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.

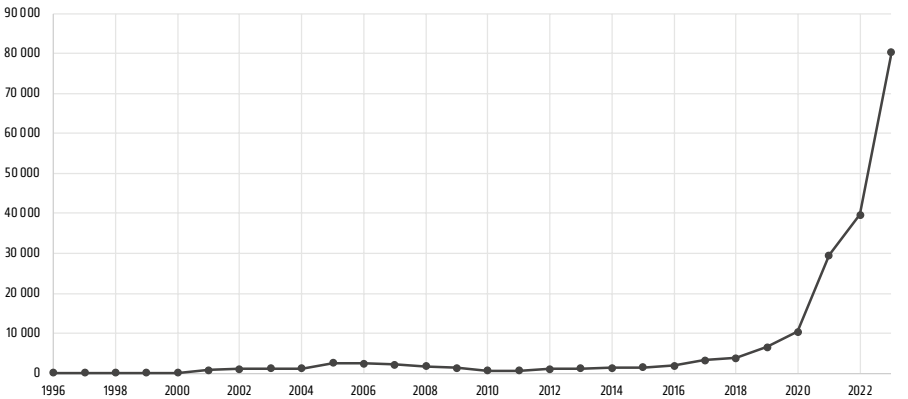
[14] Read more: *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 2018,* https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf (accessed on: 1.06.2024); *The security landscape of the Polish Internet. Annual report on the activities of CERT Polska 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).

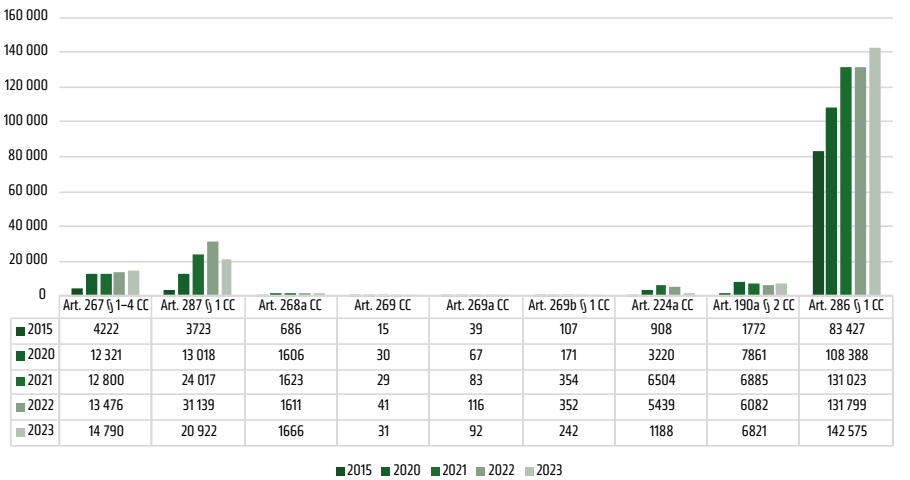
[37] Act of 4 February 1994 on Copyright and Related Rights (consolidated text Journal of Laws 2022, item 2509).

[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.