The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity

DOMINIK TYRAWA

Abstract Cybersecurity is one of the types of security that is distinguished in the field of legal sciences with respect to the legal aspects of security. This type of security is very extensive and specialised in nature. Apart from the specialised and precise legal language employed, by using approaches derived from the field of communication and information sciences, the sphere of values that underlie this type of security can also be distinguished. The variety of goods that are protected under cybersecurity leads to the multi-faceted nature of the applicable solutions in this regard. This multi-faceted character refers both to the material scope, namely, the goods that are protected in this way with the application of optimised tools, and to the subjective scope, namely, the entities protected by the system and by which entities it is protected. All these analyses clearly indicate that this involves a very complex phenomenon which is highly relevant to our daily lives.

Keywords: • axiology • security • cybersecurity • systemic • material and procedural aspects of cybersecurity • man vs state

CORRESPONDENCE ADDRESS: Dominik Tyrawa, Ph.D., Dr. Habil., University Professor, John Paul II Catholic University of Lublin, Faculty of Law, Canon Law and Administration, Department of Administrative Law, al. Racławickie 14, 20-950 Lublin, Poland, e-mail: dominik.tyrawa@kul.pl, ORCID: 0000-0001-6385-9726.

https://doi.org/10.4335/2022.1.2 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Security is one of the most important human needs. The literature on the subject, both in legal sciences, and in other disciplines (psychology, economics, management, sociology, security sciences), when describing the need for security, usually refers to A. Maslow's hierarchy of needs. This is based on the fulfilment of physiological needs, examples of which include the need for food, housing, clothing and procreation. The nature of these needs ensures that they have the strongest impact on man, and man first strives to satisfy them. It is only after fulfilling the primary needs that the will to satisfy other needs appears in man. Maslow, in creating a hierarchy of these, identified first the need for safety, then the need for belonging and love, the need for esteem and finally the need for self-actualisation. The need for safety is expressed in the search for safety and constancy, and then comes down to the pursuit of dependence, the search for protectiveness, the avoidance of unclear situations, the avoidance of chaos, the pursuit of law and order and the rule of law (Maslow, 2009: 65-71).

It should be noted that nowadays, even before the outbreak of the global COVID-19 pandemic, the need for security was often overlooked or taken for granted. In developed societies, human life was rather stable and physiological needs were more or less, met. For many people, social emphasis was on the "self" and psychological needs, and security itself was marginalised Only a threatening situation concerning law, order or authority could trigger a return to the need for security and treating it not as something obvious, but as something desirable (Tyrawa, 2018: 37).

The outbreak of the COVID-19 pandemic prompted a return to the source, and increased research into the multifaceted nature of the need for security, including that in the legal sciences, met with greater scientific interest. Somewhere in the background of this research, on its margins, there are activities and research in the field of cybersecurity. This concept naturally interacts with research related to the pandemic (for example, through the increased importance of communication and information systems and networks, in the context of e-learning, home-office, general security of business transactions, work provision, fulfilment of various types of obligations (mainly civil law obligations), when supply chains are interrupted or hindered), although it should be emphasised that research in this field was successfully conducted even before the outbreak of the pandemic.

The purpose of this paper is to indicate what cybersecurity is, how it should be embedded in the legal security system, what key values underlie the concept and how, through strictly defined institutions, the concept should be protected and guaranteed.

2 The concept of cybersecurity and its place in the legal security system

In the search for a definition of cybersecurity, the normative solutions of a given country (in this case the Republic of Poland) should be analysed first, followed by the views of legal commentators and possibly case law. It should be noted, however, that defining cybersecurity is not the main task of this paper and therefore the definitions referred to will be of a general nature and certainly not exhaustive.

The basic act on cybersecurity, in force since July 2018, is the National Cybersecurity System Act of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended). This normative act primarily organises issues related to cybersecurity at the national level. First of all, the Act introduces an extensive set of specialised concepts and specifies more precisely the system of entities covered by this systemic protection. Furthermore, the legislator points out the problem of identification and registration of operators of essential services, the duties of operators of essential services, digital service providers and public entities, and specifies the tasks of specialist entities more precisely, i.e. CSIRT MON (Computer Security Incident Response Team operating on a national level, managed by the Minister of National Defence), CSIRT NASK (Computer Security Incident Response Team operating on a national level, managed by the Research and Academic Computer Network – National Research Institute) and CSIRT GOV (Computer Security Incident Response Team operating on a national level, managed by the Head of the Internal Security Agency). In addition, it clarifies the principles of sharing information and processing personal data, and introduces and systematises the system of competent authorities for cybersecurity, the tasks of the minister in charge of computerisation, the tasks of the Minister of National Defence, as well as the issues of supervision and control of operators of essential services, digital service providers and entities providing cybersecurity services. The last relevant regulations of the aforementioned Act refer to the establishment of competent authorities for cybersecurity, i.e. the Plenipotentiary, whose task is to coordinate activities and implement the government's policy on cybersecurity; and the Committee, i.e. the opinion and advisory body in the field of cybersecurity, acting at the Council of Ministers. Beyond the aforementioned, it lays out the Strategy, i.e. the document that defines strategic objectives and relevant policy and regulatory measures aimed at achieving and maintaining a high level of cybersecurity. The final section of the Act relates to the provisions on fines.

The very description of the material scope above indicates that the stated Act is fundamental in the field of cybersecurity. At the same time, it should be noted that the regulation of such a broad material and subjective spectrum raises the question of whether this is a regulation that provides an exhaustive coverage of the issues contained in the title or a regulation that attempts to order these issues. Answering this question goes beyond the scope of this paper, although according to the Author, a statement about ordering these issues would be more appropriate.

In the context of this paper, the most important element is to specify more precisely what cybersecurity is. In the aforementioned Act, in Article 2(4), cybersecurity is defined as the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. This case involves a de facto normative mental construct denoting the security of IT systems and networks (Banasiński, 2020: 16).

Legal commentaries approach this concept in a slightly different way. The basic policy paper of the Republic of Poland in this regard defines this concept as "a process of ensuring the secure functioning in cyberspace of the state as a whole, its structures, natural persons and legal persons, including entrepreneurs and other entities without legal personality, as well as the communication and information systems and information resources at their disposal in global cyberspace" (National Security Bureau, 2015: 7-8). At the same time, the paper identifies the main objective in terms of cybersecurity as ensuring the secure functioning of the Republic of Poland in cyberspace, including an adequate level of security of national communication and information systems, especially the ICT critical infrastructure of the state, as well as private economic entities that are key to the functioning of society, in particular, those that are part of the financial, energy and health care sectors (National Security Bureau, 2015: 9).

It seems that a proper definition of cybersecurity should be linked to the concept of security in the first place. When defining the concept of "security", it should be pointed out that it refers to a number of semantic levels (Potrzeszcz, 2013: 25), and is also related to the fact that this case involves a common phenomenon in the everyday lives of individuals and societies, so the concept will be defined more precisely by intuition and will be difficult to define unambiguously (Potrzeszcz, 2014: 15). In addition, it should be noted that security is defined in various ways within the methodology of various sciences, making the concept of security all the more ambiguous. Due to the limited nature of this paper, it may be assumed that security is a state of peace, a state that gives a feeling of certainty, and a state that guarantees its maintenance. Security is the opposite of chaos or uncertainty.

Cybersecurity, then, is a state of constancy, security and peace in cyberspace. Cyberspace should be understood as a communication space that is created by online connection systems and allows people to communicate online and establish relationships in real time. Cyberspace is also an environment in which information is exchanged through networks and computer systems. This is a dimension of activities in which all actions diverge from the physical environment. This is a new dimension (in addition to the terrestrial, aquatic, air, and space environments) in which various actions, including military actions, can be carried out. This environment differs from those mentioned above primarily in that: 1) it is man-made; 2) its participants have full control over the nature of this environment; 3) it has no territorial limitations. In addition, cyberspace has four typical features: 1)

anonymity; 2) aterritoriality; 3) regularity; 4) global reach (Marczyk, 2018: 59-60). The concept of cybersecurity, which benefits most from the conceptual framework of the law of new technologies, situated within administrative law, consists of institutions of constitutional, substantive and procedural law.

In situating cybersecurity within the national security system, it should first be pointed out that cybersecurity is a specialised branch of security that includes the protection of information systems from threats (Czuryk, 2019: 42). It seems that the assumption that cybersecurity is one of the types of security is most correct. The most commonly identified types of security include: international security, state security, public security, legal security, environmental security, energy security, economic (and social) security, political (and military) security, personal security, aviation security, local security, cultural security, ICT security and health security (Tyrawa, 2018: 80-109). However, it should be stressed that these concepts are intertwined. It is impossible to set precise and fixed boundaries in this respect. In addition, the terminology is imprecise (various ways of defining a given type of security, in this case, ICT security and technological security are conceptually similar), which makes it even more difficult to analyse individual types of security.

The above reasons clearly indicate that in relation to cybersecurity, it is one of the types of security that is intertwined to varying degrees with other types of security, to the greatest extent with international security, state security, public security, energy security and aviation security. In this case, we are faced with a very specialised concept that primarily refers to an artificial man-made system based on ICT solutions.

3 The multi-faceted nature of cybersecurity

When describing the material scope (the tasks to be fulfilled by a given type of security) and the subjective scope (both the entities in relation to which a given type of security applies and the entities that carry out activities in this respect) of cybersecurity, it should first be noted how multi-faceted this phenomenon is. The material scope and subjective scope are intertwined. The material scope will be presented in detail in the next part of this paper, as will be with regard to the subjective scope. The considerations in this respect, however, must be preceded by general remarks.

When answering the question of what cybersecurity is and what the multi-faceted nature in this regard is, the analysis should begin with the material scope. The gradation of the goods that this type of cybersecurity protects can essentially be reduced to the protection of human life and health. This is expanded into individual protected goods. Their differentiation is basically an analysis of individual phenomena, where communication and information systems and networks are used. Due to the limited and introductory nature of the paper, an attempt to specify all the specific goods protected in this way is

doomed to fail. Nevertheless, it can be stated that at the end of every cybersecurity activity there is a human being.

A specific example is the situation involving the ICT protection of a given information system, i.e. a communication and information system, referred to in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks (consolidated text, Polish Journal of Laws of 2020, item 346, as amended). First of all, an extensive security system is put in place to protect a specific system (and thus the information contained in it, partly related to a specific human being). Further protection concerns the possibility of using the system, at the level of performing tasks by public administration, as well as in relation to an individual being whose sensitive data is included in the system. In addition, it should be pointed out that detailed data, first of all personal data, is protected. To sum up, this case involves multilevel protection of various goods, and in particular, protection of the organisational structure itself, which operates on the basis of these systems, and ultimately this protection concerns an individual who, being part of a given organisational structure, performs tasks on the basis of this system, as well as an individual whose sensitive data is included in this system.

In terms of the subjective scope, the multi-faceted nature of cybersecurity should be understood as an extensive system of subjective protection in this respect. It seems that it can be assumed that, first of all, cybersecurity protects communication and information systems and the individual who uses them, as well as the individual's data collected in the course of operating these communication and information systems. Another definition of a communication and information system can be mentioned here, according to which it is a set of cooperating IT devices and software that enables processing and storage, as well as sending and receiving of data via telecommunications networks by using terminal equipment that is appropriate for a particular type of network, and this definition is based on Article 2(3) of the Act of 18 July 2002 on Providing Services by Electronic Means (consolidated text, Polish Journal of Laws of 2020, item 344, as amended). Terminal equipment, in accordance with Article 2(43) of the Act of 16 July 2004 – Telecommunications Law (consolidated text, Polish Journal of Laws of 2021, item 576, as amended), should be understood as telecommunications equipment intended to be connected directly or indirectly to network terminations.

Subjective protection in this respect can be described as individual (private), mixed (private-public) and collective (public, state or supranational) protection. Individual protection is organised by such an entity, i.e. a person, e.g. by purchasing and installing antivirus software on the computer they use, or by another private entity, e.g. a company, organising its own internal communication and information system and securing it in an appropriate manner. Mixed protection is protection involving the cooperation of private entities (e.g. ICT companies, both local and global) with entities operating within the state structure (e.g. local government units or public administration authorities). Private entities as part of this cooperation provide specific know-how, and state entities are most

often the entities that order a widely understood service. Cooperation in this respect may take place within a small organisational unit and a telecommunications or IT company, but also at the state level (cooperation between the state and a global ICT company) or even supranational, where the customer is an international organisation, such as the European Union. The last type of protection is collective protection, which is guaranteed in its entirety by a local government unit, public administration or an international organisation. Determining the precise boundaries between these types of protection is in some cases difficult, as within this issue, various factual phenomena intermingle that are difficult to fit into a specific security model.

4 Values protected by cybersecurity

As already stated above, the fundamental and main good to be protected by cybersecurity is man, and, more specifically, their life and health. The presented case involves goods that can be placed highest in the hierarchy of values important for man. Without protection of human life or health, other goods recede to the background, and their protection becomes pointless.

In terms of subject matter, cybersecurity consists primarily of instruments, specialised computer programs and systems that collect relevant data. Their presentation and precise specification at this point goes beyond the scope of the paper. However, a general framework for this issue can be outlined. When indicating the instruments that are employed, they can generally be defined as the use of the Internet and other networks (Intranet, Extranet), as well as computers, phones, smartphones, tablets, servers, terminals or smart TV. These instruments are applied in order to better satisfy human needs, improve the quality of life, maximise profit (both on the part of public administration and on the part of citizens) and, above all, guarantee an increase in the efficiency and effectiveness of administration. These instruments are employed in the development of, for example, e-business, e-administration, e-health, e-culture or e-tourism.

Public administration, acting in the field of cybersecurity, uses systems involving the application of satellite telecommunications, including, for example, location, environmental monitoring and security, in the field of road, sea, air transport, in relation to the transport of dangerous goods, livestock, in the field of civil defence, crisis management, humanitarian aid, in relation to agriculture, land measurement, land surveying and land register. Other areas where communication and information systems are implemented include the extraction and distribution of fossil fuels (oil and gas), search and rescue, as well as such areas as logistics, environment, science or law enforcement.

The state is involved in the development of information society (and thus also in the development of cybersecurity), through the development of information technologies, within administration itself, in the area of its contacts with citizens, as well as in the state's investment in telecommunications infrastructure. Actions in this regard are aimed at

solving related problems. In this respect, first of all, the following aspects should be mentioned: eliminating digital exclusion, protecting consumers in electronic commerce, combating computer crime, developing electronic payment systems, respecting individual privacy and protecting intellectual property rights.

The scope concerned also includes extremely important communication and information systems that are used by public administration or individuals on a daily basis, i.e. KRS (National Court Register), KRK (National Criminal Register), NKW (New Land and Mortgage Register), PESEL (Universal Electronic System for Registration of the Population), POLTAX (a distributed system for recording and processing data on taxpayers used by tax offices), CEPiK (Central Register of Vehicles and Drivers) or REGON (Register of National Economy – National Official Register of Business Entities).

It is correct to say that the main task of administrative law is to serve man (Zimmermann, 2013: 77). This extremely general statement can also be related to the tasks that form the axiological basis of security. Referring to cybersecurity, it can be stated that the systems used by public administration protect, in the first place, data relating to the status of an individual in terms of their health status, property status (information on real property held, its location, vehicles, their mileage), data on marital status and family members, data on the address of residence (permanent address or actual residence), data on financial and economic status, data on social benefits received or data on documents used by the individual (passport, identity card, driving licence, vehicle registration certificate). Cybersecurity thus protects the part of an individual's life that can be described as "privacy".

5 Entities protecting cybersecurity – general considerations

An element complementing the considerations in the field of cybersecurity is the indication (emphasis on) of the entities that act for cybersecurity. As already stated, three types of protection can be distinguished in this regard, i.e. individual, mixed and collective protection.

Individual protection relates both to natural persons and legal persons, but also to entities without legal personality. As a rule, state action in this respect is very limited. It is the individual course of action that can be described as private (also in terms of the financial resources involved) that is key in this regard. The role of the state in this aspect should be limited to two problem areas, educational – where the state highlights and educates about cyberthreats, and training – where the state trains individuals, who then educate the public about such threats.

The second type of protection is mixed private-public protection. Its importance in the globalised world is constantly growing. This is a matter of the space that needs to be

described in detail in order to diagnose the threats and opportunities associated with its development. It is in this space that we can look for entities that will be described as hybrids of public-private transnational bodies. It seems that within this area of cooperation, it is possible to identify in more detail such entities as: formal intergovernmental regulatory bodies, informal intergovernmental regulatory networks for cooperation and coordination of arrangements, national regulatory bodies operating with reference to international intergovernmental regimes, hybrid public-private regulatory bodies, and some private regulatory bodies exercising transnational governance functions of particular public significance. The fact of distinguishing these entities is based on the contemporary needs of the international community, because transgovernmental administration is also in place, due to global interdependence (Kingsbury, Krisch, Stewart, 2005: 16).

The third type of subjective protection is collective protection. Protection in this respect is guaranteed by an entity being part of a national, supranational or international structure. In the case of supranational or international structures, such entities as the EU, NATO or the UN can be mentioned, for example. State protection is much more extensive. Entities that can be classified in this group include local government units and entities dependent on them (e.g. budget enterprises, municipal companies, but also schools or kindergartens, cultural institutions or others), central or local public administration, courts, prosecutor's offices, court enforcement officers supervised by courts with territorial jurisdiction. The secret services play very important roles in this respect. The gradation of public administration activities in the field of cybersecurity can be linked to the gradation, not only of the entities established for this purpose, but, above all, to the development (gradation) of the manner of operation of a particular entity. In this regard, traditional government (which includes the administration itself), which is based on paper documents, and higher organisational forms can be identified. The latter include e-government (including e-administration), based on static ICT tools and Internet 1.0, Government 2.0, based on Internet 2.0 and social media, and M-government (mobile government), which is built on mobile information technologies (Khan, 2015: 135-149).

A large number of entities performing cybersecurity tasks are specified in Article 4 of the Act on the National Cybersecurity System. Such agencies are components of a system identical to the specification that was made in the text in terms of classification as actors involved in state protection. As already brought forward, subjective protection is multifaceted in nature. The values protected by these entities are part of the system of values that underlie cybersecurity as a type of security.

6 Conclusion

As stated in the text, the phenomenon of the multi-faceted nature of cybersecurity can be readily identified. This nature is both material and subjective. The values that cybersecurity should protect are crucial in this case. The most important good protected

in this way is the protection of individual privacy, but also the protection of health and life. Both private and public entities should tailor protective measures to the good to be protected and the threats that may affect it. Building a proper system in this respect, based on the tools available, is a challenge in times of growing threats to electronic security, especially in terms of the extensive digitalisation of social life.

References:

Banasiński, C. (2020) Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa, In: Banasiński, C. & Rojszczak, M. (eds.) *Cyberbezpieczeństwo* (Warszawa: LEX a Wolters Kluwer business), pp. 15-38.

Biuro Bezpieczeństwa Narodowego (2015) *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* (Warszawa: Centrum Poligrafii Sp. z o.o.).

Czuryk, M. (2019) Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity, *Cybersecurity and Law*, 2, pp. 39-50.

Khan, G.F (2015) The Government 2.0 utilization model and implementation scenarios, *Information Development*, 2, pp. 135-149.

Kingsbury, B., Krisch, N. & Stewart, R.B. (2005) The Emergence of Global Administrative Law, *Law and Contemporary Problems*, 68, pp. 15-61.

Marczyk, M. (2018) Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, *Przegląd Teleinformatyczny*, 1-2, pp. 59-72.

Maslow, A. (2009) *Motywacja i osobowość* (Warszawa: Wydawnictwo naukowe PWN).

Potrzeszcz, J. (2013) *Bezpieczeństwo prawne z perspektywy filozofii prawa* (Lublin: Wydawnictwo KUL).

Potrzeszcz, J. (2014) *Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa*, In: Lis, W. (ed.) *Bezpieczeństwo państwa. Zagadnienia podstawowe* (Lublin: Wydawnictwo KUL), pp. 15-34.

Tyrawa, D. (2018) *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym* (Lublin: Wydawnictwo KUL).

Zimmermann, J. (2013) *Aksjomaty prawa administracyjnego* (Warszawa: LEX a Wolters Kluwer business).