European Research Studies Journal
Volume XXIV, Issue 2, 2020

pp. 68-77

Information Security in Poland and in the European Union: Administrative and Legal Conditions

Submitted 03/03/21, 1st revision 27/03/21, 2nd revision 23/04/21, accepted 185/05/21

Boguław Kogut[1] Marek Magniszewski[2]
Paweł Lubiewski[3] Stanisław Topolewski[4]

Abstract:

Purpose: *Information has an impact on the attitudes, behavior and actions of its recipients, and given its important role in public life, it should be subject to appropriate protection to ensure its security. It therefore becomes important to create appropriate administrative and legal conditions for the protection of information security, which is currently a priority both in Poland and in the European Union.*
Design/Methodology/Approach: *The research was conducted using the methods of problem analysis and synthesis, with the main objective being to optimize the research field with a view to future studies.*
Findings: *The research analysis has found the significant impact of administrative and legal conditions, in particular the need to create normative solutions to ensure information security. Due to the category of threats to information security, the desired solutions concern both Poland in particular and the European Union as a whole.*
Practical Implications: *The problems addressed in the paper may help raise awareness of the rapid spread of information security and generate interest for different bodies in the category of related threats..*
Originality: *The paper tackles problems that are particularly important nowadays from the standpoint of both individual citizens as well as different entities which use information, regardless of their function in society.*

Keywords: *Security, administarttive and legal conditions, normative solutions.*

JEL codes: *J52, K15.*

Paper type: *Research paper.*

[1]*Academia WSB in Dabrowa Gornicza, Poland, ORCID: 0000-0003-4431-8283.*
bogkog@gmail.com
[2]*Rzeszow University of Technology, Poland, ORCID: 0000-0002-9088-8159, agniszewski@prz.edu.pl*
[3]*Police Academy in Szczytno, Poland, ORCID: 0000-0001-5149-7908, pawel.lubiewski@onet.eu*
[4]*University of Natural Sciences and Humanities in Siedlce, Poland, ORCID: 0000-0001-8268-3754, stanislaw_topolewski@wp.pl*

1. Introduction

The need to provide protection of information (beyond merely legal) gave rise to a new field known as information security. The concepts of information security and information safety are sometimes confused in the literature. Information security is generally defined as the protection of information against undesirable (intended and unintended) access, dissemination, destruction or deletion, as well as against the introduction of unauthorized changes and their further processing. This implies taking a number of active, protective measures to effectively secure and protect the properties of information, mainly its confidentiality, integrity and availability. Information security therefore encompasses a wide range of activities, procedures and methods used by authorized entities to safeguard, to the broadest extent possible, the integrity of the collected, processed and stored information resources (Potejko, 2009).

Attempts to define the concept of information security in Poland are reflected in the country's most important state documents, the White Paper and *The National Security Strategy of the Republic of Poland* (2014). In Appendix two, containing a list of conceptual categories included in the White Paper, we read that "information security is a transsectoral area of security whose objective, methods, measures and conditions relate to the information environment of the state, including cyberspace". *The National Security Strategy of the Republic of Poland*, meanwhile, presents a strict orientation of the concept of information security towards the field of protection, with reference being made exclusively to the security of classified information (Wiśniewski and Jakubczak, 2016).

In the academic literature, information security is considered to be the state of certainty and trust of an entity regarding the possibility of obtaining quality information and protecting it against loss. We can therefore conclude that the information-security system model consists of elements such as: humans (as subjects of information) and technology (means, systems), along with the processes taking place in-between in human environment. As already mentioned, information security is often mistakenly identified or cited in the context of information safety. Information safety is a narrower concept that forms part of the broader concept of information security. It should be strongly emphasized that information stored in databases should be protected. This mainly concerns strategic data which is of key importance to the functioning of entities such as businesses. An information system supporting strategic management should be sensitive to the problem area of information security by defining the general principles, methods and tools for the protection and monitoring of information.

Information security focuses on physical, legal, procedural and technical measures aimed at protecting information resources, whereas information safety views information merely as a product whose value depends on the security of its properties.. In what concerns the broadly outlined information-security model, its core components are, information security, information safety, information-security policy,

information-safety policy, information combat, information warfare (Kubiak and Topolewski, 2016).

State-provided information security affects internal and external security. Widespread globalization and the advancing information society and ICTs have greatly changed the current security environment at state level, including that of the Republic of Poland. Both internationally and internally nowadays, information warfare is an important challenge to beware of, as it transcends nearly all areas of public life (Wiśniewski and Jakubczak, 2016).

2. Cyberspace as an Area of Information Flow

Information security is closely linked to technological development (Jurgilewicz *et al.*, 2020; Wiśniewski, 2020). It is therefore not particularly surprising that the embrace of the Internet, coupled with a number of ongoing globalization processes, have contributed significantly to the growing importance of information security. The very term "cyberspace" is a mashup of two words, "cyber" and "space", the first of which derives from cybernetics, that is the science of control and communication, which focuses on the principles of operation of certain auto-steering systems (Liderman, 2012), whereas “space” alludes not so much to the literal, physical extent, but has instead a more abstract meaning in which a non-existent three-dimensional, artificial space enables the occurrence of certain correlations.

Let us note that, in Poland, the definition of cyberspace entered into force via the Act of 2 November 2011 amending the legal regulations of states of emergency. “Having incorporated cyberspace protection into the Polish legal system, [the Act] also introduced a definition of the concept of cyberspace. Based on the assumptions of the draft *Government Program for Cyberspace Protection of the Republic of Poland for 2011-2016* (ultimately passed in mid-2013 under the name *Cyberspace Protection Policy of the Republic of Poland*), "cyberspace" is to be understood – as per section 1.1. therein – as a space of processing and exchanging information created by the ICT systems, as defined in Article 3 point 3 of the Act of 17 February 2005 on the informatization of entities performing public tasks, together with links between them and the relations with users” (Wasilewski, 2013).

Furthermore, owing to the accession of Poland to the North Atlantic Alliance in 1999, the legal provisions binding at the level of that organization remain fully binding with the provisions of domestic law. Hence, the document explaining NATO terminology also includes the concept of cyberspace, which is defined as a specific domain functioning in the information environment and comprising interdependent information and telecommunications networks along with technical infrastructure and residence data. When defining cyberspace, we should also bear in mind its singularities, most notably its non-territoriality, meaning the inability to physically determine its geographical location. Aside from that, cyberspace is an open structure, which means that it can be accessed by anyone and disseminated freely. In other

words, cyberspace exists so long as IT systems and networks are functional and able to transmit information. Cyberspace is also marked by the anonymity of network users, although in strictly operational and technical terms, the user's identity can in most cases be traced on the basis of their equipment's IP address. An equally important feature of cyberspace is the unprecedented speed of information transfer and the mass nature of interactions and social relations occurring within the broadly understood virtual space (Colesniuc, 2013).

3. The Essence of Threats to Information Security

A security threat means, broadly speaking, a certain state or situation in which factors exist that may, whether directly or indirectly, expose an individual (or another security entity) to the loss of goods, values, or in any other real way cause a sense of fear, anxiety or uncertainty regarding their survival and proper functioning. Threat may also imply a potential or real action which, again directly or indirectly, affects its subject and which can be perceived objectively or subjectively in terms of both military and non-military threats. Apart from the determinants of information-security threats, attention should also be paid to the very nature of these threats. Existing theories regarding information threats indicate that they can divided into incidental and non-incidental. Incidental events are related to environmental factors, not targeting by themselves the area of information security; these can be random or result from other potentially threatening activities. On the other hand, non-incidental events have a specific purpose, are strictly organized and thoroughly thought-out, while their execution is preceded by intensive planning; these are aimed at disrupting the process of transmitting or accessing information in IT systems, manipulation or modification of data, or its theft, disclosure or illegal use (Jurgilewicz *et al.,* 2019).

Information is currently perceived as one of the most valuable drivers of a state's power and of its relative advantage in the global arena. No wonder then that, over the years, intelligence activities have gained in momentum and in importance. Intelligence, being a state institution, focuses on the methods and abilities of obtaining information for the purposes of state activities. One of these activities is espionage, which - from the perspective of information security - is a threat due to the very fact of data interception but also because of its possible implications. "The presence of information technology in the real world is contributing to the virtualization of international relations, therefore discussion on cyberterrorism and cyberwar as new threats to national and international security is becoming commonplace. This discourse is becoming extremely popular, and to a certain extent, even fashionable" (Eriksson and Giacomello, 2006).

As a result of the progressive informatization and information-based espionage, cyberspace has become not only a tool for collecting information and processing it in real time, but also for analyzing huge amounts of data in a relatively short time and creating predictive models of behavior. In this way, a new field has emerged, referred to in the literature as cyber espionage, which consists in obtaining, stealing or gaining

access to confidential, classified information from an individual, a business, a research center, an organization or a government, using to this end the ICT infrastructure and computer systems where this data is located. Due to the reduced risk of detecting the actual culprit, cyber espionage is currently one of the most actively pursued techniques of spying. Another very important threat to information security are cyberterrorism and information terrorism. As a rule, terrorist activities intend to force changes in the political landscape (mainly through the use of violence), intimidate a part of the population, and manifest certain ideological views. The same can be said of cyberterrorism, which itself is a combination of two concepts: terrorism and cyberspace. Let us note that cyberterrorism does not concern just illegal attacks on ICT infrastructure, computer networks and information stored therein, but also the very threat of such attack (Bellaby, 2016)[5].

Threats to state cyber security include remote and unauthorized interference with ICT systems aimed at disrupting work, taking control or intercepting data belonging to state services, public institutions or commercial and individual users (Terlikowski, 2009). In turn, the term "cybercrime" - as has already been mentioned – refers to the forms of using telecommunications networks, computer networks and the Internet for the purpose of violating any good that is protected by law. Nowadays, nearly all illegal activities are reflected on the Internet in one way or another. "The global nature of the Internet has enabled instantaneous communication and the transfer of most forms of human activity to the Internet, including those negative. Cyberspace is being increasingly often referred to as a new social paradigm where real-world problems are mirrored. Cybercrime is therefore a modern type of crime that takes advantage of digital technologies and of networked environment" (Białoskórski, 2011; Gniadek, 2009).

The most vulnerable IT systems include air-traffic control and management systems, land-transport and transmission systems, public and government-administration systems, internal systems of state institutions, especially crisis-management and emergency-alert services, systems of strategically important sectors (energy, banking, telecommunications, water supply). Another important threat is the increasingly common "hacking" of the servers of institutions established to combat terrorist organizations. An effective attack on databases, communication channels, etc. allows the aggressors to gain access to information such as that on actions being planned against them. Cyberterrorism is a mashup of the terms "cyberspace" and "terrorism". Cyberspace is a virtual world; a symbolic, intangible, binary place where computer programs operate and where multiple data are moved. Terrorism, according to the definition adopted by the US Department of State, is a carefully planned, politically motivated act of violence against various non-combatant targets, used mainly by subnational groups or secret agents and most often aimed at exerting pressure on the targeted victim. The FBI, meanwhile, uses the definition according to which "terrorism is the unlawful use of force or violence, mainly against persons and

[5] *http://www.iwar.org.uk/cyberterror/resources/house/00-05-23denning.htm.*

property, in order to intimidate or coerce the government, the civilian population, or a part thereof, with the aim of promoting political or social goals" (Aleksandrowicz, 2008). In view of the above, cyberterrorism can be said to be a deliberate, politically-motivated act of violence directed against the information, computer systems and data of non-combatant groups by subnational groups or secret agents. The main target of the attack is the systems of the critical ICT infrastructure. The scale of this phenomenon should also be heeded. For example, CERT Polska published in 2019 the annual report titled *The Security Landscape of the Polish Internet* which provides an overview of the registered threats faced by Polish Internet users in 2019. According to that report, individuals reported 1,212 such incidents (18.7%), banking entities - 1,057 (16.3%), media entities - 748 (11.5%), wholesalers and retailers - 624 (9.6%), and finally, digital infrastructure - 550 (8.5%). The report shows that *phishing* was by far the most popular type of incident reported to CERT Polska last year, accounting for over half of all cases (54.2%, to be exact) [6].

Meanwhile, the most echoed cases of hacker attacks in Poland in recent years have seemed to target and generate financial losses for local governments, namely: in Gidle – PLN 300,000, in Rząśnia – PLN 500,000, in Jaworzno Municipal Office - over PLN 2 million, Podlaskie Province Traffic Authority - approx. PLN 3.7 million[7].

The progressing informatization at global level, combined with the gradual process of making virtually all areas of public life dependent on information, has offset a race in accessing it and gaining advantage over other international players. While this is not exactly anything new, given that over the centuries information was acquired and knowledge expanded, but ever since the technological revolution, new powerful tools for obtaining and utilizing information have emerged and their potential has not gone unnoticed. Due to the role they play and the vast opportunities they offer, a phenomenon known as information warfare, or information combat, has emerged. Information warfare, itself a product of competition between states, influences public awareness at the level of information through means and methods of controlling information resources using to this end the available IT infrastructure (Ciborowski, 2001; Durczewska 2014).

Last but not least, let us briefly discuss two other worrying phenomena. One is information void (lack of access to information), which can be due to the state's poorly developed intelligence and counterintelligence infrastructure, while the other is information noise (excess of information), which is triggered by the widespread sharing of content without comprehensive state supervision. The existing security gaps encourage unauthorized users to modify or misuse ITC infrastructure, or in any case, leave the gates open for accessing these system resources at a convenient time.

[6]*https://www.computerworld.pl/news/Raport-Cert-Polska-pokazuje-zagrozenia-z-jakimi-mieli-w-zeszlym-roku-do-czynienia-uzytkownicy-internetu,421995.html.*
[7]*https://ikmj.com/cyberbezpieczenstwo-w-polsce-statystyki.*

4. Information Security in Cyberspace

Information security of a country cannot be effectively ensured without cooperation with other countries. This includes numerous organizational and legal undertakings concerning the formation of policies, strategies and regulations for information protection, as well as network users traffic within their respective area. In Poland, for matters related to information security at state level, legal regulations are primarily outlined in the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws No. 78, item 483, as amended). Art. 54 of the Constitution grants every citizen the universal right to freedom of expression and to obtaining and disseminating information, while art. 49 ensures protection of the above-mentioned freedoms, including them among the fundamental values subject to protection, bearing in mind the freedom and will of every human being to obtain, transfer, gather and reproduce information. Lastly, art. 61 extends the scope of the rights held by the possibility of gaining access to data on the activities of public authorities and administration.

A breakthrough in Poland, in terms of regulating matters related to cybersecurity and the protection of critical infrastructure, came with the Crisis Management Act of 26 April 2007, in which an obligation was imposed on the government administration to ensure the smooth operation of critical infrastructure. This includes: collecting and processing information on threats to critical infrastructure; development and implementation of procedures in the event of threats to critical infrastructure; critical-infrastructure recovery; cooperation between public administration and (in)dependent owners of facilities, installations or devices of critical infrastructure in the scope of its protection (art. 6 of the Crisis Management Act). The entity implementing the policy of critical-infrastructure protection was the Government Center for Security with the support of the Ministry of Infrastructure and Development, among other entities (Wasilewski, 2013).

When speaking about the legal regulations concerning information security, the Act of 6 June 1997 Penal Code (OJ 2019, item 1950, as amended, hereinafter the Penal Code) is another important document to note. Chapter XXXIII of the Penal Code regulates the issues related to offenses against the protection of information which refer to data of particular importance for the country's defense or which have been classified, as well as other important information or violations of ICT systems. Art. 265 and 266 Penal Code provide for legal sanctions in the event of disclosure or use of classified information marked with secrecy clauses (top secret, restricted, confidential), including when such a breach results from the official duty or activities associated with the position held. Meanwhile, art. 267 Penal Code focuses on the crime, in general terms, of gaining access to third-party information by physically acquiring it (opening a letter or a file), as well as interference with the ICT network or its security (Jurgilewicz *et al.*, 2019).

It is therefore evident that the mere reading of content not intended for a person committing a prohibited act already entails criminal and legal consequences. Similar

applies to those who make it difficult or impossible for authorized persons to access data (art. 268 Penal Code). In addition, the Penal Code also contains provisions individually referring to the use of information in cyberspace. These are mainly provisions relating to the offense of grooming, i.e. the production, recording and transmission of pornographic content via a system or ICT network or establishing contact with minors under the age of 15 (art. 200a Penal Code).

At international level, a set of such regulations has been developed by the International Standardization Organization - the ISO 27000 family of standards. It is a collection of norms that define the safety requirements related to the construction, operation and maintenance of information management systems, their control and implementation of corrective measures.[8]

Another important document regulating the legal basis of information security is the 2016 NIS Directive (Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. – OJ.EU.L No. 194, p. 1). When analyzing the provisions contained in the Directive, it can be seen that the attention has been focused on specific entities, which, according to the CoE, bear the greatest responsibility for network security. No attention is devoted to the functioning and role of public administration bodies, or to contemporary websites and portals. Moreover, European law does not deal there at all with the security of the individual citizen. Importantly, the provision on the creation of a Network of Computer Security Incident Response Teams, obliging each Member State to create a special Cooperation Group whose aim would be to significantly improve strategic cooperation in the field of network and information systems protection between members of the EU (the CSIRT Team was established in Poland).

Since cyberspace has become another area of human activity with many of its features reflecting the current reality (activities, sectors of the economy, etc.), it was necessary to put forward certain rules according to which users could navigate the web. In cyberspace, thus, users have to adhere to certain frameworks and norms in order to build a safe environment and society in cyberspace. Published in 2011, *The Charter of Fundamental Rights and Principles for the Internet* presents a set of principles containing good practices for users, service providers and website administrators to follow[9].

Implementation of the provisions of the NIS Directive at national level led to the creation of the CSIRT GOV Computer Security Incidents Response Team operating within the structures of the Internal Security Agency. The appointed team focuses primarily on identifying, detecting and counteracting cyber threats that might jeopardize the security of the most important ICT systems of public-administration

[8]*https://www.pbsg.pl/rozwoj-rodziny-standardow-serii-iso-27000/.*
[9]*https://internetrightsandprinciples.org/wp-content/uploads/2020/03/polish.pdf.*

bodies or IT systems and networks of critical infrastructure. CERT Computer Crisis Response Teams from individual Member States were also included in the network of European Computer Security Incident Response Teams[10].

In order for the fight against cybercrime to be effective, due to its cross-border and international nature, the rapid exchange of information between law-enforcement agencies and services by countries in whose jurisdiction a cyberspace has been reported is crucial. "The legal framework for combating cybercrime in the European Union was created by Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and amending Council Framework Decision 2005/222/JHA.

The Internal Security Agency actively participates in combating crime related to information-security breaches in cyberspace. When establishing this service, the legislator specified that the Agency shall be competent to protect the internal security of the state and the constitutional order, and its tasks shall focus on combating and counteracting all threats that might disturb that order. Another competent entity appointed to ensure information security and combat different types of criminal activity with the use of online information is the Polish Police, who are responsible for prosecuting not only the acts listed in Chapter XXXIII, i.e., concerning strictly crimes against the protection of information, but also other prohibited acts accompanied by illegal activity involving information. In order to ensure an effective fight against cybercrime, a special Cybercrime Unit was established at Police Headquarters in 2016 (Jurgilewicz, 2017).

5. Conclusion

To summarize these deliberations, information security in cyberspace is an extremely complex area that is still developing, and as such, it requires decisive and immediate measures at legal, organizational, executive and technical level alike. The current legislation is clearly deficient in the extent of rights and freedoms of both network users and services and authorities responsible for data protection in cyberspace. It is equally important to establish close cooperation between individual services (national and international), all while ceaselessly raising public awareness of the vulnerability to information-cybersecurity threats and promoting responsible response to any observed violations on the Internet.

Finally, let us note that, although cybercriminals operate in a virtual world, the effects of their actions are all but real. Cybercrime institutions estimate that humans lose over one hundred billion dollars a year due to cybercrime and cyberterrorism. According to World Economic Forum estimates, the economic toll of cybercrime is rising

[10] *https://www.cert.pl/o-nas/ (20.01.2021).*

sharply. In 2020 alone, attacks that break the existing IT-security solutions will cost the global economy as much as USD 3 trillion[11].

References:

Aleksandrowicz, T. 2008. Terroryzm międzynarodowy. Warsaw.
Bellaby, R.W. 2011. Justifying Cyber-intelligence? Journal of Military Ethics, Vol. 15.
Białoskórski, R. 2011. Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki, Warsaw.
Ciborowski, L. 2001. Walka informacyjna. Toruń.
Colesniuc, D. 2013. Cyberspace and Critical Information. Informatica Economica, Vol. 17.
Darczewska, J. 2014. The anatomy of Russian information warfare. The Crimean Operation: The case study. Warsaw.
Eriksson, J., Giacomello, G. 2006. The Information Revolution, Security, and International Relations: (IR) relevant Theory? International Political Science Review, Vol. 27, No. 3.
Gniadek, A. 2009. Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne [w:] Cyberterroryzm. Nowe wyzwania XXI wieku, T. Jemioło, J. Kisielnicki, K. Rajchel (ed.). Warsaw.
Jurgilewicz, M. 2017. Rola podmiotów uprawnionych do użycia lub wykorzystania środków przymusu bezpośredniego i broni palnej w ochronie bezpieczeństwa i porządku publicznego. Siedlce.
Jurgilewicz, M., Jurgilewicz, O. 2019. Management of information security and its protection in criminal matters: case of Poland. Journal of Security and Sustainability, 8(3).
Jurgilewicz, M., Michalski, K., Kubiak, M., Grądzka, A. 2020. The implementation of selective passenger screening systems based on data analysis and behavioral profiling in the smart aviation security management - conditions, consequences and controversies. Journal of Security and Sustainability, 9(4), June.
Kubiak, M., Topolewski S. 2016. Bezpieczeństwo informacyjne w XXI wieku. Siedlce–Warsaw.
Liderman, K. 2012. Bezpieczeństwo informacyjne. Warsaw.
Potejko, P. 2009. Bezpieczeństwo informacyjne [in:] Bezpieczeństwo państwa, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.). Warsaw.
Terlikowski, M. 2009. Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe [in:] Bezpieczeństwo teleinformatyczne państwa, M. Madej, M. Terlikowski (ed.). Warsaw.
Wasilewski, J. 2013. Zarys definicyjny cyberprzestrzeni. Przegląd Bezpieczeństwa Wewnętrznego, no. 9(5).
Wiśniewski, B., Jakubczak, R. (ed.). 2016. Wyzwania, szanse, zagrożenia i ryzyko dla bezpieczeństwa narodowego RP o charakterze wewnętrznym, Szczytno.
Wiśniewski, B. 2020. Praktyczne aspekty badań bezpieczeństwa, Warsaw.

[11] *https://ikmj.com/cyberbezpieczenstwo-w-polsce-statystyki/.*