E-ISSN 2544-9567
ISSN 1230-3801

Zeszyt 165 nr 3/2023, str.101 - 132
Volume 165 No. 3/2023, pp. 101 - 132

NORMATYWNE WYMAGANIA BEZPIECZEŃSTWA INFRASTRUKTURY INFORMACYJNO-KOMUNIKACYJNEJ PAŃSTWA W PRAWIE KRAJOWYM

NORMATIVE REQUIREMENTS FOR STATE INFORMATION-COMMUNICATION INFRASTRUCTURE SECURITY IN THE NATIONAL LAW

Ewa CISOWSKA-SAKRAJDA, *ewa.cisowska-sakrajda@aws.edu.pl*, ORCID: 0000-0001-8383-6951
Akademia Wymiaru Sprawiedliwości w Warszawie, *University of Justice, Warsaw, Poland*

DOI 10.5604/01.3001.0053.9222

Streszczenie: Artykuł prezentuje normatywne wymagania infrastruktury informacyjno-komunikacyjnej, które zarazem tworzą standard jej bezpieczeństwa. Główny nurt rozważań koncentruje się wokół pojęcia normatywnych wymagań bezpieczeństwa infrastruktury oraz klasyfikacji i charakterystyki wymagań. Analiza obejmuje także zasady obowiązujące przy określaniu przez podmiot publiczny samych wymogów stosowanych dla infrastruktury i jej interoperacyjności, a także zasady stosowane już przy tworzeniu i modernizacji konkretnej infrastruktury informacyjno-komunikacyjnej.

Słowa kluczowe: zasady ogólne, wymagania dla systemów teleinformatycznych, wymagania dla interoperacyjności systemów i rejestrów publicznych, wymagania dla rejestrów publicznych i wymiany cyfrowych informacji, prawo administracyjne

Abstract: The article presents the normative requirements of the information and communication infrastructure, which also form the standard of its security. Its main considerations focus on the concept of normative infrastructure security requirements as well as their classification and characteristics. The analysis also includes the rules applicable to the public entity's definition of the requirements applicable to infrastructure and its interoperability, as well as the principles already applied when creating and modernizing a specific information and communication infrastructure.

Keywords: general principles, requirements for ICT systems, requirements for the interoperability of public systems and registers, requirements for public registers and exchange of digital information, administrative law

1. Wprowadzenie

Infrastruktura informacyjno-komunikacyjna państwa stanowi niezwykle istotne technologiczne narzędzie funkcjonowania współczesnego państwa, a zarazem przedmiot odrębnej – od informacji publicznej - ochrony prawnej i szerokiego unormowania wymagań jej bezpieczeństwa. Nic w tym dziwnego skoro jest ona tak powszechnie i na tak dużą skalę wykorzystywana do przechowywania, przetwarzania,

1. Introduction

State’s information and communication infrastructure creates both an especially important technological tool of functionality of the present state, and an object of legal protection, distinct from public information, and wide standardisation of its security requirements. Anyway, it is not strange as it is commonly and widely used for storing, processing, collecting and sending uncounted

gromadzenia i przesyłania niezliczonej ilości cyfrowych danych (informacji publicznych), które generują różne podmioty realizujące zadania publiczne. Rodzi to po stronie tych podmiotów prawny obowiązek zagwarantowania bezpieczeństwa stosowanej przez nie infrastruktury technicznej, a ściślej systemów teleinformatycznych[1]. A obowiązek ten spoczywa na nich przy podejmowaniu przez nie całego spektrum różnorodnych działań, jak: projektowanie, tworzenie, modernizacja i użytkowanie infrastruktury. Równie ważny jest też obowiązek zapewnienia interoperacyjności, spójności działania różnych systemów teleinformatycznych używanych do realizacji zadań publicznych oraz rejestrów publicznych i wymiany informacji publicznej w postaci elektronicznej z podmiotami publicznymi, a jednocześnie zapewnienia sprawności wymiany informacji w postaci elektronicznej między podmiotami publicznymi, także innych państw lub organizacji międzynarodowych. Razem tworzą one przecież infrastrukturę informacyjno-komunikacyjną państwa, w której poszczególne jej elementy w założeniu powinny ze sobą współdziałać.

Tym celom służą przyjęte na gruncie prawa krajowego normatywne wymagania bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa[2]. Jednocześnie tworzą one

amounts of digital data (public information), produced by different entities performing public tasks. Then a legal obligation arises on the side of these entities to warrant the security of used technical infrastructure, i.e. tele-informative systems[3]. This obligation is born by them when they undertake a whole spectrum of different actions, such as a designing, preparation, upgrading and using of the infrastructure. There is also important to meet the obligations for the interoperability, and the coherence of operation for different tele-informative systems used for execution of public tasks, and public registers, and exchange of public information in the electronic form with public entities, and moreover to provide the efficient exchange of information between public entities, including the foreign states and international organisations, as well. It is so because they together create the state information-communication infrastructure and it is assumed that its particular components have to work together.

For these purposes some normative specifications were accepted for the state information-communication infrastructure on the ground of the national law[4]. At the same time they create a universal security standard of this infrastructure which may be defined

[1] Na temat definicji bezpieczeństwa informacyjnego zob. zwłaszcza W. Kitler, Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne [w:] W. Kitler (red.), J. Taczkowska-Olszewska, (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017, s. 31, J. Taczkowska-Olszewska, Bezpieczeństwo informacyjne jako kategoria prawna [w:] W. Kitler (red.), J. Taczkowska-Olszewska, (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017, s. 47, T. Aleksandrowicz, Bezpieczeństwo informacyjne państwa, Studia Politologiczne 2018, z. 49, s. 41 i n., P. Zaskórski, K. Szwarc, Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki 2013 nr 9, rok 7, s. 41.

[2] Na temat roli wymagań dla systemów teleinformatycznych zob. I. J. Jóźwiak, A. Szleszyński, Specyfikacja wymagań dla bezpieczeństwa informacji przechowywanej i przetwarzanej w systemie operacyjnym serwera, PAK 2011 tom 57, nr 9, s. 1075 -1076.

[3] On definition of the safety of information see especially W. Kitler, Denomination and extension of the state information security, systemic and definition settlements [w:] W. Kitler (red.), J. Taczkowska-Olszewska, (red.), Information security. Legal-administrative aspects, Warsaw 2017, p. 31, J. Taczkowska-Olszewska, Information security as a legal category [w:] W. Kitler (red.), J. Taczkowska-Olszewska, (red.), Information security. Legal-administrative aspects, Warsaw 2017, p. 47, T. Aleksandrowicz, State information security, Politics studies 2018, v. 49, p. 41 and next, P. Zaskórski, K. Szwarc, Safety of information assets as a determinant of informative management technologies. Scientific notebooks of Warsaw's High School of Informatics, 2013 nr 9, year 7, p. 41.

pewien uniwersalny standard bezpieczeństwa tej infrastruktury, który można zdefiniować jako stosowanie w ramach danego systemu teleinformatycznego bądź kompleksu współdziałających, powiązanych ze sobą systemów teleinformatycznych, jednolitych, wspólnych, względnie trwałych reguł i zasad.

Tak zidentyfikowany obszar badawczy uzasadnia w pierwszej kolejności rozważenie sposobu rozumienia samego terminu normatywne wymagania infrastruktury informacyjno-komunikacyjnej jako odrębnego od pojęcia standard, aczkolwiek znaczeniowo bardzo zbliżonego, a następnie podjęcie próby usystematyzowania wymagań normatywnych. Naturalnym tego następstwem jest scharakteryzowanie poszczególnych normatywnych wymagań tej infrastruktury, wskazanie zakresu ich zastosowania oraz cech je odróżniających od innych. Z tym ściśle wiąże się przyjęty przez rodzimego normodawcę poziom dla poszczególnych wymagań normatywnych i elementów składowych infrastruktury. A mianowicie czy jest on minimalny, czy w równym stopniu ma zastosowanie do wszystkich składników sytemu teleinformatycznego, wreszcie czy podmioty realizujące zadania publiczne mają jakąkolwiek dozę dyskrecjonalności w procesie „budowania" własnego systemu teleinformatycznego. Nie mniej interesujące jest to, czy normatywne wymagania można uznać za wystarczające dla zapewnienia bezpieczeństwa infrastruktury, czy aktualne przepisy są adekwatne do zmieniających się zagrożeń dla bezpieczeństwa infrastruktury oraz tak dynamicznie zachodzących zmian technologicznych w obszarze informacyjno-komunikacyjnym.

as an application in the frame of a given tele-informative system, or mutually combined tele-informative systems, of rules and principles which are uniform, common, and relatively unchangeable.

The domain of research identified in such way substantiates, in the first order, a consideration of the understanding of the alone term of normative requirements for information-communication infrastructure to be set in a separated position than the notion of standard, even still having the close meanings, and in the next step an attempt of systematic arrangement of the normative requirements. Characterisation of particular normative requirements of this infrastructure and indication of the scope of their application and features distinguishing them from the others is a natural consequence of that. It is strictly connected with a level accepted by the national legislator for particular normative requirements and components of the infrastructure. And namely, if this level is minimal, and if it has to be applied in equal degree for all components of tele-informative system, and finally if the entities performing the public tasks have any kind of discretion in the process of "building" an own tele-informative system. Not the less interesting is whether the normative requirements can be recognised as sufficient ones for safeguarding the security of the infrastructure, and if the present regulations are adequate to changeable threats for infrastructure security and dynamic technological changes in the information-communication domain.

[4] On the meaning of requirements for tele-informative systems see I. J. Jóźwiak, A. Szleszyński, Specification of requirements for information stored and processed in server operational system, PAK 2011 vol. 57, nr 9, p. 1075 -1076.

2. Pojęcie normatywne wymagania bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa

Termin normatywne wymagania bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa można zdefiniować - pomimo braku jego definicji na gruncie aktów normatywnych - jako określony prawem zespół warunków: parametrów, cech, właściwości odpowiednich (adekwatnych) dla poszczególnych elementów infrastruktury informacyjno-komunikacyjnej oraz cech informacyjnych, które są niezbędne dla zapewnienia prawidłowego i bezpiecznego ich działania, w tym umożliwienia wymiany danych z innymi systemami, zapewnienia dostępu do zasobów informacyjnych i umożliwienia współdziałania różnych systemów teleinformatycznych i baz informacyjnych, a także zapewnienia spójności systemów teleinformatycznych, rejestrów publicznych i wymiany informacji[5]. Wymagania te stanowią zatem pewne uniwersalne warunki (kryteria, właściwości, cechy), które powinna spełniać infrastruktura informacyjno-komunikacyjna państwa, a ściślej poszczególne jej elementy składowe, aby cyfrowe informacje przekazywane za jej pośrednictwem były chronione przed nieuprawnionym dostępem, a różne systemy teleinformatyczne były interoperacyjne.

Zważywszy na różnorodność elementów infrastruktury informacyjno-komunikacyjnej państwa, termin normatywne wymagania jest pojęciem zbiorczym, które obejmuje wymagania o niezwykle różnorakim charakterze.

2. The Notion of Normative State Information-communication Infrastructure Security Requirements

The term of normative state information-communication infrastructure security requirements may be defined – despite the lack of its definition on the ground of normative acts – as a number of conditions described by law: parameters, features, properties relevant (adequate) for particular components of information-communication infrastructure, and informative characteristics which are indispensable to provide their proper and safe operation, including the exchange of data with other systems, and provision of access to information resources, and cooperation of different tele-informative systems and data bases, and also the coherence of tele-informative systems, public registers, and exchange of information[14]. Therefore, these requirements create some universal conditions (criteria, properties, characteristics) which have to be met by the state information-communication infrastructure, and more precisely its components, to protect digital data transferred by it against unauthorised access, and provide interoperability for different tele-informative systems.

Regarding the variety of components of the state information-communication infrastructure, the term of normative requirements is a collective notion which encompasses the requirements of highly differentiated character. Among them are, firstly,

[5] Definicję tą sformułowano w oparciu o całokształt regulacji normatywnej w tym przedmiocie, a zwłaszcza poprzez odwołanie do definicji legalnych pojęć minimalne wymagania dla systemów teleinformatycznych, minimalne wymagania dla rejestrów publicznych i wymiany informacji oraz Krajowych Ram Interoperacyjności. Zob. zwłaszcza ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j.: Dz. U. z 2023 r. poz. 57, zwaną ustawą o informatyzacji podmiotów publicznych, i rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, t.j. Dz. U. z 2017 r. poz. 2247, zwane rozporządzeniem w sprawie Krajowych Ram Interoperacyjności lub rozporządzeniem w sprawie KIR.

Wśród nich znajdują się, po pierwsze, sformułowane na poziomie ustawy zasady ogólne dotyczące wdrażania, rozbudowy i modernizacji oraz użytkowania systemów teleinformatycznych[6]; po drugie określone na poziomie norm normalizujących zasady ogólne stosowania wymogów określonych w tych normach[7]; a po trzecie, sformułowane na poziomie ustawy i aktu do niej wykonawczego oraz norm normalizujących szczegółowe wymagania, odrębnie unormowane dla różnych elementów infrastruktury, a mianowicie wymagania dla systemów teleinformatycznych[8], wymagania dla interoperacyjności systemów teleinformatycznych i rejestrów publicznych[9] oraz wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[10]. W gruncie rze-

the general principles formulated on the level of an act relating to implementation, extension and upgrading and use of tele-informative systems[15]; and secondly, the general principles determined on the level of normalising norms for application of requirements specified in these norms[16]; and thirdly, formulated on the level of an act and its relevant executing act, and norms normalising detailed requirements which are separately normalised for different components of the infrastructure, and namely the requirements for tele-informative systems[17], requirements for interoperability of tele-informative systems and public registers[18], and requirements for public registers and the exchange of information in the elec-

[14] Definition was formulated on the base of the overall normative regulation in this subject, and especially by the reference to legal definitions of denominations for minimal requirements for tele-informative systems, minimal requirements for public registers and exchange of information and the National Frames of Interoperability. See especially the Act from 17 Feb., 2005 on informatisation of public entities performing the public tasks, i.e.: Law Monitor from 2023, pos. 57, named as the Act on informatisation of public entities, and disposition of the Board of Ministers from 12 April, 2012 on the National Frames of Interoperability, minimal requirements for public registers and exchange of information in the electronic form and minimal requirements for tele-informative systems, i.e. Law Monitor from 2017, pos. 2247, named as disposition ion the National Frames of Interoperability or disposition on NFI.

[6] Zob. zwłaszcza art. 1 pkt 2 i 3, art. 13 ust. 2 i art. 18 pkt 1 ustawy o informatyzacji podmiotów publicznych oraz § 3 ust. 1 pkt 2 czy § 4 ust. 3 rozporządzenia w sprawie KRI.

[7] Tak np. pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN nr PN-ISO/IEC 27001 System zarządzania bezpieczeństwem informacji, s. 7.

[8] Jest to „zespół wymagań organizacyjnych i technicznych, których spełnienie przez system teleinformatyczny używany do realizacji zadań publicznych umożliwia wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych oraz zapewnia dostęp do zasobów informacji udostępnianych za pomocą tych systemów". Zob. art. 3 pkt 9 ustawy o informatyzacji podmiotów publicznych.

[9] Jest to zawarty w Krajowych Ramach Interoperacyjności „zestaw wymagań semantycznych, organizacyjnych oraz technologicznych dotyczących interoperacyjności systemów teleinformatycznych". Zob. art. 3 pkt 21 ustawy o informatyzacji podmiotów publicznych.

[10] Jest to „zespół cech informacyjnych, w tym identyfikatorów oraz odpowiadających im charakterystyk elementów strukturalnych przekazu informacji, takich jak zawartości pola danych, służących do zapewnienia spójności prowadzenia rejestrów publicznych oraz wymiany informacji w postaci elektronicznej z podmiotami publicznymi". Zob. art. 3 pkt 10 ustawy o informatyzacji podmiotów publicznych.

[15] See especially art. 1 pt. 2 and 3, art. 13 pos. 2 and art. 18 pt. 1 of the Act on informatisation of public entities and § 3 pos. 1, pt. 2 or § 4 pos. 3 of disposition on NFI.

[16] For instance pt. 1 titled The scope of norm and pt. 0 titled Introduction, subpoint 01, § five of PN nr PN-ISO/IEC 27001 System for information security management, p. 7.

[17] It is a „catalogue of organisational and technical requirements which have to be met by a tele-informative system used for execution of public tasks to provide data exchange with other tele-informative systems used for execution of public tasks and which ensures the access to information assets published by these systems". See art. 3 pt. 9 of the Act on informatisation of public entities.

[18] It is "the catalogue of semantic, organisational and technological requirements contained in the National Frames of Interoperability relating to interoperability of tele-informative systems". See art. 3 pt. 21 of the Act on informatisation of public entities.

czy wymagania dla poszczególnych elementów infrastruktury informacyjno-komunikacyjnej znajdują się – co jest naturalne dla wszelkich rozwiązań technologicznych - w normach i dyrektywach technicznych. Odwołanie do obowiązujących w technice, a zwłaszcza w poddanej tak szybkim zmianom informatyce i telekomunikacji, norm i standardów zmierza do ujednolicenia i ustandaryzowania wymagań dla systemów teleinformatycznych. Jednocześnie taki zabieg legislacyjny zapewnienia ich kompatybilność i zdolność do wzajemnej „współpracy" (wspólny poziom kompatybilności rozwiązań technologicznych i ich zdolności do współpracy).

Tak ujęte normatywne wymagania infrastruktury informacyjno-komunikacyjnej państwa nie zostały przyjęte na tożsamym poziomie. Wymagania dla systemów teleinformatycznych, rejestrów publicznych i wymiany informacji, a dla interoperacyjności wymagania techniczne mają bowiem charakter minimalny. Wobec tego rozróżnienia, co znajduje swoje odzwierciedlenie także w tytule i systematyce rozporządzenia w sprawie Krajowych Ram Interoperacyjności, nie ma, po pierwsze, najmniejszej wątpliwości, że zespół wymagań dla interoperacyjności systemów jest szerszy niż dla samych systemów. Obejmuje on bowiem – obok wymagań organizacyjnych i technologicznych – dodatkowo wymagania semantyczne, a wymagania te są określone na różnym poziomie szczegółowości i kategoryczności. Tym samym prawodawca daje do zrozumienia, że nie są to takie same zespoły/zestawy wymagań, lecz są one determinowane właściwościami poszczególnych elementów infrastruktury informacyjno-komunikacyjnej państwa, dla którego ów ze-

tronic form[19]. Actually, the requirements of particular components of information-communication infrastructure are included – what is natural for all technological solutions – in technical norms and directives. Any reference to norms and standards binding in technology, especially in rapidly changing domain of informatics and telecommunication, is aimed to unification and standardisation of requirements for tele-informative systems. At the same time, such legislative approach provides their compatibility and capacity for mutual "cooperation" (common level of compatibility for technical solutions and their capacity of co-operation).

Normative requirements of the state information-communication infrastructure perceived in such way were not accepted on the identical level. The requirements for tele-informative systems, public registers and exchange of information, and technical requirements for interoperability, have namely a minimal character. Due to this distinction, what is also reflected in the title and the systematics of disposition on the National Frames of Interoperability there is, firstly, no doubts that the specification of requirements for systems interoperability is wider than for the systems alone. It namely comprises – beside the organisational and technical requirements – additional semantic requirements, which are formulated at different levels of details and categorisation. Thus, the legislator passes the information that these are not the same catalogues/specifications of requirements, but they are determined by the properties of particular components of state information-

[19] It is „a catalogue of information features, including identifiers and characteristics of structural components of the information transfer corresponding to them, such as content of data field used to provide the coherence of public registers and to exchange information in electronic form with the public entities". See art. 3 pt. 10 of the Act on informatisation of public entities.

spół/zestaw został skonstruowany. Niemniej stanowią one – pomimo występujących między nimi różnic definicyjnych – spójny zespół czy zestaw określonych parametrów czy wartości (cech), gwarantujących prawidłowe funkcjonowanie systemów teleinformatycznych – przetwarzanie i transfer/wymianę danych. Po drugie, wymagania dla systemów teleinformatycznych rodzimy prawodawca przyjął na minimalnym poziomie. Jednocześnie odsyłając do norm technicznych i innych norm normalizacyjnych, nie precyzuje – pomimo sformułowania definicji legalnej pojęcia „minimalne wymagania" – samego pojęcia „minimalne". Podejmując próbę doprecyzowania tego pojęcia doktryna podkreśla, że „minimalne wymagania to niezbędne parametry pozwalające na prawidłowe współdziałanie systemów teleinformatycznych, a więc kompatybilnych i interoperacyjnych"[11]. Wobec tego przyjąć można, że „dzięki minimalnym wymaganiom, respektując różne technologie, powinna być umożliwiona wzajemna komunikacja, informacje zawarte w systemach organów naczelnych i centralnych powinny być dostępne na wszystkich szczeblach administracji i bez przeszkód dalej przekazywane w kontaktach z tzw. otoczeniem zewnętrznym"[12]. Po trzecie, wymagania te łącznie – niezależnie od tego, czy zostały przyjęte dla systemu teleinformatycznego, rejestrów publicznych, wymiany informacji, czy dla ich interoperacyjności - tworzą określony dla nich uniwersalny standard, który podmioty realizujące zadania publiczne obowiązane są stosować. Niewątpliwie określają one przyjmowany dla systemów teleinformatycznych, rejestrów publicznych i wymiany informacji model, wzorzec odpowiednio dla projektowania,

communication infrastructure for which that catalogue/specification was prepared. Nevertheless, they create – despite definition differences between them – a coherent set of specific parameters, or values (characteristics) warranting the proper functioning of tele-informative systems – processing and transfer-exchange of data. And secondly, the requirements for tele-informative systems were accepted by the national legislator at the minimal level. And at the same time after reference to technical norms and other normalising norms the alone notion of "minimal" is not defined despite formulation of a legal definition for the notion of "minimal requirements". In an attempt for precising this notion the doctrine stresses that „the minimal requirements are the indispensable parameters for correct cooperation of tele-informative systems, i.e. compatible and interoperating ones"[20]. Thus, it can be accepted that "the minimal requirements, respecting different technologies, provide mutual communication, and access to information contained in the systems of main and central institutions on each level of administration, and its transfer to the so called outer environment without any disturbances"[21]. And thirdly, these requirements jointly – independently if they were accepted for a tele-informative system, public registers, the exchange of information, or for its interoperability – create a universal standard specified for it which has to be followed by the entities performing the public tasks. They undoubtedly specify a model, or pattern, accepted for tele-informative systems, public registers and the exchange of information used respectively for designing, implemen-

[11] Tak A. Monarcha-Matlak, Obowiązki administracji w komunikacji elektronicznej, Oficyna 2008, Lex z 2022.
[12] A. Monarcha-Matlak, op. cit. wersja z Lex.
[20] As A. Monarcha-Matlak, Obligations of administration in electronic communication, Oficyna 2008, Lex 2022.
[21] A. Monarcha-Matlak, op. cit. version from Lex.

wdrażania i eksploatacji systemów teleinformatycznych, zarządzania usługami realizowanymi przez systemy teleinformatyczne, prezentacji danych w systemach teleinformatycznych oraz zarządzania bezpieczeństwem informacji[13]. Niektóre z tych wymagań przy tym same w sobie stanowią standard dla konkretnego elementu tej infrastruktury.

tation, and use of tele-informative systems, and for management of services provided by tele-informative systems, and for presentation of data in tele-informative systems, and for governing the security of information[22]. Some of these requirements create themselves the standards for a specific component of the infrastructure.

3. Klasyfikacja normatywnych wymagań bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa

Normatywne wymagania bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa są specyficzną, a zarazem niezwykle złożoną i zróżnicowaną, pod wieloma względami, kategorią prawną. Dzieje się tak za sprawą różnego centra prawodawczego i kaskadowej (odesłaniami pierwszego i drugiego stopnia) oraz kazuistycznej regulacji prawnej, ale przede wszystkim za sprawą ich odmiennej natury prawnej, dedykowanej poszczególnym, równie zróżnicowanym, elementom tej infrastruktury, rozległego i zróżnicowanego zakresu przedmiotowego, wreszcie ich interdyscyplinarnego charakteru, wymagającego wiedzy z przeróżnych dziedzin nauki, począwszy od nauk o technologii, a skończywszy na naukach społecznych. Są to też niezwykle zmienne w czasie parametry i właściwości technologiczne elementów składowych tej infrastruktury. Zmienność ta – dość dynamicznie zachodząca - jest pochodną pojawiania się na rynku usług telekomunikacyjnych w szybkim tempie nowej generacji, z punktu widzenia konstrukcji narzędzi, urządzeń i ich zabezpieczeń – rozwiązań tech-

3. State Information-communication Infrastructure Security Normative Requirements Classification

Normative requirements for the state information-communication infrastructure security create a specific, and highly complex and differentiated, legal category with many aspects. It is so due to different legislative centres, and descending (references of the first and second levels) and casuistic legal regulation, and most of all due to their changeable legal nature dedicated to particular, equally differentiated, components of the infrastructure, and a large and differentiated scope of the subject matter, and finally their interdisciplinary character demanding the knowledge in various domains of science, starting from technology sciences, and ending on social sciences. They also include technological parameters and properties of components of the infrastructure which are rapidly changing in time. This changeability – of enough dynamic rate – is a derivative of the rapid appearance on the market of telecommunication services of a new generation of technological solutions regarding the design of tools, devices, and their protections. It enforces in some way a permanent "up-

[13] Na temat bezpieczeństwa tworzenia i eksploatacji systemów teleinformatycznych zob. np. H. Tańska, A. Władzińska, Zróżnicowane aspekty bezpieczeństwa wytwarzanych systemów informatycznych, Rocznik KAE 2019, z. 40, s. 274 i n.

[22] About the safety of building and using tele-informative systems see e.g. H. Tańska, A. Władzińska, Distinct aspects of safety for developed informative systems, Yearly KAE 2019, notebook 40, p. 274 and next.

nicznych i technologicznych. Wymusza to niejako nieustanną „aktualizację" – obok bieżącego monitoringu prawidłowości funkcjonowania elementów infrastruktury informacyjno-komunikacyjnej państwa - wymagań bezpieczeństwa tej infrastruktury.

Znaczne różnicowanie normatywnych wymagań infrastruktury informacyjno-komunikacyjnej państwa skłania do podjęcia próby ich usystematyzowania. Zasadniczy podział jaki się rysuje na tle obowiązującej regulacji prawnej pozwala ująć je – przyjmując za kryterium podziału rodzaj normy prawnej – w dwie grupy: wymagania materialne, odnoszące się do samych warunków poszczególnych elementów tej infrastruktury, oraz procesowe, normujące reguły i mechanizmy postępowania oraz obowiązki podmiotów realizujących zadania publiczne przy użyciu systemów teleinformatycznych. Tak ujęty podział wymagań wyraża jednocześnie materialny i procesowy wymiar bezpieczeństwa informacyjnego państwa. Z tego punktu widzenia wymagania infrastruktury informacyjno-komunikacyjnej mają również dwojaki charakter, a mianowicie organizacyjno-prawny oraz techniczno-prawny. Te pierwsze, co oczywiste, z uwagi na ich naturę stanowią pewnego rodzaju prawne reguły ogólne, które podmioty publiczne obowiązane są uwzględniać przy tworzeniu i stosowaniu systemów teleinformatycznych. Te drugie zaś są w istocie normami technicznymi, ustanowionymi przez krajowe i/lub międzynarodowe organizacje normalizujące, które poprzez umieszczenie w normie prawnej rozporządzenia w sprawie Krajowych Ram Interoperacyjności, uzyskały rangę normy prawnej, lecz o charakterze technicznym. Podążając dalej kryterium odnoszącym się do normy prawnej daje się wskazać wymagania ustanowione na poziomie krajowym, międzynarodowym oraz unijnym – zarówno przez pań-

dating" of security requirements for this infrastructure conducted parallelly to a current monitoring of correct operation of the state information-communication infrastructure components.

A high distinction of normative requirements for the state information-communication infrastructure is a chance to take attempts for their systematisation. The general division which can be noted on the background of binding legal regulation allows for dividing them – taking the type of legal norm as a criterium of division – on two groups: material requirements relating entirely to conditions of particular components of this infrastructure, and processive requirements normalising the rules and mechanisms of procedures for entities performing the public tasks with the use of tele-informative systems. The material and processive dimension of state information security is at the same time reflected in such division of requirements. From this point of view the requirements of information-communication infrastructure also have a dual character, namely legal-organisational and legal-technological. The first ones create, what is obvious, regarding their nature, general legal rules of some kind which have to be observed by public entities at development and use of tele-informative systems. The second ones are in reality the technical norms settled by the national and/or international normalising organisations which through the incorporation into the legal norm of disposition on the National Frames of Interoperability received the category of legal norm, but of a technical nature. Following along the criterium relating to legal norm, some requirements can be indicated as established on the national, international and union levels by a state, international organisations, or by national or international normal-

stwo, organizacje międzynarodowe, jak i przez krajową lub międzynarodową jednostkę normalizacyjną lub jednostkę normalizacyjną UE, jak przykładowo: Polski Komitet Miar i Jakości, Internet Engineering Task Force (IETF) czy World Wide Web Consortium (W3C). Są to zarazem wymagania określone w powszechnie obowiązujących przepisach prawnych (rangi ustawowej i podustawowej) oraz w normach nie mających charakteru prawa stanowionego przez państwo, a zawartych w standardach lub rekomendacjach krajowej, międzynarodowej jednostki normalizującej lub jednostki normalizującej UE. Te pierwsze formułują wymagania na znacznym poziomie ogólności, a także poprzez odesłanie do konkretnie wskazanych norm normalizujących. Do tej kategorii należą: zasady ogólne konstruowania systemów teleinformatycznych (zasada neutralności technologicznej/zasada równego traktowania rozwiązań informatycznych, zasada jawności używanych standardów i specyfikacji, zasada prowadzenia rejestrów danych kontaktowych przy użyciu systemów teleinformatycznych, zasady używania oprogramowania interfejsowego) oraz wymagania dla systemów teleinformatycznych, rejestrów publicznych i wymiany informacji oraz ich interoperacyjności (wymagania semantyczne, organizacyjne i techniczne). Te drugie stanowią z kolei wskazane (indywidualnie oznaczone) szczegółowe normy, określające wzory i standardy dla poszczególnych elementów infrastruktury informacyjno-komunikacyjnej państwa oraz powinnego zachowania podmiotu publicznego oraz zawarte w tych normach zasady ogólne stosowania wymagań (jak: zasada kompletności wymagań oraz zasada równoważności wymagań). Wymagania infrastruktury informacyjno-komunikacyjnej można również pogrupować – wedle kryterium przedmiotu unormowania – na wymagania

ising body of the EU, as for instance: the Polish Committee of Measures and Quality, Internet Engineering Task Force (IETF), or the World Wide Web Consortium (W3C). They are at the same time the requirements specified in commonly biding legal regulations (on the level of act and sub-act) and in the norms which have not a character of any law established by the state, but are included in standards or recommendations of the national, international normalising body, or a normalising body of the EU. These first ones formulate the requirements on a significant level of generality and by referring to explicitly indicated normalising norms. This category includes: general principles for designing tele-informative systems (principle of technological neutrality/principle of equal treatment of informative solutions, principle of openness for used standards and specifications, principle for keeping contacting data registers with the use of tele-informative systems, principles for using the interface software) and the requirements for tele-informative systems, public registers, and the exchange of information and its interoperability (semantic, organisational and technical requirements). The second ones create on the other hand the indicated (individually marked) detailed norms determining the patterns and standards for particular components of the state information-communication infrastructure, and expected behaviour of the public entity, and the general principles included in these norms for application of the requirements (like: principle of completeness of requirements and principle of equivalency of requirements). Requirements of information-communication infrastructure may be also divided – according with criterium of normalised subject – on the requirements for tele-informative systems (designing, implementation, and use and upgrading,

dla systemów teleinformatycznych (projektowania, wdrażania i eksploatacji oraz modernizacji, wymagania dla kodowania znaków w dokumentach elektronicznych, prezentacji zasobów informacyjnych, systemu zarządzania bezpieczeństwem informacji), wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej, wymagania dla ustalania Krajowych Ram Interoperacyjności (KRI), wymagania dla interoperacyjności systemów teleinformatycznych oraz wymagania dla struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących. Przyjmując za punkt klasyfikacji wymagań rodzaje zabezpieczeń infrastruktury informacyjnej wskazywane są z kolei wymagania organizacyjne (administracyjne aspekty bezpieczeństwa informacji, w tym odpowiedzialność w zakresie postępowania z ryzykiem) oraz techniczne (bezpieczeństwa sprzętu, zarządzania systemami i sieciami, kontroli dostępu do sieci, systemów operacyjnych, aplikacji i informacji, przetwarzania mobilnego i pracy na odległość, poprawnego przetwarzania w aplikacjach, zabezpieczeń kryptograficznych oraz bezpieczeństwa plików systemowych) - realizowane w trzech obszarach: organizacyjnym (bezpieczeństwo osobowe), informatycznym i fizycznym[23]. Wreszcie – co istotne dla przyjętej w dalszej części charakterystyki wymagań infrastruktury informacyjno-komunikacyjnej państwa, a będącej w dużej mierze wynikiem dokonanego przez samego normodawcę rozróżnienia – wskazać można zasady ogólne oraz wymagania szczegółowe. Są to z jednej strony zasady ustalania wymagań dla systemów teleinformatycznych, jak: zasada neutralności technologicznej i zasada jawności używanych standar-

and requirements for coding the marks in electronic documents, presentation of informative resources, security information management system), the requirements for public registers and exchange of information in electronic form, requirements for establishing the National Frames of Interoperability (NFI), requirements for interoperability of tele-informative systems, and the requirements for the structures of electronic documents, data formats, and coding and communication protocols. On the other hand, taking the types of information infrastructure protections as a base of classification of the requirements there are indicated the organisational requirements (administrative aspects of information security, including the responsibility for proceeding with a risk), and technical ones (security of equipment, management of systems and networks, control of access to the net, operational systems, applications and information, mobile processing and distant work, proper processing in applications, cryptographic protections and security of systemic files) – executed in three areas: organisational (personal security), informative and physical[29]. And finally – what is important to the characteristics of requirements for the state information-communication infrastructure, and resulting in great degree from a distinction made by the normaliser himself – the general principles and detailed requirements may be indicated. On the one side they are the principles for establishing the requirements for tele-informative systems, such as: principle of technological neutrality and principle of openness of used standards and specifications[30]; and on the other side the principles

[23] Tak zob. J. Krawiec, System zarządzania bezpieczeństwem informacji – zabezpieczenia, Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie 2017 t. 15, z. 1(38), s. 48.

dów i specyfikacji[24]; z drugiej zaś zasady stosowania wymagań, jak: zasada kompletności wymagań oraz zasada równoważności wymagań[25]; wreszcie przykładowo zasady zarządzania bezpieczeństwem informacji[26] czy zasady przetwarzania danych w systemie teleinformatycznym[27]. Wymagania szczegółowe – konkretyzowane w normach standaryzujących i wskazujące konkretne rozwiązania technologiczne lub formaty i struktury dokumentów - można natomiast ująć w trzy grupy: wymagania techniczne, organizacyjne i semantyczne[28].

4. Zasady ogólne stosowane w procesie wdrażania, eksploatacji i modernizacji systemów teleinformatycznych

Zasada neutralności technologicznej, stosownie do jej definicji legalnej, oznacza „zasadę równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań". Zasada ta – ukształtowana pod koniec lat dziewięćdziesiątych niezależnie przez instytucje unijne oraz publiczne i

for application of requirements such as: the principle of completeness of requirements and the principle of equivalency of requirements[31]; and finally, for instance, the principles governing the information security[32], and principles for data processing in tele-informative system[33]. Detailed requirements – specified in standardising norms and recommending specific technological solutions, or formats and structures of documents – may be collected in three groups: technical, organisational and semantic requirements[34].

4. General Principles Used at Implementation, Use and Upgrades of Tele-informative Systems

The principle of technological neutrality, accordingly to its legal definition, means "the principle of equal treatment by the public authorities of tele-informative technologies, and creation of conditions for their fair competition, including prevention against elimination of competitive technologies at extension and modification of used tele-informative systems, or at creation of competitive products and solutions". The principle – formulated at the end of nineties independently by the Union institutions, and the

[29] See J. Krawiec, Information safety management system – safeguards, Scientific Notebooks of the High School of Informatics, Management and Administration in Warsaw, 2017 vol. 15, notebook 1(38), p. 48.
[30] See especially art. 1 pt. 2 and 3, art. 13 pos. 2 and art. 18 pt. 1 of the Act on informatisation of public entities and § 3 pos. 1 pt. 2 of disposition on NFI.
[24] Zob. zwłaszcza art. 1 pkt 2 i 3, art. 13 ust. 2 i art. 18 pkt 1 ustawy o informatyzacji podmiotów publicznych oraz § 3 ust. 1 pkt 2 rozporządzenia w sprawie KIR.
[25] Zob. np. pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN-ISO/IEC 27001, s. 7.
[26] Zob. np. § 20 ust. 2 pkt 8 czy 11rozporządzenia w sprawie KIR.
[27] Zob. art. 19h ustawy o informatyzacji podmiotów publicznych.
[28] Por. zwłaszcza § 5 - § 8 i rozdział III i IV rozporządzenia w sprawie KRI oraz art. 1 pkt 2 i pkt 3 oraz art. 3 pkt 9, pkt 10 i pkt 21, art. 13 ust. 1 ustawy o informatyzacji podmiotów publicznych.
[31] See e.g. pt. 1 titled Scope of the norm and pt. 0 titled Introduction subpoint 01 § five PN-ISO/IEC 27001, p. 7.
[32] See e.g. § 20 pos. 2 pt. 8 or 11 of disposition on NFI.
[33] See art. 19h of the Act on informatisation of public entities.
[34] Compare especially § 5 - § 8 and chapter III and IV of disposition on NFI and art. 1 pt. 2 and pt. 3 and art. 3 pt. 9, pt. 10 and pt. 21, art. 13 pos. 1 of the Act on informatisation of public entities.

prywatne podmioty na całym świecie biorące udział w szeroko rozumianym procesie tworzenia nowego reżimu prawnego dotyczącego technologii, a w szczególności technologii informacyjnych i komunikacyjnych[35] - postrzegana jest jako zasada tworzenia legislacji, w Europie jako zasada prawidłowej legislacji. Wedle tej zasady „w możliwym zakresie tworzone prawo (przepisy), mające na celu regulowanie rynku handlu elektronicznego, powinno być neutralne technologicznie, a to z kolei oznacza, że przepisy nie powinny zarówno wymagać, jak i wskazywać konkretnej technologii. (…) aby w przyszłości prawo nie utrudniało korzystania z technologii oraz jej rozwoju. (…) dla uniknięcia tworzenia niewłaściwych (nieproporcjonalnych) norm prawnych, należy tworzyć prawo przewidywalne, minimalistyczne, logiczne oraz proste"[36]. Doktryna wyraża wręcz pogląd, że „zasada neutralności technologicznej jako zasada prawna powinna służyć regulacji efektów istnienia i stosowania rozwiązań ICT, a nie regulacji technologii jako takiej. (…) Konstrukcja przepisów powinna w możliwie maksymalnym stopniu abstrahować od konkretnych technologii, tj. nie powinna wskazywać określonych rodzajów technologii, a kształtowanie przepisów faktycznie zapewniających realizację zasady neutralności technologicznej powinno być dokonywane w oparciu o faktyczne stosowanie technologii i ocenę wpływu stosowania tych technologii na realizację zasady równego traktowania podmiotów gospodarczych na rynku technologii informatycznych oraz zachowania warunków ich uczciwej konkurencji"[37]. Gwarancję realizacji tej zasady stanowi obowiązek podmiotu publicznego[38] zapewnienia aby system teleinformapublic and private entities all over the world participating in development of a new widely understood legal regime for technologies, and especially the information and communication technologies[47] - is perceived as the principle for developing the legislation, and in the Europe as the principle of proper legislation. Following the principle „the law (regulations) created for controlling the market of electronic trade has to be possibly neutral technologically, what means that the regulations shall not demand or recommend any specific technology. (…) to prevent any harm the law can inflict in the future to the use and development of technology. (…) to avoid development of improper (disproportional) legal norms the law has to be predictable, minimalistic, logical, and simple"[48]. The doctrine even expresses that „the principle of neutrality as the legal principle has to be used to control the effects of existence and application of ICT solutions, and not for control of alone technology. (…) The structure of the regulations has to be possibly far away from the specific technologies, i.e. it shall not indicate specific types of technology, and formulation of regulations actually providing the effectiveness of the principle for technological neutrality has to be performed on the basis of an actual use of technologies and evaluation of impacts these technologies can make to the effectiveness of the principle for equal treatment of economic entities on the market of informative technologies and preservation of conditions for their fair competition"[49]. The obligation of a public entity[50] for insurance that a teleinformative system used for execution of

[35] Zob. T. Filipowicz, Zasada równego traktowania wykonawców w zamówieniach publicznych dotyczących technologii informatycznych, LEX 2015, dostęp z dnia 13 lipca 2022 r.
[36] Zob. T. Filipowicz, op. cit., wersja z Lex.
[37] Zob. T. Filipowicz, op. cit., wersja z Lex i podana tam literatura.
[38] Zakres pojęciowy „podmiot publiczny" określa art. 2, zwłaszcza ust. 1 i ust. 2, ustawy o informatyzacji podmiotów publicznych.

tyczny używany do realizacji zadań publicznych spełniał – obok minimalnych wymagań dla tego systemu – także wymóg „równego traktowania rozwiązań informatycznych”[39].

Zasada jawności używanych standardów i specyfikacji, nie mająca swojej definicji legalnej, wyraża się z kolei w obowiązku podmiotów publicznych upublicznienia w Biuletynie Informacji Publicznej (BIP) lub udostępnienia w inny sposób określonych normatywnie informacji dotyczących używanych przez te podmioty systemów teleinformatycznych. Są to, w szczególności udostępniane w BIP: informacje o zestawie stosowanych w oprogramowaniu interfejsowym systemu teleinformatycznego (używanego przez ten podmiot do realizacji zadań publicznych) struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących, a także co do zasady testów akceptacyjnych[40]; oraz informacje o dostępności opisów uznanych na poziomie międzynarodowym standardów umożliwiających wymianę danych z innymi systemami teleinformatycznymi[41]. Obowiązek informacyjny podmioty publiczne realizują nadto poprzez opublikowanie w repozytorium interoperacyjności (na platformie ePUAP) opisu struktur danych (protokołów i struktur wymiany danych usługi sieciowej, struktur danych cech informacyjnych osób fizycznych, podmiotów i obiektów przestrzennych), oraz rekomendacji, stanowiących dobre praktyki ułatwiające osiągnięcie interoperacyjności na poziomie organizacyjnym, semantycznym i

public tasks has met – beside minimal requirements for this system – also the requirement “of equal treatment of informative solutions”[51] is a warranty for the effectiveness of this principle.

Principle of openness for used standards and specifications, even without its legal definition, is expressed by obligation of public entities for publication in the Bulletin of Public Information (BPI), or making accessible in other way, of the information, which is normatively specified, about tele-informative systems used by these entities. The BPI especially includes: information about a system of structures of electronic documents used in the interface software of tele-informative system (used by this entity for execution of public tasks), data formats and communication and coding protocols, and also, as a rule, the acceptation tests[52]; and the information about accessibility of descriptions of standards accepted on the international level enabling data exchange with other tele-informative systems[53]. Moreover, the informative obligation is fulfilled by public entities through publications in the interoperability repository (on platform ePUAP) of descriptions for data structure (protocols and structures of network service data exchange, and data structures of information characteristics of natural persons, subjects, and spatial objects), and recommendations belonging to good practices facilitating the achievement of interoperability

[47] See T. Filipowicz, Principle of equal treatment of contractors in public orders relating to informative technologies, LEX 2015, accessed on 13 July, 2022.
[48] See T. Filipowicz, op. cit., version from Lex.
[49] See T. Filipowicz, op. cit., version from Lex with included literature.
[50] The notional scope of „public entity” is determined by art. 2, especially pos. 1 and pos. 2, of the Act on informatisation of public entities.
[39] Zob. art. 13 ust. 2 pkt 1 w zw. z ust. 3 ustawy o informatyzacji podmiotów publicznych.
[40] Zob. art. 13 ust. 2 pkt 2 ustawy o informatyzacji podmiotów publicznych.
[41] Zob. § 16 ust. 3 rozporządzenia w sprawie KRI.

technologicznym[42]. Wyrazem tej zasady jest również obowiązek zapewnienia publicznej dyskusji nad rekomendacjami interoperacyjności[43] oraz obowiązek informowania o sposobie dostępu i zakresie użytkowym serwerów dla usług realizowanych przez podmioty publiczne i miejscu publikacji tych informacji oraz publikowania i uaktualniania w BIP opisów procedur obowiązujących przy załatwianiu spraw z zakresu ich właściwości drogą elektroniczną[44].

Zasada kompletności wymagań wyraża uniwersalną regułę, w myśl której przy wdrażaniu, eksploatacji i modernizacji systemów teleinformatycznych wykluczone jest pominięcie jakiegokolwiek z wymagań określonych w normie, jeśli podmiot publiczny realizujący zadania przy użyciu tych systemów, deklaruje zgodność systemów teleinformatycznych z normą międzynarodową[45]. Za prawidłowo skonstruowane i spełniające warunki bezpieczeństwa mogą zatem zostać uznane tylko takie systemy teleinformatyczne, które spełniają wszystkie ustanowione w normie standaryzującej kryteria.

Zasada równoważności wymagań oznacza natomiast, że przedstawione w normie wymagania nie odzwierciedlają ich wagi ani nie implikują kolejności, w jakiej powinny być one wdrażane, a elementy list są numerowane tylko po to, by umożliwić odwoływanie się do nich[46].

on the organisational, semantic, and technological levels[54]. The principle is also reflected in obligation for ensuring a public discussion on interoperability recommendations[55], and the obligation to inform about the way of access and the scope of use of servers for the services executed by the public entities, and about the place where the information is published, and to publish and update in the BPI the descriptions of procedures binding at handling the matters in the scope of their appropriate duties via electronic way[56].

The principle of completeness of requirements expresses a universal rule excluding any omitting of any requirement specified in a norm at implementation, use and upgrading of tele-informative systems if the public entity executes the tasks with the use of these systems and declares the compliance of these tele-informative systems with the international norm[57]. Therefore, only tele-informative systems meeting all criteria set in the standardising norm can be recognised as properly designed and fulfilling conditions of security.

The principle of equivalence of requirements means that the requirements listed in a norm do not reflect their meaning, nor implicate the order of their implementation, and the fragments of the list are numbered exclu-

[51] See art. 13 pos. 2 pt. 1 in reference to pos. 3 of the Act on informatisation of public entities.
[52] See art. 13 pos. 2 pt. 2 of the Act on informatisation of public entities.
[53] See § 16 pos. 3 of disposition on NFI.
[42] Zob. G. Szpor, K. Wojsyk, Tryb określenia minimalnych wymagań [w:] Cz. Martysz, G. Szpor, K. Wojsyk, Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz, Wydanie II, Lex 2015, oraz § 6, § 8 ust. 3 i § 10 ust. 5, ust. 6, ust. 11 i ust. 12 rozporządzenia w sprawie KRI.
[43] Zob. § 9 pkt 1 rozporządzenia w sprawie KRI.
[44] Zob. § 5 ust. 2 rozporządzenia w sprawie KRI.
[45] Przykładowo zob. pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN-ISO/IEC 27001, s. 7.
[46] Przykładowo zob. pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN-ISO/IEC 27001, s. 7.
[54] See G. Szpor, K. Wojsyk, Procedure for specification of minimal requirements [w:] Cz. Martysz, G. Szpor, K. Wojsyk, The Act on informatisation of operation of entities executing the public tasks. Comments, Edition II, Lex 2015, and § 6, § 8 pos. 3 and § 10 pos. 5, pos. 6, pos. 11 and pos. 12 of disposition on NFI.
[55] See § 9 pt. 1 of disposition on NFI.
[56] See § 5 pos. 2 of disposition on NFI.

W myśl tej zasady podmiot publiczny nie ma więc obowiązku – przy wdrażaniu i eksploatacji systemów teleinformatycznych – przestrzegania kolejności sformułowania w normie standaryzującej wymagań. Nie jest bowiem istotne, które wymagania zostaną wdrożone w pierwszej, a które w dalszej kolejności.

5. Wymagania organizacyjne infrastruktury informacyjno-komunikacyjnej państwa

Wymagania organizacyjne - wobec braku ich definicji legalnej – można określić, w oparciu o całokształt regulacji prawnej, zwłaszcza rozporządzenia w sprawie Krajowych Ram Interoperacyjności, jako zespół różnego rodzaju „aktywności o charakterze organizacyjnym" (działań) oraz „procedur organizacyjnych", a także zespół obowiązków, które podmioty publiczne powinny wykonywać: po pierwsze, w celu zapewnienia „funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności" systemów teleinformatycznych oraz w celu zastosowania przewidzianych dla tych systemów norm oraz uznanych w obrocie profesjonalnym standardów i metod; po drugie, w celu zapewnienia poufności, dostępności i integralności danym przetwarzanym i przesyłanym za pośrednictwem tych systemów; a po trzecie, w celu dostarczania usług za pośrednictwem tych systemów na deklarowanym poziomie dostępności i w oparciu o udokumentowane procedury. Jest to zatem zestaw „efektywnych i udokumentowanych" zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania - zestaw wymagań składających się na przyjętą przez podmioty realizujące zadania publiczne polity-

sively for the reference reasons[58]. According to the principle a public entity at implementation and use of tele-informative systems is not obliged to follow the order the requirements are formulated in the standardising norm. Thus, the order of requirements implementation is not important.

5. State Information-communication Infrastructure Organisational Requirements

Organisational requirements – at the lack of their legal definition – may be described on the ground of a wholesome legal regulation, and especially the disposition on the National Frames of Interoperability, as a system of different types of "activities of organisational character" (actions) and "organisational procedures", and also a system of obligations which the public entities have to fulfil: firstly, to provide „functionality, reliability, usefulness, efficiency, transferability, and curability" of tele-informative systems, and to apply the norms and standards and method accepted in professional trading into these systems; secondly, to provide confidentiality, accessibility and integrity of data processed and transferred via these systems; and thirdly, to provide services by means of these systems on a declared level of accessibility and on the base of documented procedures. Thus, it is a system of „efficient and documented" principles and procedures together with a schedule for its implementation and execution – specification of requirements contributing into the policy of security in information domain accepted by the entities performing the public tasks[70]. The sum

[57] See e.g. pt. 1 titled Scope of norm and pt. 0 titled Introduction subpoint 01 § five PN-ISO/IEC 27001, p. 7.
[58] See for instance pt. 1 titled Scope of norm and pt. 0 titled Introduction subpoint 01 § five PN-ISO/IEC 27001, p. 7.

kę bezpieczeństwa w sferze informacyjnej[59]. Suma tak ujętych wymagań organizacyjnych – wespół zastosowanych przez podmiot publiczny – stwarza w założeniu normodawcy gwarancję bezpieczeństwa warstwy technologicznej sfery informacyjnej państwa[60].

Wymagania te na poziomie rozporządzenia w sprawie Krajowych Ram Interoperacyjności normodawca określa, po pierwsze, odwołując się - najogólniej to ujmując – do celu, który podmiot publiczny ma osiągnąć wprowadzając i używając określony system teleinformatyczny oraz system zarządzania bezpieczeństwem informacji, a wyrażony niedookreślonymi zwrotami odpowiednio „funkcjonalność", „niezawodność", „używalność", „wydajność", „przenaszalność" oraz „pielęgnowalność", „poufność", „dostępność" i „integralność", przy jednoczesnym uwzględnieniu atrybutów bezpieczeństwa samych informacji, również ujętych w sposób niedookreślony pojęciami takimi jak: „autentyczność", „rozliczalność", „niezaprzeczalność" i „niezawodność". Po drugie - wskazując na pewien minimalny, niekiedy przykładowy, katalog obowiązków lub działań podejmowanych przez pomiot publiczny - konstruuje warunki umożliwiające bezpieczeństwo systemu teleinformatycznego i systemu zarządzania bezpieczeństwem informacji i tym sposobem wskazuje drogę do osiągnięcia zakładanych celów przy używaniu systemów teleinformatycznych. Po trzecie, wymagania organizacyjne normodawca uznaje za spełnione, gdy system teleinformatyczny i system zarządzania bezpieczeństwem informacji został sporządzony z uwzględnieniem lub opracowany na podstawie konkretnie wskazanych (zindywidualizowanych) Polskich Norm (ISO). Odesłanie to

of such organisational requirements – applied jointly by the public entity – is, in intention of the legislator, a warranty of security of the technological layer in the state information domain[71].

These requirements are identified by the normaliser on the level of disposition for the National Frames of Interoperability, firstly, referring to – in general – the objective which the public entity has to achieve by introduction and use of a specific teleinformative system and the system for information security management, and which is expressed respectively by unprecise terms of "functionality", "reliability", "usefulness", "efficiency" "transferability", "curability", "confidentiality", "accessibility", and "integrity", at simultaneous regard to the security attributes of the information alone, which are also presented imprecisely by such terms as: „authenticity", „accountability", „non-denying" and „reliability". Secondly, pointing to a minimal and sometimes exemplary catalogue of obligations or activities undertaken by the public entity, the normaliser forms the conditions for the security of teleinformation system and the information security management system to indicate in this way a method for achievement of assumed objectives at the use of teleinformative systems. And thirdly, the normaliser assumes that the organisational requirements are met if tele-informative system and the information security management system were prepared or developed on the ground of specifically indicated (individualised) Polish Norms (ISO). The mentioned reference makes the entities using

[70] For procedural regulations in the area of application of management informative technologies see for instance P. Zaskórski, K. Szwarc, op. cit., especially p. 47/48.
[59] Na temat uregulowań proceduralnych w obszarze stosowania informatycznych technologii zarządzania zob. np. P. Zaskórski, K. Szwarc, op. cit., zwłaszcza s. 47/48.
[60] Por. § 15 i § 20 rozporządzenia w sprawie KRI.
[71] Compare § 15 and § 20 of disposition on NFI.

sprawia, że podmioty używające systemów teleinformatycznych zostały wyposażone - poza wskazaniem celów, które muszą uwzględnić przy stosowaniu tych systemów – w konkretne „narzędzia", służące do osiągnięcia minimalnych wymagań dla systemów teleinformatycznych, wskazówki co do sposobu realizacji zakładanych celów. Po czwarte, na poziomie rozporządzenia zapewnienie minimalnych wymogów organizacyjnych wyraża: w zakresie zarządzania usługami informatycznymi (IT) obowiązek dostarczenia usług publicznych *online* na deklarowanym przez podmiot publiczny poziomie dostępności i w oparciu o udokumentowane procedury[61]; w zakresie zarządzania bezpieczeństwem informacji zaś – obowiązek zapewnienia warunków umożliwiających realizację i egzekwowanie przykładowo wymienionych – lecz różnorodnych co do charakteru – działań, które uproszczając obejmują procedury i mechanizmy zapewnienia bezpieczeństwa informacji na pożądanym poziomie[62]. Osiągnięcie interoperacyjności systemów teleinformatycznych na poziomie organizacyjnym zapewnia z kolei nałożony na podmioty publiczne: obowiązek informacyjny o sposobie dostępu oraz zakresie użytkowym serwerów, a także miejscu publikacji tych informacji; obowiązek publikowania i aktualizowania opisów procedur obowiązujących przy załatwianiu spraw drogą elektroniczną; oraz obowiązek standaryzacji i ujednolicenia procedur w sposób zapewniający poprawną współpracę podmiotów realizujących zadania publiczne[63].

Na poziomie Polskich Norm (Technika Informatyczna)[64], uniwersalnych dla każdej, bez

tele-informative systems were equipped with – beside indication of objectives which have to be regarded at application of these systems – some specific "tools" for achieving minimal requirements for tele-informative systems, the guidelines facilitating the execution of assumed objectives. And fourthly, on the level of disposition the assurance of minimal organisational requirements addresses: for the management of informative (IT) services the obligation to provide public services *online* at the level of accessibility declared by the public entity and on the basis of documented procedures[72]; for the management of information security – the obligation to provide conditions for performance and execution of exemplary listed – but different in character – activities which in general include procedures and mechanisms for assurance of information security at the demanded level[73]. Achieving the interoperability of tele-informative systems on the organisational level assures in turn the obligation, imposed on the public entities: to inform about ways of accessing the servers and their scope of using, and also about the place where this information is published; to publish and update descriptions of procedures which have to be observed at handling the matters in an electronic way; and to standardise and unify the procedures to provide proper cooperation of entities performing public tasks[74].

On the level of the Polish Norms (Informatic Technology)[75], which are universal for each organisation using tele-informative

[61] Zob. § 15 ust. 1 i ust. 2 rozporządzenia w sprawie KRI.
[62] Zob. § 20 ust. 2 rozporządzenia w sprawie KRI.
[63] Zob. § 5 ust. 2 rozporządzenia w sprawie KRI.
[64] Na temat norm w zakresie bezpieczeństwa informacyjnego szerzej zob. K. Bobkowski, Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji, Zarządzanie i Finanse *Journal of Management and Finance* Vol. 16, No. 3/2/2018, s. 20 i n.
[72] See § 15 pos. 1 and pos. 2 of disposition on NFI.
[73] See § 20 pos. 2 of disposition on NFI.
[74] See § 5 pos. 2 of disposition on NFI.

względu na jej publiczny czy prywatny charakter organizacji używającej systemów teleinformatycznych, występuje wielość norm (organizacyjnych) przyjmowanych przez rodzime i międzynarodowe, w tym unijne, organizacje normalizacyjne i standaryzujące. Normy te ustanawiają warunki organizacyjne dla różnych elementów bezpieczeństwa systemów teleinformatycznych, jak: zarządzanie usługami IT czy zarządzanie bezpieczeństwem informacji, w tym odrębnie wymagania, specyfikacje i procedury. Ich wspólnym mianownikiem jest to, iż konstruują one pewien katalog szczegółowo i precyzyjnie określonych obowiązków organizacji, a więc i podmiotów publicznych, dla normowanego obszaru. W oparciu o Polskie Normy - które uwzględniają normy ISO, a wręcz je powielają – przykładowo w zakresie zarządzania usługami IT[65] oraz w zakresie zarządzania bezpieczeństwem informacji[66] można sformułować ogólnie ujęty zakres ich unormowania, a w konsekwencji katalog obowiązków podmiotów publicznych względem stosowanych systemów teleinformatycznych. Zakres

systems, independently if public or private, there are many (organisational) norms accepted by the national and international, including the Union, normalising and standardising organisations. These norms identify organisational conditions for different components of security in tele-informative systems, such as: management of IT services or the security of information including distinct requirements, specifications and procedures. Their common denominator is that they create a catalogue of specific obligations for organisations, including also the public entities, for the normalised domain which are specified in details and precisely. On the ground of the Polish Norms – which regard the ISO norms, and usually follow them – for instance in the management of IT services IT[76] and in management of information security[77], a generally perceived range of their normalisation, and in consequence a catalogue of obligations for public entities against the applied tele-informative systems, may be formulated. The subjective scope of

[75] Find more about norms on information safety in K. Bobkowski, Management of information safety in the view of selected normative acts for the Information Safety Management System, Management and Finance, *Journal of Management and Finance* Vol. 16, No. 3/2/2018, p. 20 and next.

[65] Zob. standard ISO/IEC 20000, na który składają się dwie normy: ISO/IEC 20000-1:2011 - International Standard - Information Technology - Service Management - Part 1: *Service management system requirements* oraz ISO/IEC 20000-2:2005 - *International Standard - Information Technology - Service Management - Part 2: Code of practice*. Ich polska, zharmonizowana wersja opublikowana została w 2007 roku. Polskie wydanie niczym nie różni się od oryginału: PN-ISO/IEC 20000-1:2007 - Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja oraz PN-ISO/IEC 20000-2:2007 - Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania.

[66] Zob. PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji - Wymagania; PN-ISO/IEC 27002:2017-06/Ap1 Technika informatyczna Techniki bezpieczeństwa Praktyczne zasady zabezpieczania informacji - w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005:2011 Zarządzanie Ryzykiem w Systemach Bezpieczeństwa Informacji.

[76] See standard ISO/IEC 20000, containing two norms: ISO/IEC 20000-1:2011 - International Standard - Information Technology - Service Management - Part 1: *Service management system requirements* and ISO/IEC 20000-2:2005 - *International Standard - Information Technology - Service Management - Part 2: Code of practice*. Its Polish harmonised version was published in 2007. The Polish edition is identical to original: PN-ISO/IEC 20000-1:2007 – Information technology – Service management – Part 1: Specification and PN-ISO/IEC 20000-2:2007 – Information technology – Service management – Part 2: Code of Practice.

[77] See PN-EN ISO/IEC 27001:2023-08 Security of information, cybersecurity and protection of privacy – Information security management systems – Specifications; PN-ISO/IEC 27002:2017-06/Ap1 Information technology Security technologies Practical principles for safeguarding the information – in reference to establishment of safeguards; PN-ISO/IEC 27005:2011 Risk Management in Information Security Systems.

przedmiotowy tych norm co prawda różni się, bowiem w pierwszym przypadku zapewnia ramy i systematyczne podejście do planowania, wdrażania, obsługi, przeglądu, utrzymania i doskonalenia systemu zarządzania usługami informatycznymi; w drugim zaś zawiera wymagania dotyczące wdrożenia zabezpieczeń chroniących aktywa informacyjne organizacji. Niemniej jednak – poza tą różnicą przedmiotową – normy te posiadają pewien wspólny trzon unormowania i określają zestaw działań o charakterze organizacyjnym, które podmioty zobowiązane są podjąć w celu zapewnienia bezpieczeństwa poszczególnych elementów systemów teleinformatycznych, a składających się na infrastrukturę informacyjno-komunikacyjną. W pierwszej kolejności normy te wskazują, w pewnym znacznym uproszczeniu to ujmując, na konieczność określenia przez organizacje – podmioty publiczne polityki i celów przyjmowanego systemu zarządzania czy to usługami IT, czy to bezpieczeństwem informacji, w tym przyjmowanych zabezpieczeń, oraz czynników wewnętrznych i zewnętrznych istotnych dla celów działania organizacji. Działania te pozwalają tym podmiotom zrozumieć odpowiednio jak zarządzać zasobami, wdrażać niezbędne środki nadzoru i określać jasne cele w doskonaleniu świadczenia usług, a także określać i szacować ryzyko a następnie identyfikować i oceniać warianty postępowania z ryzykami oraz przygotowywać deklaracje stosowania zabezpieczeń. W efekcie pozwala na przyjęcie systemu zarządzania bezpieczeństwem zgodnie z obowiązującymi przepisami prawnymi i wymaganiami oraz innymi zobowiązaniami podmiotu, a także na regularne sprawdzanie stanu jego zgodności z tymi regułami. To ułatwia ciągłe doskonalenie systemu zarządzania w celu zwiększenia jego wyników. Za konieczny element zapewnienia bezpieczeństwa systemom teleinformatycznych w wymiarze organizacyjnym normy te uznają po-

these norms is different anyway, as in the first case it provides the frames and a systematic approach to planning, implementation, handling, overhaul, maintenance and improvement of the system managing the tele-information services; and in the second case it contains requirements for implementation of safeguards protecting the informative assets of an organisation. Nevertheless, despite this subjective difference, the norms have a common domain of normalisation and describe a catalogue of actions of organisational character which have to be implemented by the entities to safe the security of particular components of tele-informative systems, contributing to the information-communication infrastructure. In the first turn and at some simplifications, these norms point out a necessity for organisations – public entities to determine the policy and objectives of the accepted system for management of IT services or safety of information, including implemented safeguards, and the inner and outer factors important for the activities of the organisation. These activities are helpful for these entities in respectful understanding how to control the resources, implement necessary means of supervision and identify well defined objectives for improvement of rendered services, and also to identify and estimate the risk and next identify and evaluate the options of dealing with the risks and to prepare declarations for application of safeguards. Finally, it allows for acceptation of the security management system according to the binding legal regulations and requirements, and with other obligations of the entity, and also for checking its compliance with these regulations. It facilitates a continuous improvement of the management system to increase its efficiency. As a necessary component of assurance of security for tele-informative sys-

dział ról kierownictwa organizacji w zapewnieniu bezpieczeństwa informacji, odpowiedzialności i uprawnień w zakresie zapewnienia zgodności systemu zarządzania bezpieczeństwem informacji z wymaganiami normy międzynarodowej, obowiązującej dla danego systemu. Odrębne unormowania normy dedykują planowaniu systemów zarządzania usługami czy bezpieczeństwem informacji, w tym obowiązkowi opracowania i wdrożenia postępowania z ryzykiem w bezpieczeństwie informacji oraz ustanowienia celów tego bezpieczeństwa dla odpowiednich funkcji i szczebli organizacji. Wprowadzają również obowiązek organizacji określenia i zapewnienia zasobów potrzebnych do ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji (analogicznie usług), w tym określenia kompetencji i nadzoru nad osobami wykonującymi pracę przy systemach, uświadomienia pracowników w zakresie polityki bezpieczeństwa informacji czy potrzeb w zakresie komunikacji wewnętrznej i zewnętrznej dotyczącej systemu zarządzania bezpieczeństwem informacji. Dwie ostatnie pozycje normy poświęcone są katalogowi działań operacyjnych. Katalog ten obejmuje, po pierwsze, planowanie i nadzór nad działaniami operacyjnymi, monitorowanie, pomiar, analizę i ocenę wyników działań na rzecz bezpieczeństwa informacji oraz skuteczności systemu zarządzania bezpieczeństwem informacji i usług; po drugie, okresowe audyty wewnętrzne w zakresie zgodności systemu zarządzania bezpieczeństwem z przyjętymi wymaganiami, skuteczności wdrożenia i utrzymania systemu oraz okresowe przeglądy systemu zarządzania bezpieczeństwem informacji, w celu zapewnienia jego stałej przydatności, adekwatności i skuteczności; a po trzecie, także doskonalenie systemów, w tym wprowadzanie działań korygujących w razie stwierdzenia niezgodności z normami. Dla zindywidualizowania tych ogól-

tems in the organisational dimension these norms accept the division of tasks in the organisation management in assurance of information safety, responsibility and entitlements ensuring the compliance of the information safety management system with the requirements of the international norm binding for a given system. Distinct normalisations of the norm are dedicated to planning management systems for services, or information safety, including the obligation for development and implementation of procedures dealing with the risk in the safety of information, and to establish the objectives of this safety for relevant functions and levels of the organisation. They also introduce the obligation of the organisation for determination and provision of resources needed for establishment, implementation, holding and permanent improvement of the information security management system (and services), including specification of competences and supervision over personnel working with the systems, and for making the personnel aware over the policy of information security, or the demands of outer and inner communication for the security information management system. The two last positions of the norm are dedicated to a catalogue of operational actions. The catalogue includes, firstly, planning and supervision over the operational actions, monitoring, measurement, analysis and evaluation of results of actions in favour of the safety of information and the efficiency of information and services security management system; and secondly, the periodical inner audits for compliance of the security management system with accepted requirements, efficiency of implementation and maintenance of the system, and periodical overhauls of the information security management system to provide its permanent usefulness, adequacy,

nie określonych w normie standaryzującej obowiązków normodawca, na poziomie rozporządzenia w sprawie Krajowych Ram Interoperacyjności, wskazał w zakresie systemu zarządzania bezpieczeństwem informacji konkretne działania, które podmioty publiczne obowiązane są realizować, w oparciu o przyjęte przez te podmioty akty wewnętrzne, jak przykładowo: szkolenia osób uczestniczących w procesie przetwarzania informacji, uaktualnianie oprogramowania służącego do przetwarzania danych, okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji czy aktualizację regulacji wewnętrznych w zakresie zmieniającego się otoczenia[67].

Dla zobrazowania różnorodności normatywnych wymogów organizacyjnych można – na przykładzie systemu zarządzania bezpieczeństwem informacji i w oparciu o zestaw działań (obowiązków) organizacji – podzielić je na kilka podstawowych przykładowo wyróżnionych grup. Po pierwsze, są to wymagania w zakresie bezpieczeństwa informacji i zasad postępowania z informacją; po drugie, wymagania w zakresie przyjętego poziomu bezpieczeństwa w systemie teleinformatycznym oraz czynności, w tym prawnych, dotyczących serwisowania tych systemów; po trzecie, są to wymagania w zakresie kompetencji i uprawnień personelu organizacji; po czwarte, wymagania w zakresie monitorowania stanu i aktualności zasad, reguł wewnętrznych stosowanych w organizacji w zakresie bezpieczeństwa informacyjnego, sprzętu i oprogramowania; po piąte, wymagania w zakresie okresowych analiz dotyczących ryzyk związanych z incydentami, okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji; oraz po szóste, wymagania w zakresie zasad i procedur gwarantujących przetwarzanie informacji mobilnie i zdalnie.

and efficiency; and thirdly, the improvements of systems including the corrective actions in the case of any incompliances with the norms. In order to individualise these duties which are generally specified in the standardising norm the normaliser indicated, in disposition on the National Frames of Interoperability, specific actions for the information security management system which have to be performed by the public entities on the basis of inner acts accepted by these entities, as for instance: training of persons involved in processing of information, updating the software for data processing, periodical analyses of risk for a loss of integrity, accessibility or confidentiality of information, or updating the inner regulations against the changeable environment[78].

In order to show the variety of organisational normative demands – on the example of an information security management system and on the base of a catalogue of organisation actions (obligations) – they can be divided into a few basic groups which are distinguished in the example. Firstly, they are the requirements for the safety of information and principles of handling the information; secondly, the requirements for the accepted level of safety in tele-informative system and the activities, including legal ones, for servicing these systems; thirdly, they are the requirements for the scope of competences and entitlements of organisation personnel; fourthly, the requirements for monitoring the status and validity of inner principles, rules applied in the organisation to information security, equipment and software; fifthly, the requirements for periodical analyses of risks connected with the incidents, and periodical inner audit over the information security; and sixthly, the require-

[67] Katalog przykładowych działań wymienia § 20 ust. 2 rozporządzenia w sprawie KIR.
[78] A catalogue of exemplary actions is listed in § 20 pos. 2 of disposition on NFI.

Ujęte w ten sposób normatywne wymagania organizacyjne systemów teleinformatycznych wyrażają niewątpliwie ideę ciągłego udoskonalania systemu teleinformatycznego i systemu zarządzania bezpieczeństwem informacji, która wywodzi się z modelu procesu zarządzania opartego na tzw. cyklu *Deminga* (planuj - wykonuj - sprawdzaj - działaj, ang. *Plan - Do - Check - Act*)[68]. Wymagania te tworzą bowiem reguły prawno-organizacyjne przyjmowane przez podmioty publiczne w toku procesu projektowania, wdrażania, eksploatowania, monitorowania, przeglądania, utrzymania i udoskonalania samego systemu teleinformatycznego i systemu zarządzania bezpieczeństwem danych przetwarzanych i przekazywanych za pośrednictwem tego systemu. Reguły te umożliwiają temu podmiotowi realizację i egzekwowanie określonych działań, które są podejmowane w celu zagwarantowania bezpieczeństwa sytemu teleinformatycznego oraz przetwarzanych i przekazywanych przy jego udziale danych. Instrumentami umożliwiającymi kontrolę jakości i integralności systemów informacyjnych administracji są zaś – jak podkreśla doktryna – „standardy informacyjne i teleinformatyczne"[69].

6. Wymagania technologiczne infrastruktury informacyjno-komunikacyjnej państwa

Wymogi technologiczne odnoszą się – stosownie do ich nazwy - do warstwy technicznej systemów teleinformatycznych, a więc takich

The normative organisational requirements of tele-informative systems presented in this way undoubtedly express an idea of permanent improvement of a tele-informative system and an information safety management system originating from a model of management process based on the so called *Deming's* cycle (Plan – Do – Check – Act)[79]. These requirements, namely, create the organisational-legal rules accepted by the public entities in the process of designing, implementation, using, monitoring, overhauling, maintaining, and improving of an alone tele-informative system, and a system managing the security of data processed and transferred by this system. These rules make the entity can perform and execute specific actions which are taken to warrant the safety for tele-informative system and for data processed and transferred with its use. And „information and tele-informative standards"[80] are tools controlling the quality and integrity of administration information systems, according to the doctrine.

6. State Information-communication Infrastructure Technological Requirements

Technological requirements relate – according to their name – to technological layer of tele-informative systems, thus to such

[68] Szerzej na temat tzw. cyklu *Deminga* zob. K. Świtała, Prawnoadministacyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych, PPP 2013 nr 10, s. 21-30, Lex 2022 dostęp 30 czerwca 2023 r. i K. Bobkowski, op. cit., s. 24 i n.

[69] J. Oleński, Standardy informacyjne w e-administracji [w:] Z. Olejniczak, J.S. Nowak, J.K. Grabara, Systemy informatyczne w administracji, Warszawa 2004, s. 29.

[79] Wider about the so called Deming's cycle see K. Świtała, Legal and administrative aspects of information security issues in public entities, PPP 2013 nr 10, p. 21-30, Lex 2022 accessed on 30, June 2023 and K. Bobkowski, op. cit., p. 24 and next.

[80] J. Oleński, Information standards in e-administration [w:] Z. Olejniczak, J.S. Nowak, J.K. Grabara, Informative systems in administration, Warsaw 2004, p. 29.

elementów infrastruktury informacyjno-komunikacyjnej jak: sieci, urządzenia, sprzęt czy oprogramowanie umożliwiające wymianę danych. Wymogi te prawodawca określa poprzez odesłanie do norm technicznych oraz uznawanych w obrocie profesjonalnym standardów i metodyk[81]. Odesłanie to obejmuje odpowiednie Polskie Normy (PN), normy międzynarodowe, a nawet standardy uznawane w drodze dobrej praktyki przez organizacje międzynarodowe i powszechnie stosowane w obrocie gospodarczym dotyczącym narzędzi telematycznych. Wymagania technologiczne nie stanowią jednolitej, lecz zróżnicowaną pod względem zastosowania i pochodzenia, kategorię wymagań. Można w ich katalogu wskazać wymagania obowiązujące przy projektowaniu, wdrażaniu i eksploatacji systemów teleinformatycznych, wymagania dla zarządzania usługami realizowanymi przez systemy teleinformatyczne, wymagania dla sprzętu i oprogramowania stosowanego do wymiany danych z innymi systemami, wymagania dla kodowania znaków w dokumentach wysyłanych z systemów teleinformatycznych, wymagania dla formatów danych udostępnianych za pośrednictwem systemów teleinformatycznych, wymagania dla prezentacji zasobów informacji oraz wymagania dla systemu zarządzania bezpieczeństwem informacji[82].

Normodawca w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności przyjmuje dwie techniki określenia tych wymagań. Zasadniczo – nie wnikając w technologiczne aspekty infrastruktury - wskazuje, które konkretne (indywidualnie oznaczone) normy niekiedy nawet różne z nich dedykuje konkretnemu elementowi systemu (infrastruktury) lub systemowi jako całości[83]. W efekcie regulacja

components of the information-communication infrastructure as: the nets, equipment, or software for data exchange. The legislator specifies these requirements by reference to technical norms and to the standards and methodologies which are accepted in the professional trade[90]. The reference includes relevant Polish Norms (PN), international norms, and even the standards recognised in the way of a good practice by international organisations and commonly used in economic trade for telematic tools. Technological requirements are not a uniform category of requirements but are a distinct category regarding the application and origin. In their catalogue the requirements may be pointed out as binding at designing, implementation, and the use of tele-informative systems, the requirements for governing the services performed by tele-informative systems, requirements for hardware and software used for data exchange with other systems, requirements for coding the marks in documents sent out with tele-informative systems, requirements for data formats available by tele-informative systems, requirements for presentation of information resources and requirements for the information safety management system[91].

The normaliser in disposition on the National Frames of Interoperability accepts two techniques for specification of these requirements. In general – omitting technological aspects of infrastructure – he points out specific norms (individually denominated), sometimes different of them, are dedicated to a specific component of the system (infrastructure) or to the system as the whole[92]. In effect the regulation of the disposition for

[81] Por. § 15 i n. oraz § 5 pkt 4 w zw. z § 15 i n. rozporządzenia w sprawie KRI.
[82] Zob. § 15 do § 21 rozporządzenia w sprawie KRI.
[83] Przykładowo § 15 ust. 3, § 17 ust. 1, § 18 czy § 19 oraz załącznik nr 2, 3 i 4 rozporządzenia w sprawie KRI.
[90] Compare § 15 and next and § 5 pt. 4 in relation to § 15 and next of disposition on NFI.
[91] See § 15 to § 21 of disposition on NFI.

rozporządzenia w zakresie wymogów technologicznych systemów teleinformatycznych jest kazuistyczna i szczegółowa, by nie powiedzieć zindywidualizowana, a dla określenia standardu wystarczająca jest analiza rozporządzenia, w tym poszczególnych jego załączników i pozycji. Jednocześnie w pewnych sytuacjach normodawca pozostawia podmiotowi publicznemu pewną dozę swobody wyboru standardu, a swobodę tę określa dwojako[84]. Raz bowiem, jak ma to miejsce w przypadku formatu danych, jedynie zezwala na wybór jednego z możliwych do zastosowania ze wskazanych standardów, co wyraża zwrotem „co najmniej jednego z formatów danych określonych w", bez jakichkolwiek wskazówek dokonywania wyboru, pozostawiając tym samym podmiotowi całkowitą swobodę wyboru[85]. Innym zaś razem, posiłkując się normatywnym pojęciem niedookreślonym „w pewnych uzasadnionych przypadkach", dopuszcza zastosowanie równorzędnych i alternatywnych norm technicznych, jak w przypadku kodowania znaków w dokumentach[86]. Zastrzega jednak, że zastosowanie w tych przypadkach alternatywnego (zamiennego) wymogu (standardu) technologicznego dopuszczalne jest pod warunkiem, że ów alternatywny standard nie wpłynie negatywnie na współpracę z systemami teleinformatycznymi używającymi podstawowego standardu[87]. Dla systemu zarządzania bezpieczeństwem informacji w przypadkach uzasadnionych analizą ryzyka normodawca zaleca natomiast – poza obligatoryjnym zastosowaniem wskazanego standardu technologicznego – zastosowanie dodatkowego zabezpieczenia, lecz nie wskazuje konkretnego standardu dla tego zabezpieczenia[88].

technological demands of tele-informative systems is casuistic and detailed, if not individualised, and for identification of the standard the analysis of the disposition, including particular annexes and positions, is sufficient. At the same time, in some cases, the normaliser leaves for the public entity a margin of freedom at selection of a standard and specifies this freedom in two ways[93]. Once, namely, as it is in the case of data format, he allows for selection of one of indicated standards which can be used, what is addressed in wording „at least one of data formats specified in", without any hints for the choice, and by the same leaving the whole freedom of choice to the entity[94]. In another case, using imprecise normative denomination „in certain reasonable cases" he permits the use of equivalent and alternative technical norms, as in the case of coding the marks in documents[95]. But he stipulates the application of an alternative (replacing) technological demand (standard) in these cases is acceptable provided that this alternative standard will not jeopardise the cooperation with tele-informative systems using the basing standard[96]. Moreover, for the information safety management system in cases substantiated by the analysis of risk the normaliser recommends – beside the obligatory application of indicated technological standard – the application of an additional safeguard, but he does not indicate a specific standard for this safeguard[97]. By using imprecise denominations in form of „reasonable case" and „cases substantiated by the

[92] For instance § 15 pos. 3, § 17 pos. 1, § 18 or § 19 and annex nr 2, 3 and 4 of disposition on NFI.
[84] Zob. § 17 ust. 2 i § 18 rozporządzenia w sprawie KRI.
[85] Zob. § 18 rozporządzenia w sprawie KRI.
[86] Zob. § 17 ust. 2 rozporządzenia w sprawie KRI.
[87] Zob. § 17 ust. 3 rozporządzenia w sprawie KRI.
[88] Zob. § 20 ust. 3 i ust. 4 rozporządzenia w sprawie KRI.
[93] See § 17 pos. 2 and § 18 of disposition on NFI.
[94] See § 18 of disposition on NFI.
[95] See § 17 pos. 2 of disposition on NFI.

Poprzez zastosowanie pojęcia niedookreślonego w postaci „uzasadniony przypadek" oraz „w przypadkach uzasadnionych analizą ryzyka" normodawca przyznaje podmiotowi publicznemu realizującemu zadania publiczne przy użyciu systemów teleinformatycznych władzę dyskrecjonalną w zakresie zamiany standardu podstawowego na standard alternatywny, ograniczając ją jednocześnie dolną i górną granicą nieostrości zastosowanych pojęć prawnych. Granica nieostrości wymaga zaś każdorazowo od podmiotu publicznego ustalenia kryteriów jej określenia przy uwzględnieniu indywidualnych okoliczności danego przypadku. Niekiedy też – określając wymagania technologiczne - jedynie odwołuje się do przepisów lub regulacji normalizującej (standaryzującej) ustanowionych przez krajową lub unijną jednostkę normalizacyjną ewentualnie rekomendacji ustanowionych przez którąś z tych jednostek, a w przypadku ich braku wskazuje jako właściwe przykładowo wymienione standardy międzynarodowe. Jednocześnie zastrzega, że wymagania te muszą być adekwatne do potrzeb wynikających z realizowanych zadań oraz bieżącego stanu technologii informatycznych (zasada adekwatności)[89].

7. Wymagania semantyczne infrastruktury informacyjno-komunikacyjnej państwa

Wymagania semantyczne – ustanowione dla interoperacyjności systemów teleinformatycznych oraz rejestrów publicznych a wyrażające ich zdolność do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów podmiotów publicznych, a więc zapewnienia poprawnej współpracy systemów teleinformatycznych i rejestrów stosowanych przez różne podmioty publiczne –

analysis of risk" the normaliser grants to the public entity, performing public tasks with the use of tele-informative systems, a discretional authority for changing the basic standard into an alternative standard, and limiting it at the same time by the bottom and upper limit of impreciseness of applied legal denominations. The limit of impreciseness demands each time from the public entity the settlement of criteria for its determination with the regard of individual circumstances of a given case. In some cases – at specification of technological requirements – he refers to regulations, or to a normalising (standardising) regulation, established by the national or Union normalising body, or finally to recommendations established by any of these bodies, and in the case of missing them, he indicates some examples of international standards as proper ones. And at the same time he makes a reservation that these requirements have to be adequate to demands resulting with performed tasks and the current state of the art in informative technology (principle of adequacy)[98].

7. Semantic Requirements for State Information-communication Infrastructure

Semantic requirements – established for interoperability of tele-informative systems and public registers, and addressing their capacity for cooperation in favour of mutually beneficial and agreed objectives of public entities, and so to ensure a correct cooperation of tele-informative systems and registers used by different public entities – specify the essence and structure

[96] See § 17 pos. 3 of disposition on NFI.
[97] See § 20 pos. 3 and pos. 4 of disposition on NFI.
[89] Zob. § 16 ust. 1 i ust. 2 rozporządzenia w sprawie KRI.
[98] See § 16 pos. 1 and pos. 2 of disposition on NFI.

określają treść i strukturę danych przetwarzanych i przekazywanych za pośrednictwem systemów teleinformatycznych[99] [znaczenie i funkcje znaków zastosowanych w tych danych (udostępnianych i odczytywanych odpowiednio za pomocą tych systemów)]. Odnoszą się również do formalnego opisu architektury systemu teleinformatycznego (modelu architektury), a ściślej do składników tego systemu oraz powiązań i relacji między tymi składnikami (architektury systemu teleinformatycznego)[100]. Do opisu protokołów i struktur wymiany danych usługi sieciowej wykorzystuje się przy tym – jak wynika z rozporządzenia w sprawie KRI - *Web Services Description Language* (WSDL)[101]; dla struktur danych cech informacyjnych obiektów (osób fizycznych, podmiotów i obiektów przestrzennych) stosuje się schemat XML oraz inne dopuszczone wzory w trakcie tworzenia lub modernizacji rejestrów publicznych; zaś do struktur identyfikatorów obiektów – PESEL, REGON oraz identyfikator punktu adresowego lub działki identyfikacyjnej[102]. Jednocześnie normodawca w rozporządzeniu odsyła do wskazanych w załączniku do rozporządzenia formatów oraz standardów zapewniających dostęp do zasobów informacji (rejestrów, baz danych) udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych; formatów danych obsługiwanych przez podmioty realizujące zadania publiczne w trybie odczytu, w tym rozszerzenia formatu oraz pliku; wreszcie zaś opisu standardu oraz formatu, organizacji określającej format lub standard oraz oznaczenia lub nazwy normy albo dokumentu zawierającego specyfikację techniczną wskazanego formatu udostępnia-

of data processed and transferred by tele-informative systems[104] [denomination and functions of marks used in the data (accessible and readable respectively by these systems)]. They also take a reference to formal description of tele-informative system architecture (model of architecture), and more precisely to components of the system and links and relations between these components (architecture of tele-informative system)[105]. For description of protocols and structures of data exchange in the net services there is used – according to disposition on NFI - *Web Services Description Language* (WSDL)[106]; and for data structures of information features of objects (real persons, entities and spatial objects) the pattern of XML is used and other permitted patterns during creation or upgrades of public registers; and for identificatory structures of the objects – PESEL, REGON, and identifier of the address point or the identificatory field[107]. At the same time the normaliser in the disposition refers to formats and standards indicated in the annex to disposition securing the access to information assets (registers, data bases) shared by tele-informative systems used for execution of public tasks; data formats handled by the entities executing the public tasks in the form of reading, including the extension of the format or file; and finally, description of standard and format, organisation identifying the format or standard, and denominations or names of the norm or document containing technical specification of the indicated format for shared data, and the title of the norm, standard, or normalising or

[99] Por. § 5 ust. 3 w zw. z § 8 ust. 3 w zw. z ust. 2 i w zw. z § 10 ust. 5, ust. 6, ust. 11 i ust. 12 rozporządzenia w sprawie KRI oraz M. Szymczak (red.), Słownik języka polskiego, tom III, Warszawa 1981, s. 195.
[100] Zob. § 2 pkt 7 w zw. z § 2 pkt 1 rozporządzenia w sprawie KRI.
[101] Zob. § 8 ust. 2 rozporządzenia w sprawie KRI.
[102] Zob. § 10 ust. 5 i ust. 6 oraz załącznik nr 1 rozporządzenia w sprawie KRI.

nych danych oraz nazwy normy, standardu lub dokumentu normalizującego albo standaryzującego formatu danych do odczytu[103].

Z woli normodawcy interoperacyjność systemów teleinformatycznych i rejestrów publicznych osiąga się poprzez spełnienie trzech warunków: stosowanie określonych w rozporządzeniu struktur danych i znaczenia danych zawartych w tych strukturach; stosowanie określonych w rozporządzeniu struktur danych i znaczenia danych w tych strukturach publikowanych w repozytorium interoperacyjności; oraz stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

Zakończenie

Normatywne wymagania infrastruktury informacyjno-komunikacyjnej państwa nie zostały, na poziomie aktu normatywnego, zdefiniowane ani jako ogólne pojęcie normatywne, ani jako poszczególne ich rodzaje. Dookreślane są poprzez odwołanie do konkretnych norm technicznych lub przyjmowanego uniwersalnego wzorca, albo poprzez ich opis tekstowy albo wskazanie określonych działań podmiotów publicznych. Z teoretycznego punktu widzenia konstrukcja prawna wymagań normatywnych infrastruktury informacyjno-komunikacyjnej państwa nie budzi większych zastrzeżeń. Ale same wymagania zostały ujęte niekiedy w sposób dość zawoalowany, a cechą je wyróżniającą jest obszerność i złożoność ich unormowania. W praktyce może to jednakże rodzić wiele trud-

standardising document for a format of data to be read out [108].

It is the will of the normaliser that the interoperability of tele-informative systems and public registers is achieved by meeting three conditions: application of data structures and the meaning of data included in these structures specified in the disposition; application of data structures and the meaning of data included in these structures specified in the disposition and published in repositorium of interoperability; and application of references to the registers containing the referential data in the registers kept by the public entities in the extension which is necessary for the execution of tasks.

Summary

Normative requirements for the state information-communication infrastructure were not defined on the level of a normative act in a form of general normative denominations, and nor as their particular types. They are described more precisely by referring to specific technical norms, or to an accepted universal pattern, or by their wording description, or by indication of specific actions of the public entities. Theoretically, the legal structure of normative requirements for the state information-communication infrastructure can be taken without greater reservations. But the alone requirements were sometimes presented with a degree of ambiguity, and the vastitude and complexity of normalisation is their distinguishing feature. It can rise

[104] Compare § 5 pos. 3 in reference to § 8 pos. 3 and pos. 2, and to § 10 pos. 5, pos. 6, pos. 11 and pos. 12 of disposition on NFI, and M. Szymczak (red.), Glossary of Polish language, vol. III, Warsaw 1981, p. 195.
[105] See § 2 pt. 7 with reference to § 2 pt. 1 of disposition on NFI.
[106] See § 8 pos. 2 of disposition on NFI.
[107] See § 10 pos. 5 and pos. 6 and annex nr 1 of disposition on NFI.
[103] Zob. załącznik nr 2 i 3 rozporządzenia w sprawie KRI.
[108] See annex nr 2 and 3 of disposition on NFI.

ności. Tak skonstruowane wymagania nie zostały przyjęte na jednakowym poziomie dla wszystkich elementów infrastruktury. Niekiedy bowiem prawodawca określa je jako minimalne, co pozwala sądzić, że podmioty realizujące zadania publiczne mogą przyjąć bardziej restrykcyjny zestaw warunków niż wymagany prawem. Niekiedy zaś pozostawia tym podmiotom swobodę wyboru alternatywnego warunku dla określonego elementu infrastruktury. A odwołanie do norm i dyrektyw technicznych oraz organizacyjnych, powszechnie uznawanych w obrocie międzynarodowym dla urządzeń technologicznych i ich oprogramowania, stanowi gwarancję, że normatywne warunki są wystarczające dla zapewnienia bezpieczeństwa infrastruktury i przesyłanych za jej pośrednictwem informacji publicznych. Te uwzględniają bowiem rozwój technologiczny i – aktualne do najnowszej wiedzy i rozwoju technologii informacyjno-komunikacyjnej (ICT) - warunki bezpieczeństwa. Ich kształtowanie w drodze aktu wykonawczego do ustawy stwarza zaś swoistą „furtką szybkiego reagowania" na zmiany technologiczne i nowe zagrożenia. Niemalże wraz z nowymi systemami zabezpieczającymi infrastrukturę i narzędziami zabezpieczenia pojawiają się narzędzia informatyczne umożliwiające zdalną nielegalną ingerencję w elementy infrastruktury informacyjno-komunikacyjnej państwa. Nawet bowiem najdoskonalsza i najbardziej przewidywalna regulacja prawna, ale i najszybsza ścieżka legislacyjna nie są w stanie zagwarantować całkowitej nienaruszalności infrastruktury. Pozostaje ona zawsze o krok za tak szybkim i burzliwym postępem technologicznym oraz niezwykle wyrafinowaną działalnością podmiotów trzecich.

Biorąc pod uwagę obecną treść rodzimej regulacji wymagań systemów teleinformatycznych, postulować można jedynie zwięk-

some difficulties in practice. The requirements designed in this way were not accepted on the same level for all components of infrastructure. And sometimes the legislator identifies them as the minimal ones, suggesting that the entities performing the public tasks can accept a more restrictive catalogue of conditions than demanded by the law. And sometimes he leaves to these entities the freedom of choice of an alternative condition for a specific component of infrastructure. Thus, the reference to norms and technical and organisational directives commonly accepted in the international trade of hardware and its software is a warrant that the normative conditions are sufficient to assure the safety of infrastructure and public information transferred with its use. They, namely, regard technological development and conditions of safety representing current state of the art in information-communication technologies (ICT). Shaping them by an executive order to an Act creates a unique "roadmap of rapid reaction" to technological changes and new threats. It is that the informative tools enabling illegal remote interference into the state information-communication infrastructure components appear almost concurrently with the new systems and tools safeguarding the infrastructure. It is so, because even a perfect and a most predictable legal regulation, and also the quickest legislative way, cannot warrant a complete inviolability of the infrastructure. It has been staying for ever a step behind the rapid and stormy technological progress and unusually perfidious actions of the third bodies.

Considering the present content of the national regulations on the requirements for tele-informative systems, it can be pos-

szenie bezpieczeństwa zasobów informacyjnych państwa poprzez ustanowienie prawnego wymogu ich generowania i dystrybuowania za pośrednictwem specjalnie dla nich zbudowanej i tylko im dedykowanej sieci teleinformatycznej. Pod rozwagę ewentualnie można poddać wprowadzenie – poza wymaganiami określonymi w normach standaryzujących – dodatkowego i obligatoryjnego zabezpieczenia tej sieci oraz zaostrzenie wymogów dostępu do sieci i jej zasobów informacyjnych. Zmienność otoczenia zewnętrznego i wewnętrznego państwa uzasadnia też zwiększenie aktywności i działań państwa w obszarze bezpieczeństwa informacyjnego państwa, ustawicznego monitorowania zachodzących zmian otoczenia, standardów i procedur bezpieczeństwa oraz zagrożeń dla bezpieczeństwa informacyjnego państwa, ich dostosowywania do zmieniającej się rzeczywistości, w tym nowych pojawiających się zagrożeń czy niespotykanych dotąd metod nielegalnych działań (ataków) w sferę informacyjną państwa. Zalecić można nadto zwiększenie ostrożności i czujności użytkowników infrastruktury, ich częstsze szkolenie. Ci bowiem - z uwagi na ludzką naturę: ułomności i słabości, a niekiedy brak dostatecznej wiedzy, świadomości czy ostrożności – są najsłabszym elementem systemu ochrony i zapewnienia bezpieczeństwa infrastrukturze i informacjom.

tulated that the safety of the state information assets has to be increased by the establishment of a legal obligation for their generation and distribution via a teleinformative net which is constructed and dedicated specially to them. Optionally, it can be considered to introduce – beside the requirements specified in the standardising norms – an additional and obligatory safeguard of the net and to tighten up the restrictions preventing access to the net and its information assets. Changeability of state's outer and inner environment justifies also the increase of state activity and actions over the area of state information safety, and permanent monitoring of changes in the environment, and standards and procedures of state information safety, and their adaptation to changeable reality, including newly appearing threats, or earlier unspotted methods of illegal actions (attacks) in the state information domain. Moreover, it can be recommended to increase the care and vigilance of the infrastructure users, and the rate of training. Namely, they are weakest components of the system for protection and assurance of safety to the infrastructure and the information due to the human nature, i.e. its disabilities and weaknesses, and sometimes the lack of sufficient knowledge, awareness, or caution.

Literatura / *Literature*

[1] Aleksandrowicz T., Bezpieczeństwo informacyjne państwa, Studia Politologiczne 2018, z. 49

[2] K. Bobkowski, Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji, Zarządzanie i Finanse Journal of Management and Finance Vol. 16, No. 3/2/2018

[3] T. Filipowicz, Zasada równego traktowania wykonawców w zamówieniach publicznych dotyczących technologii informatycznych, LEX 2015

[4] I. J. Jóźwiak, A. Szleszyński, Specyfikacja wymagań dla bezpieczeństwa informacji przechowywanej i przetwarzanej w systemie operacyjnym serwera, PAK tom 57, nr 9/2011

[5] W. Kitler, Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe

i definicyjne [w:] W. Kitler (red.), J. Taczkowska-Olszewska, (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017

[6] J. Krawiec, System zarządzania bezpieczeństwem informacji – zabezpieczenia, Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie 2017 t. 15, z. 1(38)

[7] W. Lang, J. Wróblewski, S. Zawadzki, Teoria państwa i prawa, Warszawa 1986

[8] A. Monarcha-Matlak, Obowiązki administracji w komunikacji elektronicznej, Oficyna 2008, Lex z 2022

[9] J. Oleński, Standardy informacyjne w e-administracji [w:] Z. Olejniczak, J.S. Nowak, J.K. Grabara, Systemy informatyczne w administracji, Warszawa 2004

[10] G. Szpor, K. Wojsyk, Tryb określenia minimalnych wymagań [w:] Cz. Martysz, G. Szpor, K. Wojsyk, Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz, Wydanie II, Lex 2015

[11] M. Szymczak (red.), Słownik języka polskiego, tom III, Warszawa 1981

[12] K. Świtała, Prawnoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych, PPP 2013/10/21-30, Lex 2022

[13] J. Taczkowska-Olszewska, Bezpieczeństwo informacyjne jako kategoria prawna, [w:] W. Kitler (red.), J. Taczkowska-Olszewska, (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017

[14] H. Tańska, A. Władzińska, Zróżnicowane aspekty bezpieczeństwa wytwarzanych systemów informatycznych, Rocznik KAE 2019, z. 40

[15] P. Zaskórski, K. Szwarc, Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki 2013 nr 9, rok 7

Akty normatywne

[1] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j.: Dz. U. z 2023 r. poz. 57

[2] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, t.j. Dz. U. z 2017 r. poz. 2247

[3] ISO/IEC 20000-1:2011 - International Standard - Information Technology - Service Management - Part 1: Service management system requirements

[4] ISO/IEC 20000-2:2005 - International Standard - Information Technology - Service Management - Part 2: Code of practice

[5] PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania

[6] PN-ISO/IEC 27002:2017-06/Ap1 Technika informatyczna Techniki bezpieczeństwa Praktyczne zasady zabezpieczania informacji

[7] PN-ISO/IEC 27005:2011 Zarządzanie Ryzykiem w Systemach Bezpieczeństwa Informacji

[8] PN-ISO/IEC 20000-1:2007 Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja

[9] PN-ISO/IEC 20000-2:2007 Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania

[10] PN-EN ISO/IEC 27001 System zarządzania bezpieczeństwem informacji