Legal labyrinth of cyberspace – a map for the responsible user

Kamil Martyniak[1]

[1]VENDETTA Law Firm & Security Center LLC, Tychy/Bielsko-Biała
Poland

***Abstract*— Today's Internet as a social medium can be perceived in many ways. In general terms, it can be a cyberspace used to provide services, sell goods, and for other purposes of public life. On the one hand, the Internet provides unlimited possibilities of freedom, access to the source of all information, but on the other hand it can be perceived as a source of threats to the accepted social order and legal order. Attacks using it are directed, among others, at systems, data and computer programs, user privacy and intellectual property. In Polish literature on the subject, the issue of counteracting and punishing crimes related to the content of information in the conditions of the perpetrator's use of electronic data processing systems has not until recently found much interest. This issue concerns not only socially and politically important and disturbing issues, which have not yet been fully scientifically developed, but is increasingly appearing in the practice of the justice system. Hence, it deserves much wider interest than before. The socially undertaken discourse on the free flow of information on the Internet and the multitude of assessments accompanying this topic prompted the author to edit the article.**

Keywords— cyberspace, law, Internet, computer crimes, information, cybersecurity.

I. NORMATIVE APPROACH TO THE ISSUE

Since 1998, Poland has also been among the countries that are adapting their legal systems to the realities of the so-called information revolution. The scope of criminalization of abuses related to the use of modern information processing technologies to disseminate illegal and harmful content and the principles of liability of entities participating in the dissemination of information prohibited by law are determined in the Polish legal system by the Act of 6 June 1997 – the Penal Code and the Act of 18 July 2002 on the provision of services by electronic means, the purpose of which was to regulate an area previously unregulated in the Polish legal system and to adapt the adopted solutions to Community law (Adamski, 2000). In the literature on the subject, there is a lack of general agreement as to the term that should be used to describe a group of prohibited acts consisting in the use of computer systems and telecommunications networks to disseminate information prohibited by law. When defining the essence of the defined crimes, the following terms are used, among others: such terms as: "crimes related to digital technology", "crimes related to information processing technology" or "internet crimes" (Adamski 2000). Terms such as "computer-related crime", "high-tech crime" are also used. (Communication from the Commission to the European Parliament, the Council and the Committee of the Regions 2007). At the same time, this type of crime is often classified as cybercrime or computer crime in general (In general, it can be stated that the group of acts referred to as cybercrimes consists in using IT systems or networks to violate any legal interest protected by criminal law. Cybercrimes also include attacks on systems, data and computer programs, i.e. a group of acts commonly referred to as *strictly* computer crimes or crimes against the security of processed information.) When discussing the issue of jurisdiction and the law applicable to the Internet, it is impossible not to refer to the concept of autonomous cyberspace law, which has won many supporters since the beginning of the global, open computer network. (Johnson, 1996). Some authors consider it justified to undertake international work on regulating the Internet as a separate place (another reality) in relation to the real world, granting it its own legal order. (Post, 2009). Such a separate legal order could apply to torts related in particular to such areas as: copyright law, industrial property law, protection of personal rights or selected issues of press and civil law. (Barta, 1997). According to the supporters of this concept, the establishment of a separate

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 28, No 4 (2024), pages 5
https://doi.org/10.19192/wsfip.sj4.2024.20
Received: November 2024, Accepted: December 2024,
Published: December 2024

cyberspace law will eliminate doubts related to jurisdiction and applicable law, and what is more, it will enable the development of new legal structures specific only to the Internet, without the risk of violating existing legal paradigms, e.g. in the sphere of copyright law. (Barta, 1997). This law could also deal with the issue of the flow of protected goods (including works) between the real world and the computer network. This concept is criticized by some authors (Kronke, 1998). They point out that there is no such thing as cyberspace in the sense of a separate space that would be regulated by separate, private international law. Acts are always committed in a specific, real and identifiable area, and damage occurs in the real world, usually within the strictly defined territorial framework of a given country. However, the issue of determining the appropriate connecting factor, such as the place of committing the act or its effect, is a completely different issue. However, it does not determine the need to exclude the application of the current conflict rules on the basis of some unspecified, virtual space. On the contrary, it is still justified to seek the jurisdiction of the courts and law of the interested countries, although it must be admitted that, as a rule, there will be a great many of these courts and national laws at stake. H. Kronke emphasizes that having familiarized himself with the literature on cyberspace, which deals with both hypothetical and actual cases in court practice, he has never encountered cases in which specific acts or their effects could not be linked to real space and its proper legal order. (Kronke, 1998). However, this author cannot deny that the Internet is characterized by many specific features that require modification of the existing rules. These include, among others, significant difficulties in identifying the parties, decentralized method of transmitting information (which may affect the indication, usually wrongly, of the jurisdiction of the courts or the law of the countries through which a given information or part of it flows (which is characteristic of the network), or in which certain technical means are located, such as servers , the possibility of access to information by third parties (e.g. server administrators), the occurrence of links, i.e. a system of connections between websites, and most importantly, potentially universal availability of all kinds of information of a tort nature (Świerczyński, 2004).Cyberspace is subject to specific limitations, which K. Węderska divided into four areas – law, space, security and threats. Each of them encounters specific problems in its field, such as inconsistency and lack of international standards in the area of law, lack of spatial, geographical boundaries in the area of space or lack of uniform solutions in the matter of security of virtual networks (Table 1).

TABLE 1. AREAS OF SPECIFIC RESTRICTIONS IN CYBERSPACE

Area	Characteristic
LAW (law)	- law unclear - inconsistent; - unclear responsibility for actions and misdemeanors; - no international (national) criteria classification and qualifications; - imprecise definitions of criminal acts and acts of threats to national security.
SPACE (space)	- no spatial boundaries; – no political boundaries; – no geographical boundaries;
	– no immediate boundaries.
THREATS (threats)	- simple, widely available technology; – anonymity of the case; – multiple forms of cyberattacks; – "domino effect" as a consequence; – characteristics of “weapons of mass disruption”; – low attack costs.
SECURITY (safety)	- lack of quick and effective solutions securing; – multitude of threat objects (attacks); – high security costs; – varied susceptibility of objects; – unpredictability of threat sources; – very high costs.

Source: (Sienkiewicz, 2015)

The issue of state jurisdiction in relation to virtual space is of key importance, especially for criminal proceedings. The justice system, and especially law enforcement agencies, may encounter significant problems when acts prohibited by the legal order of a given country are committed by a person or through a server located in another country. Similarly, in the case of typical computer crimes, such as hacking, computer sabotage or cyberterrorism, determining the place where the crime was committed is problematic, because the cybercriminal may be in another country and using a laptop or telephone to use a wireless Internet or telephone connection that makes it difficult to locate him. Such situations are increasingly common in the Polish justice system, and law enforcement agencies, acting within the procedure of detecting the perpetrators of these acts, are often forced to cooperate with IT specialists.

II. THREATS

In addition to the benefits associated with the functioning of the information society, there are also threats and new problems associated with the virtual space. "The phenomena and processes taking place in cyberspace go far beyond the technical dimension, taking on a social character. We are currently witnessing the formation of the so-called information society, i.e., regardless of various attempts to define it, a society with profound changes in social awareness, caused by the effects of the digital revolution, affecting the surrounding reality in a multidimensional, economic, political, cultural, and social way through information. This society is sometimes referred to as a risk society, due to the possible implications of threats to the security of an individual and human communities occurring in cyberspace" (Białoskórski, 2011). Threats in cyberspace concern individuals, social groups, organizations, and even states. Each of the functioning information and telecommunications systems may be associated with specific threats and susceptibility to certain criminal activities. The first group of threats is sabotage and unintentional threats, which are characterized by the occurrence of damage without direct material or informational gain. This category includes power failures, fires, natural disasters, disintegration, and other physical destructive factors. Computer viruses, logic bombs, and Trojan horses can be forms of disintegration or destruction of information, while physical destructive factors include

explosives that destroy computer equipment (Czechowski, 1993). The second group of threats is infiltration, or "actions by unauthorized persons aimed at penetrating various elements of an information system or telecommunications network in order to obtain information by various methods and means" (Czechowski, 1993). A characteristic feature of this method is the orientation towards the perpetrator gaining profit from the information obtained. Infiltration is divided into two categories - active and passive infiltration. Passive infiltration is tracking information in a specific place of its circulation. The most commonly used techniques are:

- "electromagnetic interception, consisting either in gaining access to the connections between the computer and terminals or in the directed emission of radiation and analysis of the signal reflected from the radiating device;
- connecting to data transmission lines in telecommunications networks or intercepting signals transmitted by radio;
- examining and copying unprotected resources (software piracy);
- analysis of waste paper or remnants of information carriers, resulting from either carelessness in waste paper management or disregard of the obligation to demagnetize information carriers;
- use of hidden transmitters" (Czechowski, 1993).

Active infiltration is the deliberate gaining of access to a system with the intention of interfering with the most sensitive and important links in the system. It often takes the following forms:

- "breaking security in order to access any place in the IT system while bypassing the security measures used by the legitimate user of the system (for example, accessing the security register) (...);
- interference with the structures of operating systems;
- impersonating an authorized user of computer systems;
- use of additional programs and procedures (placed in the software writing phase or during software operation)" (Czechowski, 1993).

Information warfare can take many forms. P. Sienkiewicz and H. Świeboda indicate four methods of attack - electromagnetic, fire, psychological actions and disinformation. Each of the above categories will cause different direct and further effects (Table 2). However, the goal is always the same - weakening the opponent, disinformation and destruction of his resources.

TABLE 2: EXAMPLE OF A COUNTRY-LEVEL THREAT SCENARIO

Type of destructive action	Direct effect	Further effect	Countermeasure
Electromagnetic attack. Release of electromagnetic pulses in the areas of network nodes. Launch of devices that disrupt the operation of wireless communication transmitters.	Disinformation The spreading of false information via email and other means of social communication.	Loss of administrative information. Disruption or paralysis of the city administration system. Increased sense of threat and social dissatisfaction.	Detection and assessment of threats. Immunity of devices and premises to electromagnetic attack. Organization of a system for restoring the efficiency of the system after an attack.
Fire attack. Detonation of explosive charges within network nodes. Interruption of network trunk lines.	Destruction of telephone exchanges and server rooms - paralysis of network operation. Disruption of work or paralysis of the city administration system.	Loss of administrative information. Disruption of the state administration system. Increased sense of threat and social dissatisfaction.	Detection and assessment of threats. Physically hardening the network against fire attack. Organizing a system for restoring the system's efficiency after an attack.
Psychological activities. Social engineering - recruiting office staff to participate in attacks.	Providing access to the computer network of state administration systems, disclosing classified information. Internal sabotage by recruited personnel. Financial frauds by administration employees.	External IT attack on the network. Threat to the information security of the state. Theft of classified information (e.g. personal or financial data). Deterioration of financial security. Disruptions in state administration. Increased sense of threat and social dissatisfaction.	Detecting and assessing threats. Raising awareness of personal statuses. Improving information access control procedures.
Disinformation. Disseminating false information via email and other means of social communication.	Questioning the honest intentions of the authorities and management of the state administration system organizations. Undermining the credibility and qualifications of selected staff groups. Spreading false information about the intentions of the state authorities. Providing false information about work for the interests of foreign countries and organizations by representatives of the authorities.	Causing concern, worsening moods, attempts to cause panic, worsening the quality of the state's functioning. Attempts to undermine the financial stability and financial liquidity of the state. Increased sense of threat and social dissatisfaction.	Rapid response of authorities to false information. Efficient reaching of the population and company personnel with objective information. Preserving the truth in informing. Detecting and stigmatizing disinformants.

Source: (Sienkiewicz, Świeboda, 2004).

The state may experience various types of threats aimed at weakening the centers of power. These will not only be physical attacks on systems and networks causing destruction of

electronic and electrical devices, teleinformatic networks, telephone exchanges or disruption of work or paralysis of these networks. Information warfare also takes place in the mental sphere by causing chaos, disinformation of society and the use of social engineering to persuade state personnel to participate in attacks. Information warfare can be conducted by both state entities (e.g. armed forces) and non-state entities, which through their actions can affect the security of the state. The first category includes perpetrators of "systemic" threats, i.e. state organizations, terrorist organizations or organized crime groups. The second category are perpetrators of "common" threats, i.e. vandals, hackers, crackers. These entities operate in three stages. First, they recognize the weak points of a system or an object, then they gain access to it, in order to - in the final stage - fulfill their goal, which may be theft, copying or modification of data (Sienkiewicz, 2006). In theory, the most serious consequences could be a cyberattack carried out by a state against a state. Such a form of aggression could be considered an attack within the meaning of Article 5 of the North Atlantic Treaty (North Atlantic Treaty, 1949), and consequently lead to an interstate conflict and armed actions. In practice, however, the perpetrators of attacks are more often non-state entities than state entities. This is due to several factors. The first is the greater ease of making a decision to attack (in the case of state services, this decision is more formalized, subject to plans, procedures, and service subordination), the decentralized structure means that taking appropriate steps can be a unilateral decision of the leader or a narrow group of people. In the case of an attack carried out by a single person, the decision to do so may be made even as a result of the emotional state of the perpetrator. The second is the possibility of achieving one's own goals. In the case of non-state entities, electronic attacks are often the only way to achieve their goals. In the case of state entities, the range of possible actions is much wider. Some legal theorists claim that states have many instruments to influence foreign governments, and they use electronic attacks with considerable caution, fearing serious consequences on the international stage (Trelikowski, 2009).

III. Law

The measures taken to prevent cybercrime cannot be limited to the establishment of appropriate legal regulations for this matter, because they are not able to stop all cases of illegal use of the Internet (Siwicki, 2011). Due to the complexity of the discussed phenomenon, the implementation of criminal law provisions is still a novelty in the criminological approach, as well as in the legal system itself, and it goes very deeply into the technical area of functioning of data processing systems (Wójcik, 2011). Perpetrators often take advantage of differences in the scope of criminalization, or technological solutions that significantly hinder their identification. Therefore, from the point of view of eliminating criminal behavior, a much more effective method than criminal repression seems to be reducing the risk of committing this type of abuse based on Internet service providers and users themselves (Siwicki, 2011).

Here are some key internet security laws that aim to protect personal data and ensure information security:

Penal Code (Journal of Laws 2024, item 17)

- **Article 268a** : concerns unauthorized access to computer data. This provision penalizes actions such as destroying, deleting or changing data without appropriate authorization.

General Data Protection Regulation (GDPR)

- **Art. 32** : imposes an obligation on data controllers to implement appropriate technical and organisational measures to ensure the security of personal data processing.

Personal Data Protection Act (Journal of Laws 2018, item 1000)

- It supplements the GDPR in the Polish legal order by specifying detailed rules on the protection of personal data, including security requirements.

Act on the provision of services by electronic means (Journal of Laws 2024, item 1513)

- Regulates the rules for the provision of services on the Internet, including the obligations of service providers in the field of data protection and information security.

Classified Information Protection Act (Journal of Laws 2024, item 1222)

- It specifies the principles of protecting information that is considered confidential, including in the context of its processing in IT systems.

Act on the national cybersecurity system (Journal of Laws 2024, item 1077)

- It introduces a legal framework for the protection of information systems, including obligations for essential service operators and digital service providers to ensure security.

Press Law (Journal of Laws 2018, item 1914)

- Regulates responsibility for publishing information on the Internet, including rules on the protection of personal data in the context of the media.

IV. Summary

Cyberattacks are a problem affecting states, international organizations, corporations, businesses, and individuals. Criminal activities in cyberspace include theft, hacking, sabotage, espionage, surveillance, destruction or modification of data, and fraud. We cannot forget about the threats of cyberterrorism or even cyberwar. Cybersecurity can therefore be considered a new challenge of the 21st century. That is why there are increasingly voices about the need to tighten security systems, new legal regulations, discussions at the international level, and initiatives aimed at educating societies about security and law in cyberspace. The Internet community is certainly a form of information society. Threats related to cyberspace cannot be easily identified and classified into a closed catalog. Constant changes and development of

technology make it extremely difficult to control cyberspace. The dynamics of changes in this area result in a huge number of regulatory challenges. The global reach of the Internet intensifies this phenomenon. Building an information society requires the creation of an appropriate legal base. However, these should be international standards, because the architecture of cyberspace means that undertaking appropriate work at national levels will be insufficient to effectively and comprehensively regulate both issues related to the information society and potential threats occurring in the virtual space (Worona, 2017). Due to the increasing role played by ICT systems, both in the life of society and in the state infrastructure, cyberspace has become the subject of interest not only of contemporary legal doctrine, but also of scientific thought. It was necessary and still is necessary to study the new, digital environment, which has influenced not only the form of concluding civil law contracts or performing administrative activities, but above all contributed to the emergence of new forms of crime. With the progress of civilization, new forms of threats will begin to appear in the state's cybersecurity system, and consequently, new methods of legal pragmatics in the activities of Internet users and law enforcement agencies will have to be directed in the effective fight against these phenomena. The indicated legal provisions are intended not only to protect personal data, but also to ensure security on the Internet, which is crucial in the era of the growing number of cyber threats. As technology evolves, it is necessary to continually adapt legal regulations to new challenges.

V. REFERENCES:

Adamski A., *Prawo karne komputerowe*, C. H. BECK, Wrocław 2000, s. XVIII.

Barta J., Markiewicz R., *Prawo cyberprzestrzeni i stare konwencje* [w:] "Rzeczpospolita" z 15 listopada 1997 r., nr 266, s. 37.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI w. - zarys problematyki*, Warszawa 2011, s. 13.

Czechowski R., Sienkiewicz P., *Przestępcze oblicza komputerów*, Warszawa 1993, s. 133-134.

Johnson D. R., D. G. Post: *Law And Borders - The Rise of Law in Cyberspace*, Stanford Law Review nr 48 (1996), s. 173.

Kronke H., *Applicable Law in Torts and Contracts in Cyberspace* [w:] Which Court Decides? Which Law Applies?, The Hague, London - Boston 1998, s. 65.

Post J., *Law and Order - The Rule of Informations*, 2009, s. 1367.

Sienkiewicz P., *Ontologia cyberprzestrzeni*, „Zeszyty Naukowe WWSI" 2015, nr 13, t. 9, s. 98.

Sienkiewicz P., Świeboda H., *Niebezpieczna przestrzeń cybernetyczna*, Transformacje 2006, t. 47-50, s. 58 na podstawie J.A. Warden, The Enemy as a System, „Air Power Journal" 1995, t. 9, nr 1, s. 90-92.

Siwicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 80-81.

Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, Wolters Kluwer Polska, Warszawa 2011, s. 258.

Świerczyński M., *Koncepcja autonomicznego prawa cyberprzestrzeni* [w:] Prawo Internetu, Wydawnictwo Prawnicze LexisNexis Sp. z o. o., Warszawa 2004, s. 164.

Trelikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, [w:] M. Madej, M. Trelikowski (red.), Bezpieczeństwo teleinformatyczne państwa, Warszawa 2009, s. 96-97.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Uniwersytet w Białymstoku, Białystok 2017, s. 65.

Wójcik J. W., *Cyberprzestępczość. Wybrane zagadnienia kryminologiczne i prawne*, „Problemy Prawa i Administracji" 2011, nr 1, s. 155.

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 r., Bruksela, KOM(2007) 267 wersja ostateczna, *W kierunku ogólnej strategii zwalczania cyberprzestępczości.*

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., Dz.U.z 2000 r., Nr 87, poz. 970.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. 2024 poz. 17)

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000)

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2024 poz. 1513)

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2024 r. poz. 1222)

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2024 poz. 1077)

Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U.2018 poz. 1914)