider logs which IP address was used by which customer at which time and can provide this information at the request of the authorities.

Electronic data, like other data required in criminal proceedings, can be obtained by both open and covert means. The provision on *open data acquisition* is set out in 261. § of the HCCP under the heading of data collection activities. Authorities acting in the criminal procedure may request any organ, legal person, or other organisation without a legal personality to provide data (HCCP 261. § (1) para.). Point b) of that section also refers specifically to electronic data. Within the framework of data request – among others – the transfer of electronic data may be requested (HCCP 261. § (3) para. b) point). The organisation requested to provide data is obliged to comply with the request within a set time limit or to notify of a detected obstacle to fulfilment without delay (HCCP 264. § (1) para.).

A special possibility of data request is conditional data request (HCCP 266. §). This means that the party obliged to provide the information must do so if and when the condition specified occurs. It means a kind of monitoring activity, allowing the monitoring of the subject concerned for a longer period of time.

"Electronic evidence of such crimes may be difficult to collect, owing to the volatility of data, and may require specific expertise."[21]

[20] See A. Kökényesi-Bartos, *The functioning…*, *op. cit*., p. 86.

[21] *Overview Report Challenges and best practices from Eurojust's casework in the area of cybercrime November 2020*, p. 3, https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_Cybercrime-Report.pdf (accessed on: 11.07.2023).

In the process of obtaining and collecting electronic data, particular care must be taken to ensure that their authenticity cannot be questioned, otherwise their use before the court will fail and they will not be accepted as evidence by the court.[22] The success of proving crimes committed in the IT environment is decisively influenced by the fact whether the investigating authority or the public prosecutor can ensure electronic data proving the commission of the crime during the investigation.[23]

From the point of view of collecting and recording electronic data, it is also important where they are located. Whether we are talking about data stored on a physical device (computer, phone etc.) or in the cloud.[24]

The Polish Code of Criminal Procedure:

> formally recognizes only two general types of evidence sources: personal and material (or real) evidence. (…) Since digital information does not possess a physical form, digital evidence placement in such an exhaustive division of evidence types might be problematic. However, out of necessity digital evidence falls into the "material evidence" category despite not having a physical form.[25]

But in Poland, 'there is no legal definition of "digital evidence"'.[26]

In criminal proceedings – not only concerning cybercrime cases but all cases where electronic data should be used as evidence – the access to electronic data stored in another country is crucial. In the EU, the adoption of new rules to speed up access to electronic/digital data started in 2018[27] when the European Commission put

[22] This is often emphasised by authors who write about collecting evidence. See for example: B. Simon, R. Gyaraki, *op. cit*., pp. 132, 135.

[23] I. Szabó, *Az elektronikus bizonyítékok megszerzésének időszerű problémái*, "Ügyészségi Szemle" 2018, No. 3, p. 116.

[24] See: B. Simon, R. Gyaraki, *A kiberbűncselekmények…*, *op. cit.,* p. 126.

[25] P. Lewulis, *Collecting…*, *op. cit*., p. 42.

[26] Ibidem.

[27] But the start of the process goes back to 2016, when "the Council called for concrete action based on a common EU approach to make mutual legal

forward a proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.[28] What do the Production Order and Preservation Order mean?

> The production order will allow a member state's judicial authority to directly request access to e-evidence from a service provider established or represented in another member state (…) The preservation order will prevent e-evidence from being deleted by a service provider while the production order is still being processed.[29]

From this very short introduction, it is obvious that the new regulation makes access to electronic data much easier and faster, and consequently makes the investigation and prosecution more effective.[30]

---

assistance more efficient; to improve cooperation between Member State authorities and service providers based in non-EU countries; and to propose solutions to the problem of determining and enforcing jurisdiction in cyberspace." Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Strasbourg, 17.4.2018. COM (2018) 225 final, (hereinafter: Proposal for Production and Preservation Order), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed on: 26.07.2023). The concrete background of the proposal was the terrorist attacks in Brussels of 22 March 2016 and the Joint Declaration of EU Ministers for Justice and Home Affair Ministers and Representatives of EU Institutions' two days after the attacks. See: Á.Tinoco-Pastrana, *The Proposal on Electronic Evidence in the European Union*, "Eucrim" 2020, No. 1, p. 46.

[28] Proposal for Production and Preservation Order.

[29] European Council, *Better access to e-evidence to fight crime*, https://www.consilium.europa.eu/en/policies/e-evidence/#:~:text=The%20regulation%20on%20production%20and%20preservation%20orders%20for,provider%20established%20or%20represented%20in%20another%20member%20state (accessed on: 26.07.2023).

[30] On 25 January 2023 the EU member states' ambassadors "confirmed the agreement reached between the Council presidency and the European Parliament on the draft regulation and the draft directive on cross-border access to e-evidence," https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-

8.4.2. IT EXPERT IN CRIMINAL PROCEEDINGS

In cybercrime cases, certain *special knowledge* may be necessary to determine what kind of evidence should be collected and which coercive measure if any should be used in order to collect it. Since the possibility of using electronic evidence may emerge in more and more cases, "There is a constantly increasing demand for the expertise and opinion of an IT or computer expert in criminal proceedings."[31]

Expert opinion is a very important piece of evidence. It is frequently used in cybercrime cases because members of the investigating authority, the public prosecutor and the judge do not have special technical knowledge – although they usually, but not necessarily, have user-level knowledge. "Digital traces can usually only be searched for and interpreted by people with expertise."[32]

The Hungarian CCP provides a relatively wide possibility for the involvement of the expert. If specialised expertise is required to establish or determine a fact to be proven, an expert shall be employed (HCCP 188. § (1) para.).

Regarding the involvement of the expert, it should be noted that it is neither appropriate to involve him in the procedure unnecessarily, nor to not involve him in the procedure even when necessary.[33]

---

on-new-rules-to-improve-cross-border-access-to-e-evidence/ (accessed on: 26.07.2023). The Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and the Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings were adopted on 12 July 2023 and were published in the Official Journal of the European Union on 28 July 2023.

[31] B. Elek, *Informatikus szakértés a büntetőeljárásban*, "Belügyi Szemle" 2014, No. 7–8, p. 163.

[32] T. Peszleg, *Interneten, számítógépen történő nyomrögzítés*, "Ügyészek Lapja" 2005, No. 1, p. 27.

[33] "Currently, it can generally be said that in cyber related cases of crimes the investigating authority appoints an expert because they are either afraid that the digital evidence will not be recognized, or because they fear that a procedural mistake will be made when implementing the coercive measure" or

With respect to the former, the appointment of an expert may result in unjustified prolongation of the procedure and higher procedural cost, while in the latter case, unrecoverable errors may occur:

> The analysis of digital evidence requires appropriate IT knowledge, which is often not available to the staff of the investigating authority. The forensic IT expert is the only actor in the criminal justice proceeding who can and is entitled to help in this situation.[34]

In 2020 a *methodological letter* was adopted on general principles for the examination of electronic data.[35] The material scope of this methodological letter covers the following areas of forensic informatics expert activity related to electronic data: identification, preservation, collection, conservation, acquisition, examination, and analysis of electronic data.

Experts also play a very important role in criminal proceedings in Poland, because "Polish law does not describe any specific technics or methods of material evidence gathering, leaving that to experts in relevant disciplines of forensic science."[36]

8.4.3. COVERT METHODS USED FOR OBTAINING EVIDENCE IN CYBERCRIME CASES

It is not possible to present all covert means in the framework of this chapter, so we will only briefly mention those that may be relevant to the detection of cybercrimes.

---

the prosecutor requires the appointment of an expert. B. Simon, R. Gyaraki, *A kiberbűncselekmények…*, *op. cit*., p. 146.

[34] I.Zs. Máté, *Az igazságügyi informatikai szakértő a büntetőeljárásban – doktori értekezés,* Pécs 2017, p. 112, https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/mate-istvan-zsolt/mate-istvan-zsolt-vedes-ertekezes.pdf (accessed on: 06.08.2023).

[35] Methodological letter No. 6/2020, https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf (accessed on: 06.08.2023).

[36] P. Lewulis, *Collecting…*, *op. cit*., p. 44.

Surveillance of Payment Transactions

Surveillance of payment transactions is one of the *covert means* subject to *permission of the public prosecutor*. The essence of this measures is, that an organisation providing financial services or supplementary financial services may be instructed to record, keep, and transmit data pertaining to payment transactions to the ordering entity during a specified period (HCCP 216. § (1) para.). In addition to passive surveillance, the use of this covert means may also include the suspension of the execution of the payment transaction for the purpose of evaluating data and intervening in the interests of law enforcement (HCCP 217. § (1) para.). During the suspension of the payment transaction, the ordering entity shall examine whether the suspended payment transaction can be connected to a criminal offence (HCCP 217. § (3) para.).

Covert Means Subject to Permission of a Judge

According to the HCCP, the following covert means may be used subject to permission of a judge:

a) secret surveillance of an information system,
b) secret search,
c) secret surveillance of a locality,
d) secret interception of a consignment,
e) interception of communications (HCCP 231. §).

Although in principle all covert means subject to a judicial permission can be used in cybercrime cases as well (provided that it constitutes a criminal offence, for which the law allows the use of covert means) we highlight only one of them, the *secret surveillance of an information system*. In the course of secret surveillance of an information system, the organ authorised to use covert means may, with permission of a judge, secretly access and record, by technical means, data processed in an information system. For that purpose, any necessary electronic data may be placed in an information system, while any necessary technical device may be placed at a dwelling, other premises, fenced area, vehicle, or other object used by the person

concerned, except for public areas, premises open to the public, and means of public transport (HCCP 232. § (1) para.). Covert means subject to a judicial permission may only be used in proceedings for offences and for the time period defined by the HCCP.

8.5. *De Lege Ferenda* Proposals

Due to the difficulties in the law enforcement resulting from development of information technology, it is almost impossible to develop up-to-date laws that enable efficient justice.[37] As Hungarian researchers not being familiar enough with Polish criminal procedural law and practice, we can only very cautiously make suggestions to the legislator. As Lewulis states:

> Polish law enforcement authorities may try to bypass or even ignore the described procedural shortcomings. Given the existing legal deficiencies, it is well imaginable that digital evidence is collected with the omission, or even contrary to some regulation (…) Such evidence could be considered illegally obtained.[38]

In order to avoid such actions of law enforcement authorities which result in the inadmissibility of evidence and consequently in the ineffectiveness of prosecution, the legislator must monitor law enforcement practice and respond to problems that can be solved by legislation.

The involvement of legal practitioners in the legislative process works well in many countries. Legislators must accept that they are not infallible, and the feedback of practitioners must be taken into account in the course of the correction of legislative mistakes, especially in complex, coordinated legislative processes.

[37] I. Szabó, *Az elektronikus…*, *op. cit*., p. 116.
[38] P. Lewulis, *Collecting…*, *op. cit.,* p. 50.

It is already a commonplace that the legislator should pay attention to international expectations, which means more than just compliance with the EU's requirements.

Attention must also be paid to the proposals formulated by the scientific community.

8.6. Conclusion

Although traditional forms of evidence can also be available in cybercrime cases, they have less significance. 'The evidence of cybercrime offences exists nearly exclusively in electronic form.[39]' The importance of continuous training of legal practitioners is highlighted by several authors. It is important that the authorities in criminal matters are aware of newer methods of committing offences and of the latest trends in IT crime. To this end, Petronella Deres proposed the joint training of the members of organisations involved in criminal proceedings (investigating authorities, prosecutor's offices, courts)[40]:

> Capacity building is the most effective way towards more effective investigation, prosecution and adjudication of cybercrime and other offences involving electronic evidence. A massive surge in resources and skills for criminal justice authorities, including the judiciary is required.[41]

[39] J. Riekkinen, *Evidence…*, *op. cit.*, p. 5.

[40] P. Deres, *A kibertérrel* összefüggő *bűncselekmények sajátosságai Magyarországon*, "Ügyészek Lapja" 2023, No. 1, p. 79.

[41] *Key messages of the Octopus Conference 2019. Cooperation against cybercrime, Strasbourg, 20–22 November 2019*, https://rm.coe.int/3021-110-octo19-keymessages-v3/168098e8a5 (accessed on: 10.08.2023).

REFERENCES

Belovics, E., Tóth, M., *Büntető eljárásjog*, Budapest 2017.

Deres, P., *A kibertérrel összefüggő bűncselekmények sajátosságai Magyarországon*, "Ügyészek Lapja" 2023, No. 1, pp. 75–79.

Elek, B., *Informatikus szakértés a büntetőeljárásban*, "Belügyi Szemle" 2014, No. 7–8. *Key messages of the Octopus Conference 2019. Cooperation against cybercrime 20-22 November 2019*, Strasbourg, https://rm.coe.int/3021-110-octo19-keymessages-v3/168098e8a5 (accessed on: 10.08.2023).

European Council, *Better access to e-evidence to fight crime*, https://www.consilium.europa.eu/en/policies/e-evidence/#:~:text=The%20regulation%20on%20production%20and%20preservation%20orders%20for,provider%20established%20or%20represented%20in%20another%20member%20state (accessed on: 26.07.2023).

Farkas, Á., Róth, E., *A büntetőeljárás*, Budapest 2018.

Grund, B., *A kibertér bűncselekményeiről* és *a kiberbűnözés hazai gyakorlatáról*, https://jog.tk.mta.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol (accessed on: 18.07.2023).

Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020.

Kökényesi-Bartos, A., *The functioning of internet communication and the challenges of online digital investigation*, [in:] Virág, G. (ed.), *Combating cybercrime, corruption and money laundering*, "Studies on Criminology" 2022, Vol. 59, Special Issue 2, pp. 82–92.

Lajtár, I., *A kiberbűnözésről*, "Ügyészek Lapja" 2019, No. 1.

Lewulis, P., *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, pp. 39–62, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

Máté, I.Zs., *Az igazságügyi informatikai szakértő a büntetőeljárásban – doktori értekezés,* Pécs 2017, https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/mate-istvanzsolt/mate-istvan-zsolt-vedes-ertekezes.pdf (accessed on: 06.08.2023).

Methodological letter No. 6/2020, https://miszk.hu/files/modszertani_levelek/MISZK_modszertani_level_6_2020.pdf (accessed on: 06.08.2023).

Nagy, Z., *A joghatóság problémája a kiberbűncselekmények nyomozásában*, [in:] *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára*, "Acta Universitatis Szegediensis, Acta Juridica et Politica" 2018, Vol. 81.

Overview Report Challenges and best practices from Eurojust's casework in the area of cybercrime November 2020, https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_Cybercrime-Report.pdf (accessed on: 11.07.2023).

Peszleg, T., *A digitális bizonyítási eszközök megszerzésének elvei* és *gyakorlati érvényesülésük,* "Ügyészek Lapja" 2010, No. 2.

Peszleg, T., *Interneten, számítógépen történő nyomrögzítés*, "Ügyészek Lapja" 2005, No. 1.

Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17.4.2018, COM (2018) 225 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (accessed on: 26.07.2023).

Riekkinen, J., *Evidence of cybercrime and coercive measures in Finland*, p. 1, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

Simon, B., Gyaraki, R., *A kiberbűncselekmények felderítése* és *nyomozása*, [in:] Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020.

Szabó, I., *Az elektronikus bizonyítékok megszerzésének időszerű problémái*, "Ügyészségi Szemle" 2018, No. 3.

Tinoco-Pastrana, Á., *The Proposal on Electronic Evidence in the European Union*, "Eucrim" 2020, No. 1, pp. 46–50.

Warken, C., *Classification of Electronic Data for Criminal Law Purposes*, "Eucrim" 2018, No. 4.

Basic Hungarian legal sources

2016. évi XXIX. törvény az igazságügyi szakértőkről.
2017. évi XC. törvény a büntetőeljárásról.
9/2018. (VI. 29.) LÜ utasítás az előkészítő eljárással, a nyomozás felügyeletével és irányításával, valamint a befejező intézkedésekkel kapcsolatos ügyészi feladatokról.
100/2018. (VI. 8.) Korm. rendelet - a nyomozás és az előkészítő eljárás részletes szabályairól.

DR RAFAŁ WIELKI
University of Opole | DOI: 10.32041/9788367149761/9

Chapter 9. Data Retention and Legal Problems of Investigating Cybercrime

9.1. Introduction

Investigating cybercrimes certainly requires the proper technical and substantive preparation of law enforcement agencies, but public services operate primarily on the basis and within the limits of the law. In view of the above, effective investigative activities require a proper legal basis, and there is no denying that legal regulations often have not kept pace with changes in social and technological reality.

The purpose of this chapter is to present the formation of data retention law in the European Union, as well as the problems that lawmakers have encountered over time, which were related to the position of the Court of Justice of the European Union.

Another goal is to show how Polish services operate under the law and how they obtain retention data from Internet Service Providers, while discussing the controversies that arise among lawyers.

Further considerations will be related to proposed changes at the European Union level, which may result in greater accountability of Internet Service Providers for the content they share, as well as the data they process. Finally, another problem touches on legal issues, as an answer is sought to the questions of what legal acts regulate data retention, whether existing national and international regulations are effective and whether they require possible changes, as well as in what direction these changes should go.

9.2. Law on Data Retention in European Union

Problems related to the effective prosecution of cybercrime are also grounded in the law, as many areas are not normalised in either national or international regulations. The aim of this part is to present the problem of data retention by operators of means of electronic communication in order to ensure public security. Effective investigation and combating cybercrime requires access to this data, however, it is presumed that current national as well as international regulations may not meet the needs of the services. It is necessary to reflect on the authorities authorised to access retention data, as well as to define balanced boundaries between fighting cybercrime and ensuring respect for human rights and freedoms.

We should start by considering the first piece of legislation that comprehensively addressed cybercrime, and we are referring to the Convention on Cybercrime, [1] which concerns the prevention of crimes related to the use of new technologies and aims to improve public safety in virtual space. Incidentally, it is worth adding that the Convention was ratified by Hungary in 2003, while it was not ratified by Poland until 2015. Thus, the primary purpose of the Convention was to introduce a uniform catalogue of criminal acts committed by users of information networks, to establish specific procedures for the detection and prosecution of cybercrime, and to set standards for international cooperation in this field.

These goals can be considered achieved. The Convention introduces a catalogue of types of crimes committed using computer systems. These include computer fraud, computer forgery, the crime of hacking (among others, illegal access to a computer system, as well as the manufacture or sale of "hacking tools"), dissemination, possession of child pornography, or copying and distribution of works protected by intellectual property rights. The Cybercrime Convention also requires parties to adopt appropriate procedural arrangements that are necessary for the purposes of ongoing criminal proceedings for the crimes specified in the Convention and are intended

[1] Convention on Cybercrime (ETS No. 185), Budapest 23/11/2001 – Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States.

to help authorised national authorities identify perpetrators and collect evidence of their acts. Among other things, the treaty introduces rules and guarantees for searches of computer resources or the transfer, sharing and safeguarding of computer data. The Convention also obliges parties to introduce appropriate legal measures to strengthen international cooperation in combating cybercrime through, among other things, the provision of legal assistance (including data exchange) or extradition of perpetrators. Over time, the Convention has been modernised through additional protocols on the criminalisation of racist and xenophobic acts[2] and cooperation and disclosure of electronic evidence.[3]

Importantly, the Convention addresses the problem of data retention on a baseline basis. According to Article 20(1) of the Convention:

> Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to collect or record through the application of technical means on the territory of that Party, and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party; or to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

Further reference to data retention is found in Article 21(1) of the Convention:

> Each Party shall adopt such legislative and other measures as may be necessary, in relations to a range of serious offences to be determined by domestic law, to empower

[2] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

[3] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

> its competent authorities to: collect or record through the application of technical means on the territory of that Party, and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party, or to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system'.

These regulations are not able to completely normalise the problem of data retention, hence attempts have been made on the ground in the European Union to clarify regulations that would allow law enforcement agencies to access data on network traffic collected by ICT network operators. Hence, the following were put into effect Directive 2006/24/EC of the European Parliament and of the Council.[4] The directive imposed an obligation on providers of publicly available electronic communications services or public communications networks to retain certain data generated or processed by those providers. This obligation applied to both telephone and Internet connections and covered a wide range of data necessary for:

- determine the source of the call, including the name and address of the user(subscriber),
- determining the recipient of the call, including the user(subscriber)'s number or ID, name and address,
- determining the date, time and duration of the call,
- determining the type of call,
- communication tool,
- identification of the location of the mobile communication device.

[4] Directive 2006/24/EC of the European Parliament and of the Council of March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

However, this directive has been challenged by the Court of Justice of the European Union.[5] The proceedings were initiated on the basis of a request for a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (TFEU) from the High Court of Ireland and the Verfassungsgerichtshof of Austria. The reference for a preliminary ruling arose in connection with a complaint by Digital Rights Ireland Ltd, in which the legality of national legislation on the retention of data related to electronic communications was challenged. The source for the proceedings before the CJEU was also a second complaint by the Carinthian national government and several thousand individuals also concerning the compatibility of Directive 2006/24/EC with the EU Charter of Fundamental Rights. The contradiction was limited to the extent to which Directive 2006/24/EC allows the mass collection over a long period of time of various types of data on an unlimited number of individuals. The complaints argued that the scope of the obligations imposed and the associated restrictions on rights are disproportionate, and are not necessary or are inadequate for legitimate purposes, i.e., to ensure the availability of data for the detection, conduct and prosecution of serious crimes or to ensure the proper functioning of the EU internal market. According to the ruling, in accordance with the principle of proportionality, legal acts of the European Union should contain provisions adequate to achieve the legitimate objectives they are intended to serve and should not go beyond what is necessary to achieve those objectives.[6]

9.3. Polish Approach to Data Retention

There is no doubt that the judgment discussed above has strongly influenced the shape of the proposed legislation, while at the same time provoking – at long last – legitimate discussions about the limit

[5] Judgment of the Court of European Union of 8 April 2014, C-293/12 and C-594/12.

[6] M. Wach, *Dalsze losy retencji danych po wyroku Trybunału Sprawiedliwości UE,* "Ius Novum" 2016, nr 3, p. 200.

of violating civil liberties in the name of combating threats to public security. The verdict has resulted in an approach such that the general and mass storage of mobile or Internet users' traffic and location data is allowed only in the case of a serious threat to national security, and is unlikely to be the rule. However, it should be noted that at the beginning of the new millennium, the world was shaken by successive reports of terrorist attacks, and extreme terrorist groups and organisations had a real impact on the policies pursued in many countries. Nowadays, a greater understanding of civil liberties tends to be shown, but the steady growth of cybercrime must not influence the complete abandonment of data retention, as this would tie the hands of investigators throughout the European Union.

Data retention issues are of interest to the European Union and national legislators. This is particularly relevant, so it is to be expected that data retention issues will be regulated at this level, as was the case with personal data regulated by the General Data Protection Regulation.[7] Currently in Poland there is a discussion on the shape of national data retention laws, as there is a dispute among lawyers about the compatibility of current legal norms with European Union law. The Ombudsman stresses that data collection should be limited to fighting major crimes and should be controlled by an independent body; and the citizen should find out that he or she has been so invigilated. Meanwhile, today the courts actually check this post factum on the basis of general reports from the services – as a result, they cannot reliably assess the legitimacy, adequacy and expediency of these activities. In turn, according to the Ministry of Internal Affairs and Administration, the current legislation does not violate the requirement of proportionality of interference with the right to privacy, freedom of communication and informational autonomy. In the ministry's view, on the other hand, restricting access to telecommunications data will undoubtedly make it much more difficult to detect perpetrators of crimes.

[7] See: Regulation (EU) 2016/679 of the European Parliament and the of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Let's take a look at the Police Act, for example.[8] According to Article 20c, for the purpose of preventing or detecting crimes, fiscal offences, or for the purpose of saving human life or health or supporting search and rescue operations, the police may obtain data not constituting the content of a telecommunications transmission, a postal consignment, or a transmission within the framework of an electronically provided service, respectively – as defined in specific provisions – and may process them without the knowledge and consent of the subject. These are data necessary to:

- determine the network termination, the telecommunications terminal equipment, the end user initiating the call to which the call is directed,
- determine the date and time of the call and its duration, the type of call, the location of the telecommunications terminal equipment,
- obtain data about the postal operator, the postal services provided, and information that allows identification of the users of these services, and:
  - surname and first names of the recipient of the service,
  - PESEL registration number or, if this number has not been assigned, the number of the passport, identity card or other document confirming identity,
  - address of permanent residence registration,
  - correspondence address, if different from the address referred to in item 3,
  - data used to verify the electronic signature of the service recipient,
  - electronic addresses of the service recipient,
  - designations identifying the service recipient assigned on the basis of the data,
  - designations identifying the termination of the telecommunications network or data communications system used by the service recipient,
  - information about the beginning, end and scope of each use of the electronically provided service,

[8] Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. 2023 poz. 171).

– information on the use of electronically provided services by the recipient.

It can be noted that in Polish regulations, the scope of data that can be obtained by the police without judicial supervision of pre-trial proceedings is relatively large, which is why it raises so much controversy and provokes discussions among lawyers.

9.4. Some Comments about the Future

The EU is implementing the Digital Services Act (DSA) and the Digital Markets Act (DMA),[9] which are expected to include regulations for platforms and ways to combat harmful or illegal content online. The EU's efforts are moving in the direction of regulating the Internet through regulations, rather than rules and regulations set by platforms, but it will emphasise that these regulations must protect freedom of expression and fundamental rights, avoiding censorship. And there is undoubtedly a need for regulations governing data retention by social media owners and the release of such data to investigators on the basis of EU regulations, rather than internal rules and regulations, as is often the case today.

The DSA applies to Internet intermediary services, which are used by millions of Europeans every day. The obligations of various online entities have been defined according to their role, market share and power of influence on the online ecosystem. The new EU rules will have to be complied with by all online intermediaries offering their services in the single market, regardless of whether they are based inside or outside the EU. The obligations of micro and small businesses will be proportional to their performance and market share, which does not mean they will be exempt from liability. These regulations should be viewed very positively, as up to now the Internet giants have often refused to cooperate, including in crime-fighting efforts. The Digital Services Act significantly

[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

improves mechanisms for removing illegal content and effectively protecting users' fundamental rights on the Internet, including freedom of expression. It also increases the level of public control over the activities of online platforms.

The DMA establishes strictly defined objective criteria for qualifying a large online platform as an "access gatekeeper" (controlling access to information and services). This ensures that the act remains well-targeted to the problem of large, systemic Internet platforms. Access gatekeepers will retain all opportunities to innovate and offer new services. However, they will no longer benefit unduly, as they will no longer be able to engage in unfair practices against business users and customers who depend on them. Platforms will have to allow third parties to interact with their own access gatekeeper services in certain specific situations, or allow their business users to access the data they generate when using the access gatekeeper platform.

It is worth noting that several pieces of legislation are under development at the EU level, and one of the most important in the context of cyber security is the Network and Information Security Directive (NIS2).[10] The NIS 2 proposal expands the scope of NIS by requiring more entities and sectors to take appropriate action, including providers of public electronic communications services, social media operators, manufacturers of critical products (e.g., medical devices), and postal and courier services. NIS2 also strengthened security requirements, addressed the cybersecurity of supply chains, simplified reporting obligations, and introduced more stringent supervisory measures and enforcement requirements, including harmonised sanctions. In addition, a network of cyber security crisis liaison organisations (EU-CyCLONe) has been established.

It has also been noted that EU law pays little attention to operational risks related to information and communications technology (ICT). In September 2020, the Commission presented a proposal for

[10] European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM (2020)0823 – C9-0422/2020 – 2020/0359(COD)).

a regulation on the operational digital resilience of the financial sector (DORA),[11] to introduce and harmonise key digital operational requirements across the EU to ensure the resilience of ICT operations in the event of major operational disruptions and cyberattacks. The proposed Digital Operational Resilience Act (DORA) is designed to ensure that EU financial sector operations are able to withstand operational disruptions and cyberattacks. It provides a framework governing operational digital resilience, under which all companies must make sure they can withstand, respond to and overcome all types of ICT-related disruptions and threats. The proposed regulation covers a wide range of financial institutions, including credit institutions, payment institutions and electronic money institutions, crypto-asset service providers, central securities depositories, trading venues and trade repositories. If the DORA proposal is formally adopted, the relevant European supervisory authorities will develop technical standards to regulate all financial services institutions. Implementation will be supervised and enforced by the relevant national authorities. The package is intended to foster innovation and the spread of new financial technologies, while providing an environment that guarantees an appropriate level of protection.

In conclusion, it seems that currently the problem of data retention in the law is present and needs further resolution. After the already discussed judgment of the Court of Justice of the EU, data retention issues have been set aside, so to speak, pointing to possible violations of civil liberties, which in practice means that member states regulate data retention issues individually, more or less following the CJEU ruling.[12] This state of affairs is not conducive to combating cybercrime, which is cross-border in nature, and effectively combating it requires harmonisation of regulations over a larger area, albeit the European Union, although it would be

[11] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

[12] See: European Union Agency for Fundamental Rights, *Data retention across the EU*, https://fra.europa.eu/en/publication/2017/data-retention-across-eu (accessed on: 30.07.2023).

worthwhile to develop solutions with an even broader territorial scope. The regulations introduced so far, however, may gradually bring about evolutionary changes in the approach to data processing, which over time will take into account the balance between civil liberties and law enforcement needs.

9.5. Conclusions

In view of the above, it is postulated that work should begin on the obligation of data retention by Internet Service Providers, which are most often counted among the Internet giants, and the regulation of their activities within the European Union and cooperation with law enforcement agencies. Nowadays, it is very difficult to obtain data on suspected social media users, and to a large extent, obtaining data by investigators depends on the will of service providers, who hide behind the fact that they operate outside the European Union and thus are not subject to European jurisdiction. By failing to cooperate with law enforcement in sharing traffic data on suspected users, online platforms are essentially making it easier for cybercriminals to go unpunished.

Perhaps the most important issue, which is an extension of the previously mentioned topic, is the general issue of data retention and legislation in this regard. Within the European Union, there is a problem with international cooperation on the fight against cybercrime due to the current legislation. The initial direction of what data should be collected and how it should be collected was determined by Directive 2006/24/EC of the European Parliament and of the Council, but as we mentioned, it was challenged by the Court of Justice of the European Union, which argued that the scope of the obligations imposed and the related restrictions on rights are disproportionate, and are not necessary or are inappropriate for legitimate purposes, i.e., to ensure the availability of data for the detection, conduct and prosecution of serious crimes or to ensure the proper functioning of the EU internal market.

According to the ruling, according to the principle of proportionality, European Union acts should contain provisions that are adequate

to achieve the legitimate objectives they are intended to serve and should not go beyond what is necessary to achieve those objectives. Since then, despite the introduction of many regulations that indirectly refer to the retention of telecommunications, postal data, etc., there is still a lack of legislation that regulates this issue directly.

In Poland, although there are partial regulations that give some services access to data and that force service providers to retain data, indicating the duration of storage of knowledge held, they are the subject of a dispute among lawyers, and there is still no consensus on establishing data retention rules in relation to civil liberties, and thus no balance is achieved.

The laws in force in the various EU countries are not uniform, which is not conducive to the exchange of information that is so necessary to combat cross-border cybercrime. It seems high time to raise the need for renewed discussion among member states on the creation of a legal act that would give a framework to and address the issue of civil liberties on the one hand and the needs of investigators who need access to data on the other.

REFERENCES

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

Convention on Cybercrime (ETS No. 185), Budapest 23/11/2001 – Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States.

Directive 2006/24/EC of the European Parliament and of the Council of March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

European Union Agency for Fundamental Rights, *Data retention across the EU*, https://fra.europa.eu/en/publication/2017/data-retention-across-eu (accessed on: 30.07.2023).

European Parliament legislative resolution of 10 November 2022 on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM (2020)0823 – C9-0422/2020 – 2020/0359(COD)).

Judgment of the Court of European Union of 8 April 2014, C-293/12 and C-594/12.

Regulation (EU) 2016/679 of the European Parliament and the of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. 2023 poz. 171).

Wach, M., *Dalsze losy retencji danych po wyroku Trybunału Sprawiedliwości UE,* "Ius Novum" 2016, No. 3, p. 200.

DR RAFAŁ WIELKI
University of Opole | DOI: 10.32041/9788367149761/10

Chapter 10. Crime Analysis Against the Challenges of Cybercrime

10.1. Introduction

Cybercrime is currently one of the biggest threats occurring in the public space, causing huge economic and social costs. At the same time, law enforcement agencies are constantly looking for new ways to combat criminals who take advantage of new technologies and their constant development to remain elusive.

Several main goals can be recognise in this study. One of them is to identify the characteristics of cybercrime, whereby the priority is not to create definitions, typologies or theoretical classifications, but to identify such characteristics of crimes committed in connection with new technologies that may be of great practical importance for law enforcement agencies. In addition, I would like to propose, on the basis of the characteristics developed, methods of combating cybercrime can be useful in investigations, and which are based on information analysis. Hence, the tools of information analysis as an investigative method will be discussed along with the most appropriate analytical techniques. Legal issues that relate to the problem of data retention are also an important element in the work, since without having the right data sets, investigators will not be able to effectively use the proposed solutions and thus the fight against cybercrime will be even more difficult.

In view of such stated goals of the work, several research problems can be posed. It is necessary to obtain an answer to the question

of whether cybercrime has any characteristics that distinguish it from "traditional" crime, and whether the actions of perpetrators may differ in some way. In addition, it is necessary to examine which information analysis tools can be most effective in terms of combating cybercrime.

10.2. Characteristics of Cybercrime

Without citing the historical background of cybercrime, which seems irrelevant to the considerations carried out in this article, it can be stated without controversy that cybercrime is one of the greatest contemporary threats to public security.

Early in the field, the dominant term for the misuse of information technology was "computer crime", or "crime by computer". Over time, the prefix "cyber" began to disappear to refer to everyday activities, while only the negative connotations referring to harmful or negative activities (e.g., cybercrime, cyberbullying, cyberterrorism, cyberstalking) remained in use.[1]

It is also not the purpose of this article to provide an overview of the definition, typology, or taxonomy of cybercrime, but primarily to try to identify and describe the common characteristics specific to cybercrime *in gremio*. It is difficult, moreover, to come up with any single, universally accepted definition of cybercrime, as the phenomenon is very broad and at the same time constantly and dynamically changing. Nonetheless, for the sake of order in the deliberations to be carried out, we will look at a few universal approaches to accompany the ongoing discussions.

Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime. Such a view can be found in the reports of a professional

[1] K. Philips, J. Davidson, R. Farr, C. Burkhardt, S. Canappele, M.P. Aiken, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies,* "Forensic Sciences" 2022, No. 2, p. 381.

organisation, where it is indicated, however, it is not so important from the point of view of practice.[2]

According to another, similar, straightforward definition of the problem:

> Cybercrime involves the use of the Internet, computers, and related technologies in the commission of a crime. It includes technologically specific crimes that would not be possible without the use of computer technology as well as traditional crimes committed with the assistance of a computer.[3]

We can encounter a division of cybercrimes into: cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the Internet, criminals could not commit these crimes. Cyber-dependent crime includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data, and denial of service attacks to cause financial and/or reputational damage.[4] Cyber-enabled crimes are traditional crimes facilitated by the Internet and digital technologies. The key distinction between these categories of cybercrime is the role of ICT in the offence – whether it is the target of the offence or part of the *modus operandi*.[5]

It is worth referring to a study adopted by the UK Crown Prosecution Service on the basis of the British cyber security strategy,

---

[2] International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, Geneva 2012, p. 11–12.

[3] M.-H. Maras, *Computer Forensics: Cybercriminals, Law, and Evidence,* Burlington 2015, p. 2.

[4] Europol, *Organised Crime Threat Assessment 2018,* European Union Agency for Law Enforcement Cooperation, Hague 2018, p. 15.

[5] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime. Draft-February 2013*, United Nations, New York 2013, p. 15.

which clarifies the distinctions made with the following definitions and exemplifications.[6]

Cyber-dependent crimes are crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime (e.g., developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity). Cyber-dependent crimes fall broadly into two main categories: Illicit intrusions into computer networks, such as hacking and the disruption or downgrading of computer functionality and network space, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks. Cyber-dependent crimes are committed for many different reasons by individuals, groups and even sovereign states. For example:

- Highly skilled individuals or groups who can code and disseminate software to attack computer networks and systems, either to commit crime or facilitate others to do so.
- Individuals or groups with high skill levels but low criminal intent, for example protest hacktivists.
- Individuals or groups with low skill levels but the ability to use cyber tools developed by others.
- Organised criminal groups.
- Cyber-terrorists who intend to cause maximum disruption and impact.
- Other states and state sponsored groups launching cyber-attacks with the aim of collecting information on or compromising UK government, defence, economic and industrial assets.
- Insiders or employees with privileged access to computers and networks.

Cyber-enabled crimes are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and

[6] See: HM Government, *National Cyber Security Strategy 2016–2021*, United Kingdom 2021; The Crown Prosecution Service, *Cybercrime – Prosecution Guidance*, https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (accessed on: 07.07.2023).

data theft). These are crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology. They fall into the following categories, for example:

- Economic related cybercrime, including fraud intellectual property crime - piracy, counterfeiting and forgery.
- Online marketplaces for illegal items.
- Malicious and offensive communications, including communications sent via social media.
- Cyber bullying/trolling.
- Virtual mobbing – Offences that specifically target individuals, including cyber-enabled violence against women and girls like disclosing private sexual images without consent, cyber stalking and harassment, coercion and control. Also child sexual offences and indecent images of children, including: child sexual abuse, online grooming, prohibited and indecent images of children.
- Extreme pornography, obscene publications and prohibited images.

The definitions presented related to cybercrime are very universal in nature and practical due to the inclusion of exemplification, so let's adopt them for the purpose of this work. It is worth adding that in the case of cybercrime, defining with the use of examples is a very useful and correct move, since these phenomena are dynamically subject to change, and with the development of new technologies, new acts are and will constantly appear. Hence, resorting to typologies loses its meaning, while the proposed approach allows us to understand the essence of individual acts.

It may also be that in the future we will cease to distinguish between cyber-dependent crimes and cyber-enabled crimes, as the line between individual acts is gradually blurring, and more and more "traditional" crimes are being committed with the support of new technologies, and many cases involve electronic evidence, even if the perpetrator did not use new technologies to commit the crime at all. However, it is possible that during the commission of the crime he was carrying a cell phone, smartwatch or any other

device that – for example – is able to prove his location at a specific time, which is crucial for clarifying the circumstances of the act.

Let's look at the characteristics specific to cybercrime, as well as the motivation of the perpetrators of this type of crime, as this is crucial in terms of combating crime and adapting law enforcement's tools to fight it.

To better understand how the Internet has become a channel for criminal activity, it is important to look at the key elements of Internet technologies and distributed systems. These include:

- globalisation and "glocalization",
- distributed networks and grid technologies,
- synopticism and panopticism,
- asymmetric rather than symmetric relationships,
- data trails (data doubling, data trails, and the disappearance of disappearance),
- changes in the organisation of criminal activities.

Globalisation has expanded the reach of criminals across cultures and legal systems beyond traditional boundaries, reshaping the relationship between the global and the local, thus influencing law enforcement efforts. Distributed networks and grid technologies are creating new forms of commercial and emotional relationships between individuals that create new opportunities for victimisation. Unfortunately, these same features also generate flows of multiple information that cannot be easily captured to create consistent summaries of deviant behavior and identify new forms of risk. The simultaneous synoptic and panoptic features of Internet technologies generate new forms of victimisation. Criminals can observe their victims and commit crimes from afar. However, these same features also provide significant potential for identifying crime patterns, as well as individual criminals. The relationship between criminals and victims and the justice processes resulting from changes in the organisation of criminal activity have profound implications for the justice process. For example, the problem of multiple low-impact victims scattered across jurisdictions collectively represents

significant criminal activity, but individually does not justify the expenditure of resources to investigate or prosecute.[7]

The creation and retention of data traffic on the Internet means that we are increasingly experiencing "disappearing disappearances". Every time an electronic transaction takes place, a person leaves behind a trail of data traffic. On the one hand, this helps law enforcement; on the other hand, it combines with the requirement of access technology to recreate the "duplicate data" of an individual's identity in cyberspace, and a threat to privacy and human rights is created. Moreover, the concept of "double data" is also beginning to change the relationship between the self and the state by creating new forms of subordination to maintain levels of access and privilege. Because of the desirability (and value) of access to limited resources, data doubling generates new opportunities for identity theft. Additionally, just as there have been fairly profound changes in the nature of criminal opportunities, there have also been some interesting transformations in the organisation of criminal behavior on the Internet.[8]

Another problem is that unlike traditional crime, which is committed in one geographic location, cybercrime is committed online and is often not clearly linked to any geographic location. Therefore, a coordinated global response to the problem of cybercrime is necessary. This is largely due to the fact that there are a number of issues that pose obstacles to effectively combating cybercrime. Many criminological perspectives define crime based on social, cultural and material characteristics, and view crime as taking place in a specific geographic location. This definition of crime has made it possible to characterise it and then tailor crime prevention, mapping and measurement methods to a specific target group. However, this characterisation is not transferable to cybercrime because the environment in which cybercrime is committed often cannot

[7] D.S. Wall, *The Internet as a Conduit for Criminals*, [in:] A. Pattavina (ed.), *Information Technology and the Criminal Justice System,* Thousand Oaks 2010, pp. 78–79.

[8] Ibid, p. 79.

be attributed to a geographic location or to distinctive social or cultural groups.[9]

In addition to the obvious problem of identifying the places where cybercrimes are committed, we can also talk about the specific characteristics of cybercrime victimisation. Victims do not disclose that they have experienced a crime or simply do not realise that they have been victimised. Many victims of online crime remain anonymous until law enforcement discovers their photos or images during an investigation. The supposed anonymity of online activities often provides a false sense of security and secrecy for both the perpetrator and the victim. Cybercrimes have increasingly serious consequences as they become more widespread and sophisticated, and have a more severe economic impact than many conventional crimes. The structural uniqueness of cybercrimes is also pointed out, as they use new technologies and require high levels of skill; have a higher degree of globalisation than conventional crimes; and are relatively new. Law enforcement agencies, such as the police, lack experience in these new forms of crime. In fact, local police forces in most countries are not prepared to deal with the global nature of cybercrimes. There is no denying that these crimes are rarely reported by victims, which in turn affects their already low detection rate.[10]

Other peculiarities of cybercrime include the problem of criminals' expertise. To commit a cybercrime a person needs to have a good knowledge about the computers and the Internet. In many instances cybercrime is committed by very educated people, as they have accurate knowledge of the technology and its use, and it becomes very hard to trace them.[11] However, some maintain that the majority of cyber criminals have relatively low skills levels, but their attacks are increasingly enabled by the growing online criminal marketplace, which provides easy access to sophisticated

[9] H. Jahankhani, A. Al-Nemrat, A. Hosseinian-Far, *Cybercrime Classification and Characteristics*, [in:] B. Akhgar, A. Staniforth, F. Bosco (eds.), *Cyber Crime and Cyber Terrorism Ivestigator's Handbook*, Waltham 2014, p. 152.

[10] D. Miglani, *Characteristics of Cyber Crime,* https://deepakmiglani.com/characteristics-of-cyber-crime/ (accessed on: 02.07.2023).

[11] N. Sindhu, *Cyber Crime in India: Features, Cause and Elements of Cyber Crime,* https://www.ejusticeindia.com/cyber-crime-in-india/ (accessed on: 02.07.2023).

and bespoke tools and expertise, allowing these less skilled cybercriminals to exploit a wide range of vulnerabilities.[12]

Cybercrime is also characteristic in terms of evidence, as every action generates the creation of many digital traces of activity. However, the collecting of evidence is problematic. Virtually every modern electronic device generates a mass of digital traces that can be useful in explaining a case, but it's difficult to collect them, as is matching them to specific perpetrators, acts, etc., hence the need for law enforcement to use analytical tools to facilitate the interpretation of large data sets, as will be discussed later.

One can also consider whether cybercrime is specific in terms of the motivation of perpetrators and whether the factors leading to involvement in criminal activity differ in some way from those in 'traditional' crime. Undoubtedly, this is an intriguing question. New technologies are attractive to cybercriminals, especially in the case of various types of cyberattacks, is the massive effect their actions can have. For example, by infecting hundreds of thousands of computers with a Trojan, it is possible to launch attacks with really serious consequences at the same time. Therefore, the most daunting task in such cases is the subsequent investigation of the origin of these incidents, since it is very difficult to get to the real cause of the damage: the attacks come from thousands of infected computers from different countries, whose owners may not even be aware that they were part of the infrastructure used to carry out the attacks. This fact makes it extremely difficult to identify the true author of the attacks, so these authors can achieve attractive anonymity.[13]

It is worth noting in this context the research conducted into the motivation of cyber criminals based on interviews they gave, although it should be remembered that it only concerned hackers, therefore a narrow group of cyber criminals. Nevertheless, the authors concluded that most of them are motivated by the desire for profit, which corresponds to the most common motivation

[12] HM Government, *National …*, *op. cit.,* p. 43.

[13] J.C. Fernández-Rodríguez, F. Miralles-Muñoz, *Psychological Characteristics of Cybercrime*, [in:] J.M. Ramirez, L.A. Garcia-Segura (eds.), *Cybersprace, Advanced Sciences, and Technologies for Security Applications*, Cham 2017, p. 188.

among 'traditional' criminals, but there are also noticeable issues of interest in information, privacy, technology, or even with motives indicating a desire to change the world.[14]

A very interesting look at the motivation of cyber criminals is provided by a study prepared by researchers who reviewed the literature on the profile of cyber criminals. The scientific articles reviewed show that the most common motivations are varied, such as:

- the desire to make a profit,
- malice,
- revenge,
- ideological grounds,
- commercial sabotage or espionage,
- participation in hostilities,
- entertainment,
- curiosity,
- undertaking an intellectual challenge,
- desire for publicity, fame or recognition,
- mental health disorders,
- escape from physical life,
- vandalism,
- addictions.[15]

Unfortunately, the exact distributions of motivations in the population of criminals are not currently studied, hence the exact quantitative data are not known, although the information gathered is able to guide investigators in terms of preparing strategic programs to combat cybercrime, including using the tools of crime analysis, which will be discussed later.

To conclude the considerations related to the characteristics of cybercrime, it is worth citing how a typical cybercriminal is perceived. Criminal profiling is an extremely complex activity that is constantly undergoing scientific evaluation, so the data

[14] G. Pogrebna, M. Skilton, *Navigating New Cyber Risks. How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*, Cham 2019, pp. 32–33.

[15] M. Martineau, E. Spiridon, M. Aiken, *A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature*, "Forensic Sciences" 2023, No 3, pp. 462–463.

presented below should be treated with great caution. A viable profile of the cybercriminal will be possible to determine in the future, when data retention issues can be resolved internationally and international cooperation between police services and prosecutors' offices is strengthened.

Nevertheless, a study prepared by the University of North Dakota indicates that the typical cybercriminal is a male between the ages of 29 and 49, from the Asia-Pacific region (mainly China and Indonesia), who may work alone or in a group of about six members, or working in organised groups with a defined hierarchy of executives, managers, and workers.[16] This is very modest information, but it is worthwhile to strive in science to develop criminal profiling in the field of cybercrime that will determine the characteristics of the perpetrators, but it seems that the key here is to obtain a lot of successes by the prosecution service, which will result in the dismantling of networks of cybercriminals operating internationally, and after successfully bringing the perpetrators to justice, in the future we will be able to have more data on the basis of files research.

In conclusion, it seems that an attempt can be made to characterise cybercrime in terms of its most important specific features:

- Cybercrime is characterised by a relatively high degree of anonymity of the perpetrators, but also of the victims, making detection efforts much more difficult.
- Cybercrimes are cross-border in nature, they can be committed from almost anywhere in the world, and the virtual movement of the perpetrator can occur very quickly in time. This makes it very difficult for investigations to determine the exact place and time of the crime, which is crucial from a criminal law perspective.
- Relationships are very fuzzy among perpetrators acting in a group, we often have criminals acting together, in the same interest, but the perpetrators may not even know each other

[16] University of North Dakota, *Decrypting Cyber Crime and Profiling Cyber Masterminds,* https://onlinedegrees.und.edu/blog/decrypting-cyber-crime-and-profiling-cyber-masterminds/ (accessed on: 15.07.2023).

in the real world, which makes hierarchical structures in organised crime groups less visible. Nevertheless, the digital traces left behind can help establish relationships between perpetrators or crimes.

- Cybercriminals are generally characterised by a high degree of expertise and are adept at finding their way in the world of new technologies. However, it is likely that a not inconsiderable percentage of perpetrators – especially cyber-dependent crimes – are not at all great computer scientists, but rather are people who know how to use new technologies and take advantage of ignorance in this area on the part of the victims.
- Cybercrimes do not generate many physical traces, although they leave a great deal of intangible traces that can be analysed, but a rational analysis of the evidence must take into account the need to work with large data sets that require connecting the dots to recognise the whole picture of the criminal act.
- The motivation of cybercriminals resembles that of 'traditional' perpetrators, but it is likely that in this case a larger percentage may be those who commit criminal acts for ideological motives or to gain publicity, since the Internet significantly facilitates quick and inexpensive access to a wide audience.

The presented characteristics of cybercrime can provide important information in terms of planning investigative activities using crime analysis, the essence of which is presented in the next part of the discussion.

10.3. Crime Analysis in Cybercrime Cases

The aim of this part is to show how crime analysis – as an investigative tool – can be useful in the light of the challenges posed by cybercrime. Changes in human behaviour, through shifting means of communication, supposedly forces a change in the techniques used by analysts. Researching this problem is also important for the effectiveness of investigations. Cybercrime is characterised by multiple links, a lack of information as to where the crime

was committed, and multiple actors involved in criminal cases. Crime analysis can be an effective tool in the fight against cybercrime, but a change in the techniques used may be required.

Crime analysis is closely related to the use of criminal intelligence, which in law enforcement we can call an information management system. Criminal intelligence is the process of collecting and analysing data and information, carried out in a systematic, methodical manner, in order to identify critical problems in combating crime, determine the characteristics of these problems, and provide guidance for conducting police operations at the strategic, tactical and operational levels.

Often associated with criminal intelligence is the concept of the intelligence cycle, which is an approximation of the activities undertaken by law enforcement agencies and provides an understanding of the various cognitive processes. We should add that it is sometimes presented in many forms, so it is difficult to speak of its universal character. It was adapted for the needs of law enforcement agencies from the achievements of the military.[17] We can characterise the elements of the intelligence cycle as follows:

a) determining a course of action – when information gaps appear, it is necessary to take steps to exclude them;
b) gathering information – this is the stage for obtaining information from various sources;
c) evaluation of information – when the missing information is obtained, it is necessary to make an assessment as to its relevance, reliability, probability, etc.;
d) information processing – is associated with placing the evaluated information in the relevant databases and giving it the form necessary for further use;
e) analysis and communication of results to the recipient – this is the process of formulating conclusions from the processed information and communicating decision proposals to the final recipient. If the results are satisfactory to the recipient,

[17] J. Buckley, *Managing Intelligence: A Guide for Law Enforcement Professionals*, Boca Raton 2013, pp. 184–186.

the cycle is completed – otherwise the recipient formulates further expectations and the cycle continues.

The intelligence cycle, traditionally viewed in this way, is sometimes criticised nowadays for not taking into account part of the real intelligence work, especially in the area of defining the main concepts related to decision-making in intelligence activities. On the other hand, its usefulness is recognised in terms of training and the objectives of conceptualising strategic operations.[18]

In police science, a different paradigm has begun to emerge over time to interpret phenomena in the criminal environment and the circumstances surrounding specific acts. This model is strongly oriented toward the use of the work of crime analysts, who rely on multiple sources of information, both internal (within a particular police department or other investigative organisation) and external. The information obtained should be passed on to the relevant cells that influence criminal environments, which in turn requires intelligence units to have the right attitudes in the realm of problem identification and decision-making. Decision-makers, in turn, should take such steps as to reduce crime and positively influence criminal environments, which can be understood as the implementation of two-pronged measures aimed at both investigating a specific case and implementing preventive policies.[19] Such a concept is known as the 3-i model, which takes into account three important elements: interpret, influence, and impact.

Over time, the 3-i model mentioned above has evolved and is cited today as the 4-i model: intent, interpret, influence, and impact. Today, this is probably the most up-to-date concept of police work using analysts. The model emphasises the relationship between crime analysts and decision-makers. Decision-makers assign tasks, direct, advise and guide the analysts or crime intelligence teams. They must be sure that their intentions are clear and clarified.

[18] See: A.S. Hulnick, *What's wrong with the Intelligence Cycle,* "Intelligence and National Security" 2006, Vol. 21, No. 6, pp. 959–979; J. Ratcliffe, *The structure of Strategic Thinking*, [in:] J. Ratcliffe (ed.), *Strategic Thinking in Criminal Intelligence,* Sydney 2009, p. 9.

[19] J.H. Ratcliffe, *Intelligence-Led Policing*, "Trends and Issues in Crime and Criminal Justice" 2003, No. 248, p. 3.

With respect to the 3-i model, it is these intentions that are emphasised in the 4-i model. Analysts then interpret facts related to criminal environments and influence decision-makers with the results of crime analysis. Based on these findings, decision-makers translate the criminal environments through strategic management, the creation of action plans, investigations and operations.[20]

It seems important to mention the analysts themselves, as skilled professionals who undertake the effort to fight crime while being responsible for proper communication and for the transfer of information and analysis to decision-makers. The tasks faced by analysts are not easy, moreover, they need a certain competence to perform the tasks. Technological development has led many branches of the private and public sectors to consolidate the position of analysts. One can see a growing demand for people engaged in information analysis.

The work of an analyst is characterised by adding value to the work of others (e.g., the client or the decision maker). The multidimensional approach of analysts makes this value lie in the potential of a specific way of reasoning. This characteristic is special because of internal factors in the analyst's thinking. To put it another way, the added value in an analyst's thinking is its intriguing nature, and this becomes an important argument to emphasise its importance as a separate profession.[21] Moreover, analysts are often involved in developing data collection requirements, reorganising data collection activities, or confirming and evaluating intelligence information.[22]

Predispositions and competencies play a large role, and among the most important are high self-motivation and a constantly unsatisfied curiosity about the world, hence those toiling in this profession tend to read and observe, which leads to the discovery of new information about any objects. A separate and important issue is the definition of the relationship between the analyst and the recipient

[20] J. Ratcliffe, *Intelligence-Led Policing,* Routledge, New York 2016, p. 83.

[21] N. Hendrickson, *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets*, Lanham 2018, p. 68.

[22] J.B. Bruce, R.G. George, *Intelligence Analysis – The Emerge of a Discipline*, [in:] J.B. Bruce, R.G. George (eds.), *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Washington 2008, p. 8.

of the content of his work (usually the decision-maker). Analysts actively collect information from colleagues, taking into account the needs of investigators, including those in contact with secret sources. A certain challenge for analysts can be the fact that many decision-makers are not involved in the case from the outset, if only as principals, and it is not uncommon for decision-makers to even be from outside the police service community. In addition, it sometimes happens that there are more recipients of the analysis than one might expect, a fact that is completely beyond the analyst's knowledge at the beginning of the effort, hence it is crucial to clearly establish between the decision-maker and the analyst the tasks. The final stage requires analysts to influence the thinking of decision makers.

It is worth noting that the responsibility of an analyst is high, the competencies required to perform this profession are high, and very often we have a situation where the analyst is not properly paid, so that in the Polish reality there is a shortage of people willing to take on this type of task. We may think that the current system of recruiting candidates, as well as opportunities for professional development, should be subjected to deeper reflection.

At this point, it is already necessary to address the question of the essence of crime analysis, in order to clarify what it is and its usefulness in the conduct of criminal cases. We can trace the genesis of the use of the activity we today call crime analysis to the early 20th century. The chief of police in Berkeley, California (USA) adapted the English technique of systematically classifying the modus operandi of known perpetrators on American soil. There was developed the technique of examining recorded calls for service to perform beat analyses and was instrumental in promoting the use of "pin" or "spot" maps for visually identifying areas where crime and calls were concentrated. On the assumption of regularity of crime and similar occurrences, it is possible to tabulate these occurrences within a city and thus determine the points which have the greatest danger of such crimes and what points have the least danger.[23]

[23] S. Gottlieb, S. Arenberg, edited by S. Busack, *Crime Analysis: From Concept to Reality*, Office of Criminal Justice Planning Edition, U.S. Department of Justice, Washington 1992, p. 6.

The next stage of development took place in the Chicago Police Department, which had a section that examined daily reports of serious crimes to determine location, time, special features, and similarities with other recorded acts to help identify the perpetrator or pattern of criminal activity (modus operandi).[24] Of course, similar practices have been introduced in law enforcement practice before, but they have not been systematised or described in the form of scientific textbooks that would prove the effectiveness of this tool. Therefore, it can be concluded that this is an investigative tool that is relatively young in forensic science, at the same time it is constantly being developed, and in many places – for example, in Poland – it is still not developed enough for investigators to benefit from its entire potential. It is worth noting that the need for the development of modern crime analysis can be seen in three factors. First, there has been a need to relieve the operational staff of the police and intelligence services from dealing with the processing of the information obtained and determining the direction of its acquisition. On the other hand, the author notes that there is a not-insignificant need to improve the flow of information between cooperating services and their units. Finally, one recognises the potential of information technology, which provides more opportunities than ever to process information.[25]

Thus, we can consider that the breakthrough times for crime analysis occurred in the 1990s due to widespread computerisation and access to the Internet, while today's breakthrough can be considered as equipping crime analysis tools with solutions using artificial intelligence.

In general, crime analysis is the collection and processing of crime-related information and data and the discovery of existing patterns in order to predict, understand and empirically explain crime and delinquency, as well as to carry out evaluations of law enforcement activities or to create tactics and human resource management strategies in the broader criminal law. Although crime analysis is used by

[24] O.W. Wilson, *Police Administration*, New York 1963, p. 103.

[25] A. Ibek, *Teoretyczne podstawy analizy kryminalnej*, "Przegląd Policyjny" 2011, t. 103, nr 3, pp. 24–26.

police services, constant development shows that its potential can have wider application in the social sciences or criminology. We can speak of four main goals of crime analysis: understanding and predicting crime; creating strategic assumptions and rationalising police resources; conducting evaluations of police resource allocation efficiency; conducting evaluations of police personnel performance.[26]

In addition, crime analysis is a systematic study of crime and public disorder problems, as well as other police matters, including sociodemographic, spatial and temporal factors that can help the police fight crime, reduce public disorder and prevent crime and evaluate activities.[27]

10.4. Techniques of Crime Analysis

According to the International Criminal Police Organization (hereinafter INTERPOL), in a rapidly evolving environment, threat actors (both individual and collective) have proven to be nimble in overcoming obstacles and seeking opportunities for criminal activity. In this context, law enforcement agencies must be able to quickly detect and decipher the complex dynamics of ever-evolving criminal markets and networks in order to develop and implement the most effective strategies to prevent and combat crime. Access to accurate crime analysis is a key element in obtaining this information. This is particularly important as today's threats are related to digitalisation, which is influencing the growth of cybercrime, but also financial crime, illegal trafficking, terrorism and organised crime.[28]

Within the framework of crime analysis, its four forms can be distinguished:

1. Tactical crime analysis is the daily identification and analysis of emerging or existing patterns of criminal behavior.

[26] C.M. Lum, *Crime Analysis*, [in:] J.R. Greene (ed.), *The Encyclopedia of Police Science*, New York 2007, p. 283.

[27] R. Boba, *Crime Analysis and Crime Mapping*, Thousand Oaks 2005, p. 6.

[28] INTERPOL, *2022 INTERPOL Global Crime Trend Summary Report,* Lyon 2022, p. 3.

In addition, it is an in-depth study of recent incidents and criminal activity by examining how, when and where crime occurs, as well as how patterns, trends and potential perpetrators develop. This can also be applied to the analysis of individual cases.

2. Strategic crime analysis is treated as a study of data processing to better understand long-term crime trends.
3. Administrative crime analysis is a study related to crime research and analysis of legal, political and practical concerns to inform public administration and citizens.
4. Police operations analysis is the study of police policies and practices in order to effectively dispose of personnel assignments, funds, equipment and other resources.[29]

At this point it is worth discussing the issue of techniques that are used in the framework of crime analysis. While it is certainly not a closed catalog, the most important techniques of crime analysis include the following:

- link analysis,
- flow analysis,
- event charting,
- phone call analysis,[30]
- repeat offender and victim analysis,
- criminal history analysis,
- social media analysis,
- crime pattern analysis,
- repeat incident analysis,
- linking known offenders to past crimes,[31]
- social network analysis,
- crime mapping.

[29] G. Grana, J. Windell, *Crime and Intelligence Analysis. An Integrated Real-Time Approach*, Boca Raton 2017, pp. 219–220.

[30] See: United Nations Office on Drugs and Crime, *Criminal Intelligence: Manual for Analysts,* New York 2011, pp. 35–64.

[31] See: International Association of Crime Analysts, *Definition and Types of Crime Analysis [White Paper 2014-02]*, KS: Author, Overland Park 2014, pp. 3–4.

From the point of view of combating cybercrime, due to its characteristics, several techniques may be key. First, let's turn our attention to link analysis. The basic problem for analysts is to group information in a structured way to make it easier to extract meaning from it. Link analysis makes it possible to graphically represent information about the relationships linking objects, such as people, organisations, places, phone numbers, addresses, web domains, etc. In turn, clarifying link information by presenting it in context will help in formulating conclusions. Linkage analysis can be applied to objects that, in light of the analysed findings, are connected by mutual relationships.[32] In the case of link analysis, information is most often visualised in the form of graphs or diagrams, which should serve to simplify perception so that it is easier to understand the relationships between the various data.

There are four elements most commonly found in visualisations:

- objects (e.g.: persons, companies, organisations, places, events, means of transportation),
- relationships (connected objects, which can be family, relate to legal obligations, define roles in companies, roles in criminal organisations, etc.), and
- directions (schemas of relationship flows, indicate the side of information flow, etc.),
- strength (this is a subjective assessment of the interactions occurring within the analysed data).[33]

Linkage analysis can be a very useful tool in terms of visualising the various pieces of information gathered in a case to create a kind of map of the crime in terms of objects and the connections between them. It is a practical, very useful tool, facilitating the assimilation of large data sets in the form of diagrams, and in principle – if prosecutors had unlimited resources of analysts – this type of visualisation could be presented in every case presented before the court. At the initial stage of the investigation there may be problems with having a small set of information or the problem of lack of order, but practice shows that often from simple, inconspicuous information

[32] United Nations Office on Drugs and Crime, *Criminal…*, *op. cit.*, p. 35.
[33] Ibid., pp. 45–46.

(e.g., personal data) it is possible to build quite a sizable network of facts and links between them using open-source intelligence alone. Of course, such 'connecting the dots' requires time to search the data on the Internet to an advanced degree, but with an increase in the staffing of analytical teams in law enforcement agencies, at least in the most relevant cases, it is possible to use this technique more often.

Flow analysis can be considered a modification of this technique, but it's a tool used mainly in terms of analysing the means and benefits gained from criminal activity, e.g., money, drugs, goods, cryptocurrencies. This makes it possible to gain knowledge of who the largest amount of funds ultimately goes to, as well as what the flow of funds says about the relationships within an organised group, often also indicating the hierarchy of its members.[34]

The classic approach here is to use data retained in banking systems regarding accounts, transfers, and individuals that can be linked to particular transactions. Of course, due to the smaller number of traces left during transactions in the criminal world, handling cash will still be popular. In the case of cybercrime, we often have to deal with cryptocurrency trading. Here, much depends on the specific cryptocurrency, but in the case of the most common, Bitcoin, in general, transactions between different wallets are public and anyone can observe them online. Of course, it remains a problem to determine what specific person is the user of an anonymous cryptocurrency wallet and then obtain the wallet's password, although law enforcement success stories are known here.

Event charting generally presents a chronology of an individual's or group's activities in graphic form. In other words, it is simply a timeline that offers investigators a way to focus on individual incidents to develop an overall graphical overview of the crime. In this sense, event charting answers the question of what were the actions of that person leading up to the crime in relation to time. It is worth adding that the preparation of such charts often reveals obvious discrepancies in witness testimony or in their estimates

[34] Ibid, pp. 54.

of when the incident occurred, and often reveals potentially fruitful avenues of investigation.[35]

It is generally an organising technique rather than a strictly analytical one, but it is very useful, since in cybercrime cases the problem is generally one of attributing particular acts or movements of criminals to time and place. Nonetheless, with more data collected, it can support other techniques and allow linking of individual facts gathered in a case.

Phone call analysis is one of the most widespread techniques that can produce valuable results. It can be separated into quantitative or statistical analysis and linkage analysis. The purpose of quantitative analysis is to determine patterns in a data set based on the numerical parameters of a phone call: date, time, duration. Linkage analysis uses the results of statistical analysis and linkage diagrams to formulate hypotheses about the purpose and content of calls (i.e., the relationship and purpose for which the figureheads contact each other). The data customarily collected by telecommunications operators in the course of their ordinary business can be accessed relatively easily and with minimal resources. Perhaps the most salient feature of this type of information is that it is voluntarily (and hence usually in good faith) provided by the customer and that it can be obtained from the operators without direct contact with the subscriber. With phone call analysis, it is possible to determine the numbers dialed by the suspect's phone, identify behavioral patterns and frequently dialed numbers, gain knowledge of call frequency, call duration with date and time, locate phones based on the location of base transceiver station (BTS), and obtain any other personal information managed by the subscriber's operator.[36]

We would add that phone call analysis is crucial for obtaining basic information about the interrelationships and communications between criminals, as well as for fruitful investigation. Examining the flow of telephone information makes it possible to identify individuals who play a key role within a criminal organisation

[35] M. Sparrow, *The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects*, "Social Networks" 1991, No. 13, p. 258.

[36] United Nations Office on Drugs and Crime, *Criminal…*, *op. cit.*, pp. 59–60.

or connect different subgroups. An even broader picture can be provided by correctly interpreted statistical data, if one takes into account the amount of information and its distribution over time for a given crime. At the same time, it is difficult to disagree with the statement that the analysis of cell phone network traffic for investigative and forensic activities aimed at uncovering relational dynamics between actors is a complex task.[37]

It is perhaps the most widely used forensic analysis technique in Polish investigative practice, but one that relies mainly on data obtained from mobile network operators. On the one hand, it is hardly surprising, since the slowly-building theoretical paradigm in forensic science assumes that most people carry an electronic device generating digital traces, which is most often a cell phone, which we now refer to as a smartphone. This includes criminals who use such devices, even while committing a crime (knowingly or unknowingly).

However, I would like to point out that the way cell phone users communicate is changing, and they are – it seems we can assume so theoretically – increasingly less likely to use technologies based on the infrastructure of mobile networks, moving to cloud-based services. To illustrate, let's give a simple example: Users are increasingly sending messages via instant messaging and social media, and are increasingly having real-time conversations in this way, which allow not only voice transmission, but also simultaneous voice or video. This means that mobile network operators have very modest data, which at most can relate to network traffic, but because instant messaging and social networking applications encrypt data, it is rather impossible for services to obtain information that is typically subjected to analysis. Paradoxically, it is possible that the obligation to register SIM cards, which was supposed to limit the communications of offenders, has encouraged criminals to use instant messaging. The problem is that obtaining data from service providers is unregulated by law and very complicated in practice, and in the event that the communication took place in the mobile network, it would be

[37] S. Catanese, E. Ferrara, G. Fiurama, *Forensic Analysis of Phone Call Networks,* "Social Network Analysis and Mining" 2013, No. 3, p. 33.

much easier to obtain data from operators. The problem of data retention will be discussed later in the paper.

Social network analysis in the field of forensic science supports analytical processes concerning organised crime groups or complex social relationships of actors involved in criminal procedures. A characteristic feature of cybercrime is the so-called fuzzy connections, which make it difficult to understand the role of individual objects. The analysis of social networks allows to broaden the interpretation of the information held, and also helps to determine the roles of individual people involved in the criminal network. Among other things, it is possible to determine who is the main decision-maker in the organisation, who interacts with whom and what kind of interactions they are, whether there are different subgroups in the organisation, who is the source of linkage of different groups in the network, etc.

Social Network Analysis is an analytical tool that examines the social relationships that exist within social entities, such as a criminal network. In addition, it is able to identify the overall structure of the network, how information flows between members of the networks, important individuals and potential targets. These capabilities have led to increased interest in the method because of its potential for use by law enforcement agencies.[38]

This is the analytical tool that offers the greatest potential in terms of interpreting large data sets containing various entities and relationships between them, although it requires the use of quite sophisticated software and more thorough training of analysts. No less, it is definitely worth investing in retrofitting analysts with the skills to use social network analysis, as this technique provides answers to the greatest number of questions, thanks to the fact that it uses advanced mathematical models.

In view of the presented characteristics of cybercrime, it seems that crime, together with the presented techniques, can be an effective tool against criminals. It is a tool with great, still massively underutilised potential that can significantly contribute to

[38] M. Burcher, *Social Network Analysis and Law Enforcement. Applications for Intelligence Analysis*, Cham 2020, p. 2.

the clarification of both individual criminal cases and can be useful in planning strategic actions to combat cybercrime in some area. The key thing to remember, however, is that analytical teams need to be more numerous and present in every prosecutor's office as well as in many police units, not just at the provincial and higher levels. It is also worth bearing in mind that an analyst's salary must match his or her skills, since in the private sector analysts are regarded as one of the better-paid groups of employees, which cannot be said of the public sector. However, the effective use of crime analysis capabilities requires a wealth of data, and this in many respects can present legal challenges due to the problem of regulating data retention.

10.5. Conclusions

The research I conducted as part of the Polish-Hungarian Research Platform 2023 aimed to address three main issues related to cybercrime problems. One group of problems related to the issue of what cybercrime looks like, what characterises the acts as well as their perpetrators. The second group of problems related to the issue of investigative methods that can be useful in fighting cybercrime, and what techniques should be used to address the specific challenges posed by perpetrators. The third group of problems related to the legal issues of acquiring the data necessary to effectively fight cybercrime. The conducted research made it possible to make some – it seems – cognitively and usefully interesting observations, and at the same time contributed to the formulation of final conclusions.

First of all, it is possible to identify the characteristics of cybercrime. Cybercrimes are characterised by relatively high anonymity of the perpetrators, but also of the victims; they are cross-border in nature and can be committed from almost anywhere in the world, and the virtual movement of the perpetrator can occur very quickly in time. Cybercrimes are also characterised by fuzzy relationships and less frequent hierarchical structures in the case of organised crime groups. In addition, while cybercriminals generally have a great deal of expertise, many are simply effective in committing

crimes by exploiting their advantage in knowledge and skill in handling the virtual world over and against unwitting victims. Cybercrimes leave a great many digital footprints, but obtaining this data can be very difficult and is often not regulated by any laws. Finally, it is worth noting that there may be motivation among cybercriminals from ideological and political motives or a desire to gain publicity, which is very quickly and cheaply possible through the Internet.

In view of the above conclusions, it is necessary to propose solutions in the area of lawmaking. Among the *de lege ferenda* proposals, it is suggested that international cooperation in the prosecution of cybercrimes be tightened in general, and that as many procedures as possible be regulated in a similar manner, so that laws are not mutually exclusive in different countries. It is also worth bearing in mind that the provisions of substantive criminal law similarly define individual acts, and that the sanctions provided for are similar to each other. The development of the Council of Europe's Convention on Cybercrime was an example of effective action of this kind, but its casus shows that in the case of cybercrime there are problems with the ratification of individual specific solutions, although it is good that the general idea of a common view of criminal problems in this area has been realised. Given that cybercrime enables the rapid spread of information and the possibility of large-scale attacks, including for ideological and political motives, it seems worth considering the issue of punishment. It seems that a mass attack by means of electronic communication, even if it is only a fraud, where the victims lose a relatively small amount of money, but there are many victims, should be considered a more serious act, subject to an increase in the upper penalty limit.

It has also been shown that forensic analysis can and even should be used as one of the investigative methods against the problem of cybercrime. However, it is necessary to select the right techniques to be able to establish the basic facts, the actors in the case, and the relationships between them in scattered and multi-threaded cybercrimes. Forensic analysis can also help unravel the difficulties of determining where and when a crime was committed, especially if the electronic data left behind is subjected to additional examination. Much attention, however, should be paid to the use

of phone call analysis, as one of the most widely used analytical techniques. Nowadays, criminals are turning more often to instant messaging to communicate with each other, while at the same time the tools of communication via cell phone networks are gradually being consigned to oblivion. This fact poses a very serious challenge in the form of the lack of access to network traffic data of suspected users, as currently the retention of data collected by social media and instant messaging is not regulated either by national law or international law.

REFERENCES

Boba, R., *Crime Analysis and Crime Mapping*, Sage, Thousand Oaks 2005.

Bruce, J.B., George, R.G., *Intelligence Analysis – The Emerge of a Discipline*, [in:] Bruce, J.B., George, R.G. (eds.), *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Georgetown University Press, Washington 2008.

Buckley, J., *Managing Intelligence: A Guide for Law Enforcement Professionals*, Boca Raton 2013.

Burcher, M., *Social Network Analysis and Law Enforcement. Applications for Intelligence Analysis,* Cham 2020.

Catanese, S., Ferrara, E., Fiurama, G., *Forensic Analysis of Phone Call Networks,* "Social Network Analysis and Mining" 2013, No. 3.

Europol, *Organised Crime Threat Assessment 2018,* European Union Agency for Law Enforcement Cooperation, Hague 2018.

Fernández-Rodríguez, J.C., Miralles-Muñoz, F., *Psychological Characteristics of Cybercrime*, [in:] Ramirez, J.M., Garcia-Segura, L.A. (eds.), *Cybersprace, Advanced Sciences, and Technologies for Security Applications,* Cham 2017.

Gottlieb, S., Arenberg, S., edited by Busack, S., *Crime Analysis: From Concept to Reality*, Office of Criminal Justice Planning Edition, U.S. Department of Justice, Washington 1992.

Hendrickson, N., *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets,* Lanham 2018.

HM Government, *National Cyber Security Strategy 2016–2021,* United Kingdom 2021.

Hulnick, A.S., *What's wrong with the Intelligence Cycle*, "Intelligence and National Security" 2006, Vol. 21, No. 6, pp. 959–979.

Ibek, A., *Teoretyczne podstawy analizy kryminalnej*, "Przegląd Policyjny" 2011, t. 103, nr 3.

International Association of Crime Analysts, *Definition and Types of Crime Analysis [White Paper 2014-02]*, KS: Author, Overland Park 2014.

International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* ITU, Geneva 2012.

INTERPOL, *2022 INTERPOL Global Crime Trend Summary Report,* Lyon 2022.

Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A., *Cybercrime Classification and Characteristics,* [in:] Akhgar, B., Staniforth, A., Bosco, F. (eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Waltham 2014.

Lum, C.M., *Crime Analysis*, [in:] Greene, J.R. (ed.), *The Encyclopedia of Police Science,* New York 2007.

Maras, M.-H., *Computer Forensics: Cybercriminals, Law, and Evidence*, Burlington 2015.

Martineau, M., Spiridon, E., Aiken, M., *A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature*, "Forensic Sciences" 2023, No 3.

Miglani, D., *Characteristics of Cyber Crime*, https://deepakmiglani.com/characteristics-of-cyber-crime/ (accessed on: 02.07.2023).

Philips, K., Davidson, J., Farr, R., Burkhardt, C., Canappele, S., Aiken, M.P., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies,* "Forensic Sciences" 2022, No. 2.

Pogrebna, G., Skilton, M., *Navigating New Cyber Risks. How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*, Cham 2019.

Ratcliffe, J., *Intelligence-Led Policing*, "Trends and Issues in Crime and Criminal Justice" 2003, No. 248.

Ratcliffe, J., *Intelligence-Led Policing,* Routledge, New York 2016.

Ratcliffe, J., *The structure of Strategic Thinking*, [in:] Ratcliffe J. (ed.), *Strategic Thinking in Criminal Intelligence,* Sydney 2009.

Sindhu, N., *Cyber Crime in India: Features, Cause and Elements of Cyber Crime*, https://www.ejusticeindia.com/cyber-crime-in-india/ (accessed on: 02.07.2023).

Sparrow, M., *The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects*, "Social Networks" 1991, No. 13.

The Crown Prosecution Service, *Cybercrime – Prosecution Guidance*, https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (accessed on: 07.07.2023).

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime. Draft-February 2013*, New York 2013.

United Nations Office on Drugs and Crime, *Criminal Intelligence: Manual for Analysts*, New York 2011.

University of North Dakota, *Decrypting Cyber Crime and Profiling Cyber Masterminds,* https://onlinedegrees.und.edu/blog/decrypting-cyber-crime-and-profiling-cyber-masterminds/ (accessed on: 15.07.2023).

Wall, D.S., *The Internet as a Conduit for Criminals*, [in:] Pattavina, A. (ed.), *Information Technology and the Criminal Justice System*, Thousand Oaks 2010.

Wilson, O.W., *Police Administration*, New York 1963.