E-ISSN 2544-9567
ISSN 1230-3801

Zeszyt 164 nr 2/2023, str.83-109
Volume 164 No. 2/2023, pp. 83 -109

STANDARD BEZPIECZEŃSTWA INFRASTRUKTURY INFORMACYJNO-KOMUNIKACYJNEJ PAŃSTWA W PRAWIE KRAJOWYM

SECURITY STANDARD OF THE STATE INFORMATION AND COMMUNICATION INFRASTRUCTURE IN NATIONAL LAW

Ewa CISOWSKA-SAKRAJDA ORCID: 0000-0001-8383-6951
Wojewódzki Sąd Administracyjny w Łodzi, Polska
Provincial Administrative Court in Lodz, Poland

DOI 10.5604/01.3001.0053.7234

Streszczenie: Artykuł przedstawia normatywny standard bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa oraz znaczenie bezpieczeństwa tej infrastruktury dla bezpieczeństwa informacyjnego państwa. Zasadnicze jego rozważania koncentrują się wokół pojęcia „standard bezpieczeństwa" tej infrastruktury oraz jego komponentów składowych, jak: normatywne wymagania bezpieczeństwa infrastruktury, zasady określania wymogów stosowanych dla infrastruktury i jej interoperacyjności oraz zasady tworzenia, modernizacji oraz użytkowania infrastruktury informacyjno-komunikacyjnej.

Słowa kluczowe: prawo administracyjne, standard bezpieczeństwa infrastruktury informacyjno-komunikacyjnej, zasady i wymagania infrastruktury informacyjno-komunikacyjnej

Abstract: The article presents the normative standard of security of information and communication infrastructure and the importance of security of this infrastructure for the information security of the state. Its main considerations focuses on the concept of the "safety standard" of this infrastructure and its components, such as normative requirements for infrastructure security, rules for determining requirements applicable to infrastructure and its interoperability, and principles for the creation, modernization and use of information and communication infrastructure.

Keywords: administrative law, information and communication infrastructure security standard, information and communication infrastructure rules and requirements

1. Wprowadzenie

Problematyka bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa jest – jak dowiodła dokonana w innym opracowaniu analiza rodzimej regulacji prawnej oraz poglądów rodzimej nauki[1] - niezwykle złożona

1. Introduction

Problems concerning the safety of state information-communication infrastructure are highly complex and multi directional as it was proved by an analysis performed in other publication for national legal regula-

[1] Szerzej na ten temat zob. E. Cisowska-Sakrajda, Prawne aspekty bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa, Problemy Techniki Uzbrojenia 2022 zeszyt 162, nr 4, s. 92 i n.

i wielowątkowa. W efekcie nie nadaje się ona do prostej analizy. Ta okoliczność ma dwie konsekwencje. Z jednej strony, uprawnia skoncentrowanie obecnych rozważań jedynie wokół rekonstrukcji normatywnego standardu bezpieczeństwa tej infrastruktury, jednakże bez charakteryzowania poszczególnych jego elementów. Te – z uwagi na obszerność, niekiedy zaś kazuistyczność, a niekiedy blankietowość regulacji prawnej - zasługują na rozważenie w odrębnej dysertacji. Z drugiej zaś strony, uzasadnia podkreślenie trudności w identyfikacji problematyki bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa, które ujawniają się już na poziomie terminologicznym i definicyjnym. Ich ewidentnym wyrazem są prezentowane w doktrynie różnorakie poglądy oraz rozproszona i w znacznej mierze blankietowa (odsyłająca) regulacja prawna. W celu wprowadzenia w tytułową problematykę konieczne, a zarazem wystarczające, jest stwierdzenie, że infrastruktura informacyjno-komunikacyjna państwa, w ujęciu doktrynalnym, pomijając zasygnalizowane rozbieżności, może być rozumiana jako złożony i skomplikowany układ połączonych (i współpracujących) różnorakich technologicznych elementów o różnej funkcjonalności i użyteczności, umożliwiających gromadzenie, przetwarzanie, przechowywanie i przekazywanie danych (informacji) w postaci elektronicznej oraz komunikowanie na odległość[2]. Infrastruktura ta stanowi niewątpliwie – i to niezależnie od sposobu jej określania i pojmowania - istotny obszar bezpieczeństwa informacyjnego (sfery informacyjnej) współczesnego państwa. Uznawana za techniczo-organizacyjną stronę kooperacji

tions, and opinions of scientists[14]. In effect, it cannot be subjected to a simple analysis. This fact has two consequences. Firstly, it substantiates the focusing of present considerations exclusively around a normative reconstruction of security standard for this infrastructure, but without characterisation of its particular components. They deserve to be considered in a separate elaboration due to the extensiveness, and sometimes the casuistry, and even the formalism of a legal regulation. Secondly, it justifies the stressing of difficulties over the identification of questions of the state information-communication infrastructure security appearing just on the level of terminology and definitions. Different opinions presented in the doctrine and the scattered, and in a great degree the formalistic (referential) legal regulation, is a clear evidence of them. But, as an introduction to the questions of the title it is necessary, and at the same sufficient, to state that the state information-communication infrastructure, in doctrinal aspect and leaving apart the signalled divergencies, may be understood as a system of combined and complex (and working together) different technological components with various functionalities and usability providing the acquisition, processing, storing, and transfer of data (information) in the electronic form, and the distant communication[15]. The infrastructure is undoubtedly an essential domain of information security (information domain) of the modern state, independently on the way it is identified and understood.

[2] W szerszym ujęciu pojęcie infrastruktura informacyjno-komunikacyjna – wedle normatywnej terminologii systemu teleinformatycznego, oznacza „systemy transmisyjne, które po pierwsze, służą do przetwarzania informacji w postaci elektronicznej (cyfrowej) z wykorzystaniem sprzętu i oprogramowania komputerowego; po drugie, umożliwiają telekomunikację, tj. przekazywanie (nadawanie, odbiór lub transmisję) informacji w postaci elektronicznej; po trzecie, są oparte na infrastrukturze łączności (telekomunikacyjnej); po czwarte, przekazują informacje przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego”. Zob. szerzej E. Cisowska-Sakrajda, Prawne aspekty bezpieczeństwa …, s. 110 – 118.

między różnymi podmiotami w państwie w doktrynie bezpieczeństwa państwa[3] postrzegana jest jako jedno z dwu - obok pozytywnej i negatywnej kooperacji między nimi – oblicz sfery informacyjnej państwa. Kluczową i wiodącą kategorią bezpieczeństwa informacyjnego państwa i jednocześnie obiektem najszerszej ochrony prawnej oraz zainteresowania społecznego i rodzimej nauki jest informacja. Niemniej wykorzystywanie na szeroką skalę nowych technologii informacyjno-komunikacyjnych (ang. *information and communications technology*, ICT) we wszystkich obszarach działania państwa i jego organów do gromadzenia, przetwarzania, przechowywania i przesyłania przez nie trudnej do oszacowania ilości danych o różnym charakterze i ciężarze gatunkowym czyni tę warstwę bezpieczeństwa informacyjnego państwa niezwykle ważną dla bytu państwa. Ale, co warte podkreślenia, także niezmiernie atrakcyjną dla podmiotów trzecich względem państwa, u których może zrodzić się pokusa nieuprawnionego do niej dostępu.

Od sprawnego funkcjonowania infrastruktury informacyjno-komunikacyjnej, która określana jest też jako techniczna warstwa bezpieczeństwa informacyjnego państwa, zależy bezpieczeństwo narodowe państwa, a „jej złamanie może spowodować katastrofę, której rozmiar jest z każdym rokiem coraz większy. Groźbę takiego rozwoju wydarzeń stwarzają zarówno skomplikowany charakter powiązań

It is recognised in the state security doctrine[16] as a technical-organisational sphere of cooperation between different subjects in the state and is perceived as one of two – beside the positive and negative cooperation between them – faces of the state information domain. The information is a key and leading category of state information security, and at the same time an object of the widest legal protection and of social and national science interest. Nevertheless, the wide employment of new information and communication technologies (ICT) in all domains of activities of the state and its institutions for acquisition, processing, storing and transfer of data by them in volumes which cannot be easy estimated, and with different character and meaning, makes this layer of state information security to be crucially important for the state existence. But, it is also worth to stress, it is attractive for state's third parties which can tempt to get an unauthorised access to it.

The state's national security depends on the efficient functionality of information-communication infrastructure, which is also described as a technical layer of state information security, and "any breaking of it may trigger a disaster in extension increasing by each year. The threat of such events is created both by a complex character of functional links and internal couplings of

[14] Wider on the subject see E. Cisowska-Sakrajda, Legal Aspects of State Information-communication Infrastructure Security, Issues of Armament Technology, 2022, vol. 162, nr 4, p. 92 and next.
[15] In a wider aspect the notion of information-communication infrastructure – according with the normative terminology of tele-informative system means „transmission systems which firstly, are used for the processing of information in the electronic form (digital) using computer's hardware and software; and secondly, provide telecommunication, i.e. transfer (transmission, reception or transmission) of information in the electronic form; and thirdly, are based on the communication infrastructure (tele-communication); and fourthly, transfer the information via a telecommunication system by means of a terminal device which is suitable for the given system". Wider see E. Cisowska-Sakrajda, Legal Aspects … of Security …, p. 110 – 118.
[3] Tak W. Kitler, Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe, Toruń 2018, s. 328 i n., a zwłaszcza s. 460.
[16] W. Kitler, Organisation of the National Security of the Republic of Poland. Aspects of Government System, and Legal-administrative, and Systematic, Toruń 2018, p. 328 and n., especially p. 460.

funkcjonalnych i sprzężeń wewnętrznych infrastruktury informacyjnej państwa, jak i lawinowy rozwój teleinformatyki. (…) załamanie infrastruktury informacyjnej (w tym infrastruktury teleinformatycznej) państwa doprowadziłoby do dezorganizacji funkcjonowania państwa i zagrożenia jego interesów na świecie"[4]. To ostatnie powoduje groźbę zakłócenia w przekazywaniu w odpowiednim czasie odpowiedniej treści informacji, koniecznej dla podjęcia określonych działań w danym momencie, kiedy brak komunikacji i przekazania informacji może skutkować zagrożeniem działania państwa w pewnych – zwłaszcza – kluczowych dla niego obszarach, czy też uniemożliwić przeciwdziałanie szkodom dla interesów państwa lub jego prawidłowego funkcjonowania. Uzyskana nielegalnie informacja może zaś zostać potencjalnie użyta do destabilizowania sytuacji wewnętrznej w państwie, a nawet stanowić swoistą formę nacisku na państwo na arenie międzynarodowej czy jego ośmieszenia.

Wobec tego troską współczesnych państw jest nie tylko ochrona samych informacji, uznawanych od zarania dziejów ludzkości za najcenniejsze i najbardziej pożądane dobro konsumpcyjne (przedmiot obrotu towarowego)[5], ale i infrastruktury informacyjno-komunikacyjnej, wykorzystywanej do generowania i transmisji tych informacji, a pełniącej drugorzędną (służebną) wobec nich rolę. Oczywistym jest bowiem, że zapewnienie bezpieczeństwa łącznie w dwu tych obszarach jest warunkiem *sine qua non* bezpieczeństwa informacyjnego państwa – zwłaszcza w kontekście trwa-

the state information infrastructure and by an extremely rapid development of teleinformatics. (…) the collapse of information infrastructure (including teleinformatic infrastructure) could disorganise the functionality of state and threaten its interests in the world"[17]. This last one is a threat of disturbances in transferring the relevant information messages at a suitable time needed for starting the specific actions at a given time, and the lack of communication and transfer of information may threaten the functionality of state in certain, especially crucial domains, or prevent the counteractions against harming the interests of state or its proper functioning. Moreover, illegally acquired information may be potentially used to destabilise the state internal situation, and even to become a specific form of pressure to the state in the international arena, or even to ridicule it.

Regarding the above, the contemporary states not only take care to protect the alone information, which is recognised as the most precious and demanded article of consumption since the beginning of humanity (subject of goods trading)[18], but also the information-communication infrastructure, which is used to generation and transmission of this information, and has a secondary (servicing) meaning in relation to it. It is obvious that provision of security in this two domains is a *sine qua non* condition to state information security, especially in the context of the information warfare waged

[4] A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013, s. 453/454 i powołana tam literatura.

[5] Szerzej na temat znaczenia informacji zob. J. Wyporska-Frankiewicz, E. Cisowska-Sakrajda, Dostęp do informacji publicznej a bezpieczeństwo państwa, Wiedza Obronna 2022, vol. 278 nr 1, s. 114 i n.

[17] A. Żebrowski, Poland's Information Security and Information Warfare, Annuals of the Economic Studies Board nr 29/2013, p. 453/454 and the literature.

[18] Wider about the meaning of information see J. Wyporska-Frankiewicz, E. Cisowska-Sakrajda, Access to Public Information and the State Security, Defence News 2022, vol. 278 nr 1, p. 114 and n.

jącej nieustannie na arenie międzynarodowej, za sprawą rozwoju technologii ICT, wojny informacyjnej, której najbardziej widocznym medialnie efektem jest dezinformacja, manipulacja informacją o działalności państwa i jego organów. Nie zawsze więc cel ataku przeciwko bezpieczeństwu informacyjnemu państwa stanowi sama informacja (bazy, rejestry danych) - jej pozyskanie lub zniekształcenie. Coraz częściej celem tym staje się wyłącznie infrastruktura techniczna. Ta ostatnia wymaga zatem – analogiczne jak same dane (informacje) – wprowadzenia, już na poziomie prawnym, odpowiednich mechanizmów ochronnych. Mechanizmy te jednak – zważywszy na „techniczną" naturę i charakter tego obszaru bezpieczeństwa informacyjnego państwa – są zgoła odmienne niż w przypadku informacji. Pierwszorzędne znaczenie w tym zakresie ma, będący przedmiotem dalszych rozważań, standard jej bezpieczeństwa, na który składają się normatywne wymagania i zasady tworzenia, modernizacji i używania infrastruktury informacyjno-komunikacyjnej. Niezmiernie istotnym przy tym jest to, aby standard ten stanowił z jednej strony pierwszą barierę dla nieuprawnionego dostępu do infrastruktury i danych, z drugiej zaś aby umożliwiał on organom państwa różnego szczebla i o różnym statusie na bezkolizyjną i szybką wymianę danych i komunikację.

Tak zakreślony obszar badawczy uzasadnia przede wszystkim analizę rodzimej regulacji prawnej w kontekście elementów standardu bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa. Wymaga to rozważenia wpływu rozproszonej, a niekiedy blankietowej (odsyłającej) regulacji na kształt tego standardu. Konieczne jest też ustalenie sposobu rozumienia pojęcia standard w odniesieniu do bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa, a następnie określenie gwarantowanego tym stan-

permanently on the international arena due to development of ICT, and its most visible effects in the media include disinformation and manipulation with information about the activities of state and its institutions. The alone information is not always targeted at the attacks against the state information security (data bases, registers) by its acquisition or deformation. It is most often that technical infrastructure is exclusively targeted. This last one requires then, identically as the data alone (information), the implementation of relevant protective mechanisms already on the legal level. But these mechanisms, regarding "the technical" character and nature of this domain of state information security, are completely different than in the case of information. The standard of its security, discussed later, has a key meaning in respect to this, and it contains the normative requirements and principles of building, upgrading, and using the information-communication infrastructure. And it is of high importance at the same time that the standard, from one side, is a first barrier for unauthorised access to infrastructure and data, and on the other side, provides a rapid and undisturbed communication and exchange of data for state institutions of different level and status.

The researching area outlined in such way justifies most of all the analysis of national legal regulations in the context of components of the standard for the state information-communication infrastructure security. It requires a consideration of an influence of dispersed, and sometimes formalistic (referential), regulation into the form of this standard. Moreover, it is necessary to establish the understanding of notion of the standard, regarding the state information-communication infrastructure security, and next to define a level of data (information)

dardem poziomu ochrony danych (informacji). Interesującym jest wreszcie skonstruowanie jego elementów składowych (katalogu wymagań) oraz wskazanie ich charakteru.

2. Regulacja prawna standardu bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa

Rodzime rozwiązania normatywne w zakresie standardu bezpieczeństwa infrastruktury informacyjno-komunikacyjnej (wedle ustawowej nomenklatury systemów teleinformatycznych) charakteryzują się – jak dowodzi ich analiza - daleko idącą specyfiką. Jest to podyktowane samą naturą rozwiązań technologicznych stosowanych do gromadzenia, przechowywania, przetwarzania i przekazywania danych za pośrednictwem tej infrastruktury. Z tego względu standard jej bezpieczeństwa, a ściślej składające się nań reguły i zasady, rodzimy prawodawca reguluje dwupoziomowo: na poziomie ustawowym oraz na poziomie aktu podustawowego, a w gruncie rzeczy w znacznym zakresie poprzez odesłanie do wskazanych w tym ostatnim norm technicznych – normalizujących (standaryzujących), które uznaje za obowiązujące przy tworzeniu i eksploatacji systemów teleinformatycznych.

Na poziomie ustawowym w fundamentalnej w tym zakresie ustawie o informatyzacji podmiotów publicznych[6] prawodawca określa:

1) zasady, które należy uwzględniać przy ustalaniu wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i ustalaniu Krajowych Ram Interoperacyjności (KRI), a także przy dostosowaniu już funkcjonu-

protection warranted by this standard. Finally, it is worth to build a system of its components (catalogue of requirements) and to indicate their character.

2. Legal Regulation of State Information-communication Infrastructure Security Standard

National normative solutions for standards of the information-communication infrastructure security (according with the statutory nomenclature of tele-informative systems) are characterised – as their analyses prove – by large specificity. It is dictated by the own nature of technological solutions used for acquisition, storing, processing and transferring of data by means of this infrastructure. For this reason the standard of its security, or more precisely the rules and principles it consists of, is regulated by the national legislator on two levels: on the statutory level and on the level of substatutory act, and in reality by referring in great degree to technical standards indicated in the last one which are regarded as binding at the building and using of tele-informative systems.

On the statutory level, in the fundamental act about the informatisation of public subjects[19] the legislator defines:

1) The principles which have to be taken into account at preparation of specifications for tele-informative systems used for execution of public assignments, and at establishing the Country Interoperability Frames (CIF), and also at adaptation of already functioning systems to the requirements

[6] Zob. art. 1 pkt 2 i pkt 3 oraz art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j.: Dz. U. z 2023 r. poz. 57, zwanej ustawą o informatyzacji podmiotów publicznych.

[19] See art. 1 point 2 and point 3, and art. 18 of the Act from 17 February, 2005 on informatisation of activities of the subjects performing the public assignments, i.e.: Law Monitor from 2023, pos. 57, named as the law on informatisation of public subjects.

jących systemów do wymagań dla nich ustanowionych i KRI;
2) definicje kluczowych dla budowy systemów teleinformatycznych pojęć, jak przykładowo: „minimalne wymagania dla systemów teleinformatycznych", „interoperacyjność" czy „Krajowe Ramy Interoperacyjności";
3) delegację ustawową dla Rady Ministrów do określenia minimalnych wymagań dla systemów teleinformatycznych i rejestrów publicznych;
4) obowiązki podmiotów publicznych w zakresie zapewnienia bezpieczeństwa systemów teleinformatycznych.

Natomiast warunki ochrony użytkowników usług, warunki przetwarzania danych w telekomunikacji, wymagania urządzeń radiowych, interoperacyjności usług cyfrowych transmisji radiofonicznych, bezpieczeństwa i integralności sieci i usług telekomunikacyjnych, minimalne szczegółowe środki techniczne i organizacyjne oraz metody zapobiegania zagrożeniom, wymagania techniczne i eksploatacyjne dla interfejsów umożliwiających wykonywanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego wskazuje w ustawie prawo telekomunikacyjne[7]. Na poziomie rozporządzenia w sprawie Krajowych Ram Interoperacyjności[8] normuje w szczególności wymagania techniczne (normalizujące/standaryzujące) dla systemów teleinformatycznych (infrastruktury informacyj-

which are established for them and to the CIF;
2) Definitions of following notions, having a key meaning for building of teleinformative systems, as for instance "interoperability", or "the Country Interoperability Frames";
3) A statutory delegation for the Board of Ministers for identification of minimal requirements for tele-informative systems and public registers;
4) Obligations of public subjects in provision of security for tele-informative systems.

And next, the legislator indicates in the Act on telecommunication law[20] the conditions for protection of users of services, conditions for data processing in telecommunication, requirements for radio equipment, interoperability of digital services for radiophonic transmissions, security and integrity of telecommunication networks and services, minimal detailed technical and organisational means and threat preventive methods, technical and operational requirements for interfaces enabling the performance of assignments and obligations in favour of defence and state security, and public order and security. It normalises on the level of a disposition the question of the Country Interoperability Frames[21] regarding especially technical requirements (normalising/ standardising) for teleinformative systems (information-com-

[7] Zob. np. art. 1 ust. 1 pkt 7, pkt 11, art. 132, art. 175, art. 175d, art. 176a, art. 179 czy art. 182 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t.j.: Dz. U. z 2022 r. poz. 1648, zwanej prawem telekomunikacyjnym.
[8] Zob. np. § 1, § 3 - § 5, rozdział III czy rozdział IV rozporządzenia 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 KRI.
[20] See for instance art. 1 pos. 1 point 7, point 11, art. 132, art. 175, art. 175d, art. 176a, art. 179 or art. 182 of the Act from 16 July, 2004, Telecommunication Law, i.e.: Law Monitor from 2022, pos. 1648, named as telecommunication law.
[21] See for instance § 1, § 3 - § 5, chapter III or chapter IV of disposition of the Board of Ministers from 12 April, 2012 on Country Interoperability Frames, minimal requirements for the 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 on Country Interoperability Frames, or disposition of CIF.

no-komunikacyjnej) - w tym zwłaszcza architektury tego systemu i jej modelu, kompatybilności, a także standardy, normy i procedury dla podmiotów realizujących zadania publiczne oraz reguły „użyteczności" systemu.

Taki zabieg – dwutorowości określenia warunków dla systemów teleinformatycznych oraz ich interoperacyjności i odesłania do norm technicznych (normalizujących) zdają się uzasadniać dwa zasadnicze czynniki: po pierwsze, właściwości rynku nowych technologii i samych technologii, które – w związku z dynamicznym rozwojem technologii i postępem cywilizacyjnym - dość szybko dezaktualizują się („starzeją") i są w efekcie zastępowane nowocześniejszymi, sprawniejszymi i bardziej funkcjonalnymi technologicznymi rozwiązaniami; a po drugie, także dość czasochłonny i wymagający niejednokrotnie konsultacji proces legislacyjny nad projektem ustawy oraz szybka ścieżka legislacyjna w przypadku przyjmowania rozporządzeń. To ostatnie jest wszak prawną formą działania władzy legislacyjnej, które z założenia umożliwia niemalże natychmiastowe reagowanie na zachodzące zmiany technologiczne, które to zmiany nie pozostają bez znaczenia dla funkcjonowania stosowanych do realizacji zadań publicznych systemów teleinformatycznych (infrastruktury informatyczno-komunikacyjnej). Podzielić więc należy prezentowany w doktrynie prawa administracyjnego pogląd, że „w przypadku regulowania prawem rozwiązań technicznych należy uwzględniać możliwość zmiany tych rozwiązań technicznych bez potrzeby ciągłego uruchamiania długotrwałych procesów legislacyjnych, szczególnie że zmiana technologii na nowocześniejszą i tańszą nie narusza niczyich praw"[9]. A zatem

munication infrastructure) – including especially the architecture of the system and its model, compatibility, and the standards, norms, and procedures for subjects performing the public assignments and the rules of system's "usability".

Such approach – bidirectional determination of conditions for the tele-informative systems and for their interoperability and the reference to technical standards (normalising) seems to be justified by two basic factors: at first, the nature of the market of new technologies, and the technologies alone which relatively rapidly become obsolete ("out-aged") due to a dynamical progress on technologies and civilisation, and are replaced in effect of it by more modern, efficient and functional technological solutions; and on the second by the legislative process on the bills which is relatively time consuming and often requires the consultancies, and the rapid legislation path in the case of accepting the dispositions. The last one is anyway a legal form of proceeding for legislative authorities enabling, by the assumption, almost immediate reaction to technological changes which are not meaningless for the functionality of tele-informative systems used for execution of public assignments (information-communication infrastructure). Then, an opinion presented in the doctrine of administrative law can be shared that „in the case when the law regulates technical solutions, a possibility has to be given for changing these technical solutions without a need for permanent activation of long-term legislative processes, especially as the change of technology into the newer and cheaper does not violate the rights of anybody"[22]. Therefore, in all cases where the application of

[9] Tak 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.

wszędzie tam, gdzie do wykonywania prawa konieczne jest zastosowanie techniki, a zwłaszcza tak szybko zmieniającej się, jak technologia teleinformatyczna i telekomunikacyjna, niezbędne jest wręcz uwzględnienie przez prawodawcę specyfiki postępu technologicznego i praw rządzących tym postępem i tą technologią[10]. Następuje to poprzez odwołanie się do reguł – norm i standardów stosowanych w rozwiązaniach technologicznych, a w razie ich braku do standardów uznawanych przez organizacje międzynarodowe czy rekomendacji tych organizacji. Wielokrotnie wymagania te określa także producent danego nośnika informacji, pakietu oprogramowania narzędziowego, użytkowego, pakietu programów, języka oprogramowania, który ma wystarczająco silną pozycję na rynku rozwiązań techniki i technologii, a jednocześnie na szeroką skalę prowadzi kampanię informacyjną, marketingową i szkoleniową produktu, udostępniając go bezpłatnie lub po promocyjnych cenach[11].

Tworzone w ten sposób normy techniczne stanowią – co powszechnie wiadome - dorobek społeczności międzynarodowych. Są one rozpowszechniane w postaci konkretnych technicznych rekomendacji i norm technicznych – zamieszczanych na stronach internetowych międzynarodowych i krajowych organizacji normalizujących. A co więcej dyrektywy techniczne i normy techniczne[12] mają – co zrozumiałe zważywszy na

technology is needed for the execution of law, and especially the technology which changes so rapidly as tele-informative and telecommunication ones, it is simply necessary to respect by the legislator the specificity of technological development and rules governing this development and the technology[23]. It is done by the reference to rules – norms and standards used in technological solutions, and in the case when they are missing, to the standards acknowledged by international organisations, or recommended by these organisations. In many times, these requirements are specified by the manufacturer of a given carrier of information, packet of instrumental and user's software, package of software, or programming language having a sufficiently strong position in the market of technical and technological solutions, and at the same time involved in a large scale in campaigning the product by releasing information, marketing data, and training over the product by making it accessible free of charge, or at promoting prices[24].

It is commonly known that technical standards created in such way is an output of international societies. They are spread in the form of specific technical recommendations and technical standards – placed in the internet sites of international and national normalising institutions. Moreover, technical directives and technical standards[25] have the key meaning among the all spec-

[22] G. Szpor, K. Wojsyk, Procedure for Determination of Minimal Requirements [in:] Cz. Martysz, G. Szpor, K. Wojsyk, The Act on informatisation of activities of the subjects performing the public assignments. Comments, Edition II, Lex 2015.
[10] Tak też G. Szpor, K. Wojsyk, op. cit., wersja z Lex.
[11] Szerzej zob. J. Oleński, Standardy informacyjne w e-administracji [w:] Z. Olejniczak, J.S. Nowak, J.K. Grabara, Systemy informatyczne w administracji, Warszawa 2004, s. 31/32.
[12] Szerzej na temat dyrektyw i norm technicznych zob. np. W. Lang, J. Wróblewski, S. Zawadzki, Teoria państwa i prawa, Warszawa 1986, s. 321 -324.
[23] Also G. Szpor, K. Wojsyk, op. cit., version from Lex.
[24] Wider see J. Oleński, Information Standards in E-administration [in:] Z. Olejniczak, J.S. Nowak, J.K. Grabara, Informatic Systems in Administration, Warsaw, 2004, p. 31/32.
[25] Wider about directives and technical norms see for instance W. Lang, J. Wróblewski, S. Zawadzki, Theory of State and Law, Warszawa 1986, p. 321 -324.

technologiczną naturę infrastruktury - najistotniejsze znaczenie wśród całego spektrum różnorakich wymagań. Te pierwsze, określane jako dyrektywy celowego działania formułowane w oparciu o prawa przyrody, są przy tym w szczególności wskazówkami racjonalnego (efektywnego) posługiwania się różnego typu urządzeniami technicznymi i zawierają przeważnie wzorce techniczne przedmiotów lub stanów rzeczy stanowiących wskazane w dyrektywach cele działalności technicznej. Te drugie, stanowione w oparciu o dyrektywy techniczne i wzorce techniczne, regulują postępowanie adresata w procesie jego oddziaływania na przedmioty przyrody. Wobec tego skutkiem nieprzestrzegania normy technicznej, nawet jeśli nie jest ona zabezpieczona żadną sankcją społeczną, jest niekorzystny rezultat praktycznej działalności, nieosiągnięcie zamierzonego celu lub osiągnięcie go na drodze niepotrzebnie dużych nakładów[13].

Z tak ukształtowanej regulacji prawnej wymagań bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa wyłania się ogólny zamysł prawodawcy zapewnienia z jednej strony spójności działania systemów teleinformatycznych używanych do realizacji zadań publicznych oraz rejestrów publicznych i wymiany informacji publicznej w postaci elektronicznej z podmiotami publicznymi, z drugiej zaś strony zapewnienia sprawnej i bezpiecznej wymiany informacji w postaci elektronicznej między podmiotami publicznymi, także innych państw lub organizacji międzynarodowych. Realizacji tego zamysłu służy przyjęty normatywny standard bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa używanej przez podmioty realizujące zadania publiczne.

trum of various requirements what is understandable considering technological nature of the whole infrastructure. The first ones are described as the directives of objective activity and are formulated on the base of the laws of nature, and they are specific recommendations for a reasonable (efficient) use of different types of technical equipment, and they mostly contain technical patterns of objects or states of matters constituting the objectives of technical activities indicated in the directives. The second ones, constituted on the base of technical directives and technical patterns, regulate the actions of an addressee in the process of his interaction with the objects of nature. Therefore, the effect of an incompliance with the technical standard, even if it is not safeguarded by any social sanction, is the adverse result of practical activities, or failure in achieving the aimed objective, or achieving it by excessively high efforts[26]

This legal regulation on the state information-communication infrastructure security requirements shows a general concept of the legislator for provision, from one side, of the coherence for the operation of teleinformative systems used for execution of public assignments and public registers, and for exchange of public information in the electronic form between the public subjects, and for provision, on the other side, of efficient and safe exchange of information in the electronic form between the public subjects including also other countries and international organisations. This concept is realised by an accepted normative standard of security for the state information-communication infrastructure used by the subjects performing the public assignments.

[13] W. Lang, J. Wróblewski, S. Zawadzki, op. cit., s. 322.
[26] W. Lang, J. Wróblewski, S. Zawadzki, op. cit., p. 322.

3. Pojęcie „standard bezpieczeństwa" infrastruktury informacyjno-komunikacyjnej państwa

Termin standard bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa nie ma – analogicznie jak samo pojęcie tej infrastruktury - definicji legalnej. W potocznym ujęciu pojęcie standard wyraża „przeciętną normę, przeciętny typ, model; wyrób odpowiadający określonym wymogom; wzorzec"[27]. W tym ujęciu można go określić jako wspólnie ustalone kryterium, które określa powszechne, zwykle najbardziej pożądane cechy czegoś. W technice standard ujmowany jest z kolei jako zestaw parametrów, zwykle posiadający jakąś nazwę, który zapewnia odpowiedni poziom jakości, bezpieczeństwa, wygody lub zgodności z innymi wytworami techniki[28]. W doktrynie standard oznacza natomiast „regułę, wzór, zestaw cech lub parametrów technicznych, ekonomicznych, społecznych, obowiązujących z mocy prawa bądź innych decyzji, lub rekomendowanych przez instytucje państwowe, organizacje społeczne, zawodowe, gospodarcze, przez przedsiębiorstwa lub osoby fizyczne, albo stosowanych w praktyce na mocy decyzji konkretnej jednostki organizacyjnej, w celu zapewnienia spójności i współdziałania osób, instytucji, systemów, procesów i urządzeń"[29]. Źródłem tak rozumianego standardu może być norma stanowiona przez oficjalne instytucje normalizacyjne (ISO, PKN); norma prawna: ustawa, rozporządzenie, glosa; decyzja administracyjna; rekomendacja administracyjna, rekomendacja instytucji normalizacyjnej lub re-

3. Notion of State Information-communication Infrastructure "Security Standard"

The term of state information-communication infrastructure security standard has not been legally defined, similarly as the alone notion of this infrastructure. In common aspect the notion of standard expresses "an average norm, average type, model; an article corresponding to specific requirements; a pattern"[36]. In this aspect, it may be determined as a commonly set criterium, usually identifying the most demanded features of something. Subsequently, the technique perceives the standard as a set of parameters, usually having a title, which provides a relevant level of quality, security, convenience or compliance with other products of technique[37]. And in the doctrine the standard stands for the „rule, pattern, a set of technical, economic, social features or parameters, biding by the force of law or other decisions, or recommended by the state institutions, and by social, or occupational, or economic organisations, or by enterprises or physical persons, or applied in practice by the force of a decision of specific organisational unit in order to secure the coherence and cooperation of persons, institutions, systems, processes and equipment"[38]. The norm constituted by official standardisation institutions (ISO, PKN – Polish Normalisation Committee) may be a source of a standard understood in such a way; legal norm: the Act, disposition, gloss; administrative decision; administrative recommendation, rec-

[27] M. Szymczak (red.), Słownik języka polskiego, tom III, Warszawa 1981, tom III, s. 318.
[28] Zob. https://pl.wikipedia.org/wiki/Standard, dostęp z dnia 20 lipca 2022 r.
[29] Tak J. Oleński, op. cit., s. 29.
[36] M. Szymczak (red.), Polish Language Vocabulary, volume III, Warsaw 1981, p. 318.
[37] See https://pl.wikipedia.org/wiki/Standard, accessed on 20 July, 2022.
[38] Also J. Oleński, op. cit., p. 29.

komendacja oparta na autorytecie; reguła ustalona w wyniku bilateralnej lub multilateralnej umowy lub porozumienia stron; zasada lub wzór, nawyk powszechnie stosowany w praktyce; produkt lub technologia powszechnego stosowania; a nawet wymagania przyjmowane przez monopolistycznego producenta lub dystrybutora urządzeń lub oprogramowania[30]. Niewątpliwie, w każdym z zaprezentowanych ujęć zakres pojęcia standard jest szerszy niż pojęcie norma, która jest zazwyczaj rozumiana jako standard obowiązujący z mocy prawa lub decyzji administracyjnych[31].

Można zatem przyjąć, że standard infrastruktury informacyjno-komunikacyjnej państwa oznacza stosowanie w ramach danego systemu teleinformatycznego bądź kompleksu współdziałających, powiązanych ze sobą systemów teleinformatycznych, jednolitych, wspólnych, względnie trwałych reguł i zasad. Tak rozumiany standard w ujęciu normatywnym obejmuje zestaw określonych prawem wymagań, które powinna spełniać infrastruktura stosowana przez podmioty realizujące zadania publiczne do przechowywania, przetwarzania, gromadzenia i przesyłania danych (informacji publicznych) przy użyciu technologii ICT. Zestaw tych wymagań stanowi pewien powszechnie przyjmowany dla infrastruktury informacyjno-komunikacyjnej państwa „wzorzec bezpieczeństwa", który gwarantuje integralność poszczególnych elementów systemu oraz bezkolizyjność (kompatybilność) funkcjonalną stosowanych przez różne organy państwa różnorakich elementów systemów teleinformatycznych, jak przykładowo: formatów i oprogramowania dla różnych rejestrów publicznych czy różommendation of normalising institution or a recommendation grounded on an authority; a rule established in effect of bilateral or multilateral agreement or understanding of parties; principle or pattern, a commonly practiced custom; product or technology of common use; and even the requirements accepted by a monopolistic manufacturer or distributor of hardware and software[39]. Undoubtedly, in each of presented aspects the extension of notion *standard* is wider than *norm*, which is usually understood as a standard binding by the power of law or administrative decisions[40].

It may be then accepted that the standard of state information-communication infrastructure means the use of united and common rules and principles, which are relatively unchangeable, in the frame of a tele-informative system, or a complex of working together and connected tele-informative systems. The standard interpreted in this way encompasses in the normative aspect a specification of requirements determined by the law which have to be met by the infrastructure used by the subjects performing the public assignments for storing, processing, acquisition and transfer of data (public information) with application of ICT technologies. The specification of these requirements creates certain "pattern of security" which is commonly accepted for the state information-communication infrastructure, and which warrants the integrity of particular components of the system and operation without functional collisions (compatibility) for different components of tele-informative systems used by various institutions of

[30] Tak J. Oleński, op. cit., s. 30 i 36.
[31] Tak J. Oleński, op. cit., s. 30.
[39] Also J. Oleński, op. cit., p. 30 and 36.
[40] Also J. Oleński, op. cit., p. 30.

nych technologii teleinformatycznych. Infrastruktura informacyjno-komunikacyjna państwa stanowi kompleks ściśle ze sobą powiązanych i współdziałających systemów teleinformatycznych. W założeniu każdy z systemów teleinformatycznych jest elementem infrastruktury informacyjnej państwa jako jednego supersystemu teleinformatycznego, w niezbędnym zakresie spójnym z międzynarodowymi lub globalnymi systemami informacyjnymi. Systemy te powinny być przy tym zintegrowane w zakresie wszystkich elementów, które warunkują integralność i wymianę informacji między systemami, umożliwiają korzystanie ze wspólnych zasobów informacyjnych i metainformacyjnych. W gruncie rzeczy jest to zestaw koniecznych parametrów, cech i właściwości technicznych, ekonomicznych, społecznych i organizacyjnych tej infrastruktury, którego spełnienie pozwala uznać infrastrukturę za odpowiadającą obowiązującemu dla niej standardowi i zarazem zapewniającą bezpieczeństwo zarówno samych systemów, jak i wytwarzanych i wysyłanych przy ich użyciu informacji (danych, dokumentów). Zakres stosowania jednolitego standardu dla systemów teleinformatycznych stosowanych przez podmioty realizujące zadania publiczne decyduje o zakresie integralności i współdziałania różnych systemów teleinformatycznych[32]. A jego powszechne zastosowanie przez wiele współdziałających systemów teleinformatycznych państwa (systemów teleinformatycznych różnych organów) czyni dany standard (standardy) ważnym elementem infrastruktury informacyjno-komunikacyjnej państwa. Element ten doktryna określa mianem „bazowego standardu informacyjnego", przez co rozumie „taki standard informacyjny, którego przestrzeganie jest warunkiem spójności językowej, se-

state like: formats and software for different public registers, or different tele-informative technologies. The state information-communication infrastructure is a complex of tightly connected and cooperating tele-informative systems. By the assumption each of tele-informative systems is a component of state information infrastructure as one teleinfor-mative supersystem which is coherent in a required degree with international or global systems. At the same time, the systems have to be integrated, regarding all components which affect the integrity and exchange of information between the systems and allow for using common resources of information and metainformation. As a matter of fact, it is a specification of necessary technical, economic, social and organisational parameters, features and properties of this infrastructure which have to be met in order to recognise the infrastructure as corresponding to a standard binding for it, and also providing the security both for the alone systems and for the information (data, documents) produced and sent out with their use. The level of application of the united standard for tele-informative systems used by the subjects performing the public assignments decides about the extension of integrity and cooperation between different tele-informative systems[41]. And its common application by many cooperating state tele-informative systems (tele-informative systems of different institutions) makes the specific standard (standards) to be an important component of the state information-communication infrastructure. This component is described by the doctrine as a „fundamental information standard" what stands for „such information standard that

[32] Tak też na gruncie poprzedniego stanu prawnego J. Oleński, op. cit., s. 29.
[41] Also the same on the grounds of former legal status J. Oleński, op. cit., p. 29.

mantycznej lub wymiany informacji między systemami informacyjnymi jednostek organizacyjnych administracji, podmiotów społecznych, politycznych i gospodarczych w państwie i w skali międzynarodowej w ramach systemów informacyjnych obsługujących wiele podmiotów"[33]. Standard ten dotyczy treści i jakości informacji; repertuaru znaków służących odwzorowaniu informacji; pojęć i terminologii; języków: leksyki, gramatyki, semantyki, pragmatyki; danych i metadanych; struktur odwzorowania danych i metadanych (dokumentów); struktur i formatów wymiany danych w systemach teleinformatycznych; metod projektowania systemów informacyjnych i dokumentowania projektów; oprogramowania systemowego i narzędziowego; oprogramowania użytkowego sprzętu informatycznego; transferu danych i metadanych; protokołów telekomunikacyjnych; podstaw prawnych funkcjonowania systemów teleinformacyjnych; organizacji i procedur funkcjonowania systemów teleinformacyjnych; zasad i procedur przechowywania, ochrony i udostępniania informacji; powtarzalnych podsystemów, modułów i jednostek funkcjonalnych systemów teleinformacyjnych[34]. Efektywna standaryzacja wymaga zatem spójności wszystkich warstw standardów informacyjnych i technologicznych (informatycznych).

Standard dla infrastruktury informacyjno-komunikacyjnej państwa – z uwagi na rodzaj, wagę i charakter danych – charakteryzuje się wysokim rygoryzmem wymagań i sposobu ich przestrzegania przy jej projektowaniu, realizacji czy modernizacji, a także użytkowaniu. Wobec treści regulacji prawnej nie ma bowiem wątpliwości co do tego, że infrastruktura informacyjno-komunikacyjna państwa - określana w doktrynie mianem „infrastruktury

the compliance with it is a condition of linguistic and semantic coherence, or of the exchange of information between information systems of organisational units of administration, and social, political and economic subjects in the country and in the international scale for the information systems rendering the services for many subjects"[42]. The standard concerns the context and quality of information; languages: lexis, grammar, semantics, pragmatics; data and metadata; structures for copying data and metadata (documents); structures and formats of data exchange in tele-informative systems; methods for designing the information systems and documenting the designs; systemic and hardware software; operating software of informative hardware; transfer of data and metadata; telecommunication protocols; legal backgrounds for operation of tele-information systems; organisation and procedures of operation for tele-information systems; principles and procedures for storing, protecting and making accessible the information; repeatable subsystems, modules, and functional units of teleinfor-mation systems[43]. Therefore, the efficient standardisation requires the cohesion of all layers of information and technological (informative) standards.

Standard, for the state information-communication infrastructure, is characterised by a high level of rigorism in specifications and in a method of obeying them at its designing, building, or upgrading, or using, because of the type, meaning and character of data. In the face of the context of legal regulation there is no doubts that the state information-communication infrastructure – described in the doctrine as "in-

[33] Tak J. Oleński, op. cit., s. 32.
[34] Tak J. Oleński, op. cit., s. 33/34.

informacyjnej”[35] - stanowi szczególny rodzaj infrastruktury. Ten rodzaj infrastruktury jest przy tym niezwykle „wrażliwy”, bo służący do gromadzenia, przetwarzania i wymiany informacji generowanych przez różne organy państwa w różnych jego obszarach działania, począwszy od informacji wytwarzanych czy pozyskiwanych przez służby ochrony państwa a skończywszy na wytwarzanych czy pozyskiwanych przez placówki prowadzące działalność leczniczą. Niebezpieczne dla bytu państwa lub tylko jego pozycji na arenie międzynarodowej może okazać się nie tylko nieuprawniony i nielegalny dostęp do informacji o działaniach operacyjnych służb odpowiedzialnych za bezpieczeństwo państwa czy do informacji o stanie zdrowia osób sprawujących najwyższe funkcje w państwie, w tym o zastosowanych u nich urządzeniach wszczepowych opartych na technologii ICT lub innych używanych przez nie urządzeń telematycznych umożliwiających zdalnie monitorowanie parametrów życiowych lub nimi sterowanie, zakłócanie wysyłanych sygnałów alarmowych. Ale również dostęp do samej infrastruktury celem jej użycia przeciwko państwu, w tym poprzez podszywanie się pod osobę o określonym znaczeniu dla państwa i w jej imieniu wyrażanie na arenie międzynarodowej poglądów, może być szkodliwy. Wymaga to zatem zastosowania dla infrastruktury informacyjno-komunikacyjnej państwa narzędzi i mechanizmów „technologicznego” zabezpieczenia i środków prawnych jej ochrony przed zagrożeniami o szczególnych parametrach, właściwościach i cechach.

formation infrastructure”[44] – is a particular type of infrastructure. This type of infrastructure is moreover highly “sensitive” as it is used for collection, processing, and exchange of information generated by different institutions of state in various domains of its activity, starting from information produced or acquired by the state security services and ending on data generated or acquired by the institutions of health service. A danger for the state existence and its position on international area may be caused not only by an unauthorised and illegal access to information about operations of services responsible for the state security, or to information about health condition of persons holding the highest functions in the state, including the devices implanted into their bodies based on the ICT, or other telematic devices used by them for remote monitoring of life parameters, but also controlling them or jamming the transmission of alert signals. And also, the alone access to the infrastructure may be harmful and used against the state, including for instance an impersonation of a person, having a significant meaning for the state, to express adverse opinions in the international arena. Therefore, for the state information-communication infrastructure the tools and mechanisms of “technological” security of special parameters, properties and characteristics have to be applied, together with legal means for its protection against the threats.

[42] Also J. Oleński, op. cit., p. 32.
[43] Also J. Oleński, op. cit., p. 33/34.
[35] Tak np. J. Oleński, op. cit., s. 29. Szerzej na temat rozbieżności terminologicznych zob. E. Cisowska-Sakrajda, Prawne aspekty bezpieczeństwa …, s. 102 – s. 106.
[44] As for instance J. Oleński, op. cit., p. 29. Wider about terminological differences see E. Cisowska-Sakrajda, Legal Aspects of Security …, p. 102 – p. 106.

4. Komponenty standardu bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa

Standard infrastruktury informacyjno-komunikacyjnej państwa tworzy, zważywszy na jej złożoność i wieloelementowość, szeroka gama różnorakich o zróżnicowanym charakterze wymagań. Wymagania te przyjmowane są zarówno przez władzę prawodawczą w procesie legislacyjnym (zorganizowanym procesie stanowienia prawa przez uprawnione organy państwa), jak i w formie technicznych rekomendacji i norm technicznych, zaleceń, wskazówek metodologicznych, metod działania, zestawu parametrów, zasad i reguł postępowania, struktur danych, standardowych formatów wymiany informacji, zasad kodowania i kodów, opracowywanych przez organizacje normalizujące lub standaryzujące (krajowe i międzynarodowe), a w pewnym zakresie także przez producentów rozwiązań „technologicznych". Te ostatnio przywołane stają się elementem normatywnego standardu bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa z racji odesłania do nich w tekście aktu prawnego, który reguluje warstwę technologiczną bezpieczeństwa informacyjnego państwa. W dużym uproszczeniu można przyjąć, że standard ten obejmuje z jednej strony zawarte w dokumentach organizacji i instytucji normalizujących i standaryzujących dyrektywy techniczne i normy techniczne, które zawierają m.in. wskazówki efektywnego posługiwania się poszczególnymi urządzeniami technicznymi oraz reguły postępowania użytkownika przy korzystaniu z tych urządzeń. Określają one zatem – jeśli można tak to ująć – pewne parametry, właściwości i cechy bezpieczeństwa zastosowanych w infrastrukturze rozwiązań technologicznych i urządzeń technicznych, rozumianego zarówno jako zabezpieczenie przed

4. Components of State Information-communication Infrastructure Security Standard

The standard of state information-communication infrastructure, due to its complexity and multi-componential character, is created by a wide spectrum of various specifications of different character. These specifications are accepted both by the legislative authorities in the process of legislation (organised process of constituting the law by the authorised institutions of state), and in the form of technical recommendations and norms, and guidelines, and methodological instructions, methods of proceeding, specification of parameters, rules and principles of actions, data structures, standard forms of data exchange, principles of coding and the codes, prepared by the normalising or standardising organisations (national and international), and to some degree also by the manufacturers of "technological" solutions. These recently mentioned become a normative component of the state information-communication infrastructure security standard by the force of reference to it in the text of the legal act regulating the technological layer of state information security. It may be accepted in great simplification that this standard encompasses from one side the technical directives and technical norms contained in documents of normalising and standardising organisations and institutions, including for instance the guidelines for effective use of particular technical equipment and the rules for users to be followed at using this equipment. They determine then – as it may be said so – some parameters, properties and characteristics of security measures for technological solutions and technical equipment used in the infrastructure and

nieuprawnioną w nie ingerencją, jak i bezpieczeństwo ich użytkowania przez człowieka. Z drugiej strony są to – w znacznym również uogólnieniu - przyjęte na poziomie aktów prawa powszechnie obowiązującego dyrektywy, określające model architektury infrastruktury oraz warunki jej tworzenia, modernizacji i użytkowania, a zarazem wymagania dla rejestrów publicznych i zawartych w nich danych (informacji) oraz reguły postępowania użytkownika. W oparciu o powyższe można wyróżnić dwie zasadnicze grupy normatywnych wymagań infrastruktury informacyjno-komunikacyjnej państwa: dyrektywy i normy *sensu stricto* oraz dyrektywy i normy *sensu largo*. Te pierwsze odnoszą się do warstwy technicznej i technologicznej infrastruktury informacyjno-komunikacyjnej państwa i jej poszczególnych elementów, te drugie obejmują również warstwę organizacyjną tej infrastruktury i zasady stosowane przy budowie, modernizacji i rozbudowie infrastruktury, obowiązki podmiotów realizujących zadania publiczne przy użyciu systemów teleinformatycznych. Uprawnionym w tym kontekście wydaje się również wskazanie w obrębie standardów infrastruktury informacyjno-komunikacyjnej państwa – z uwagi na jej specyfikę łączącą w sobie zarówno warstwę technologiczną, jak i informacyjną - na standardy teleinformatyczne, które gwarantują efektywność funkcjonalną, techniczną i ekonomiczną systemów teleinformatycznych tworzących tę infrastrukturę, oraz standardy informacyjne, które służą do zapewnienia jakości i integralności samych informacji (danych). Standardy infrastruktury – pomimo wyraźnego doktrynalnego rozróżniania w ramach sfery informacyjnej państwa warstwy informacyjnej i warstwy technologicznej - nie odnoszą się jednakże wyłącznie do elementów tworzących samą infrastrukturę (jej elementów technologicznych i infor-

understood as both a safeguarding against unauthorised interference with it, and the safety of its use by people. On the other side they are – also in a general view – the directives accepted on the level of legal acts of commonly binding law which identify the model of infrastructure architecture and the conditions for its building, upgrading, and using, and also the requirements for public registers and data (information) contained in them, and the rules of user's activity. Basing on the above mentioned, two general groups of normative requirements for the state information-communication infrastructure may be distinguished: directives and norms *sensu stricto* and directives and norms *sensu largo*. The first ones refer to the technical and technological layer of the state information-communication infrastructure and its particular components, and the second ones also include the organisational level of this infrastructure and the principles applied at the building, upgrading and extension of the infrastructure, and the obligations of subjects performing the public assignments by using tele-informative systems. In this context it is rightful to indicate among the standards of state information-communication infrastructure – due to its specificity combining in itself both the technological and information layers – the tele-informative standards which warrant the functional, and technical, and economic efficiency of tele-informative systems creating this infrastructure, and the information standards which provide the quality and integrity of the alone information (data). The infrastructure standards – despite a clear doctrinal distinction between the layers of information and technology in the frame of the state information domain – relate not only to components creating the alone infrastructure (its technological and informative

matycznych) jako narzędzi do gromadzenia, przetwarzania, przechowywania i przesyłania informacji (danych), ale również do formatów i struktury elektronicznych dokumentów (danych), ich wizualizacji, kodowania, języka oprogramowania, podpisu elektronicznego, zaopatrywania dokumentów w pieczęć elektroniczną, czy rejestrów publicznych. Dowodzi to zasadności twierdzenia, że sferę informacyjną państwa należy postrzegać całościowo, nie zaś – jak to zwyczajowo czyni doktryna – w odniesieniu do poszczególnych jej warstw. Wyróżnienie tych warstw jest podyktowane odrębnym zakresem regulacji prawnej warstw tej sfery oraz interdyscyplinarnym charakterem bezpieczeństwa informacyjnego państwa i wynikającym z tego „fragmentarycznym" badaniem tego obszaru bezpieczeństwa państwa w różnych jego aspektach i przy użyciu różnych metod badawczych przez badaczy różnych dziedzin nauki. To jednak takie ostre doktrynalne zakreślanie granic między różnymi warstwami bezpieczeństwa informacyjnego państwa: technologiczną, organizacyjno-ustrojową, proce-sową, materialną oraz osobową[45] nie wydaje się możliwe i uprawnione. Warstwy te przecież w mniejszym lub większym stopniu zazębiają się, niejako „nachodzą" na siebie, oddziałują wzajemnie na siebie, są „sprzężone" i silnie powiązane. Dopiero wszystkie razem rozważane i razem współistniejące gwarantować mogą bezpieczeństwo sfery informacyjnej państwa. O wiele właściwsze wydaje się kompleksowe podejście do wszystkich warstw bezpieczeństwa informacyjnego państwa i całościowe jego postrzeganie.

Zróżnicowany charakter normatywnych wymagań bezpieczeństwa infrastruktury pozwala wskazać również wymagania ogólne, ustanawiające pewne ogólne zasady (reguły,

components) as the tools for collecting, processing, storing and transferring the information (data), but also to formats and the structure of electronic documents (data), their visualisation, coding, programming language, electronic signature, application of an electronic stamp in documents, or the public registers. It proves the reason for stating that the state information domain has to be perceived in the integrity, but not – as the doctrine commonly does – respectively to its particular layers. The distinction of these layers is dictated by an individual scope of legal regulations for the layers of this domain and by the interdisciplinary character of state information security resulting in "fragmental" investigation of this domain of state security in its different aspects at employment of different research methods and by researches of different fields of science. But any distinctive doctrinal outline of borders between different layers of the state information security: technological, organisational-systemic, legal, material and personal[60] seems to be impossible and not justified. It is because of the fact that these layers engage to each other in a smaller or greater degree, or in some way cover some parts of them, or interact as they are "coupled" and strongly connected. Therefore, only when all of them are considered and exist together they may warrant the security of state information domain. A complex approach to all layers of state information security at its overall perception seems to be a most proper one.

Differentiated character of normative specifications for the security of infrastructure can be helpful at indication of some general requirements establishing some general principles (rules, guidelines) used at

[45] Szerzej zob. E. Cisowska-Sakrajda, Prawne aspekty bezpieczeństwa …, s. 97/98.
[60] Wider see E. Cisowska-Sakrajda, Legal Aspects of Security …, p. 97/98.

wskazówki) stosowane przy kształtowaniu wymagań dla projektowanej infrastruktury czy udostępnianiu danych z rejestrów publicznych, oraz wymagania szczegółowe, określające w szczególności parametry, cechy lub właściwości poszczególnych elementów infrastruktury zarówno o charakterze technologicznym, jak i organizacyjnym. Katalog tych pierwszych - zasad ogólnych, postrzegany literalnie poprzez treść regulacji prawnej, z pozoru tylko wydaje się niezbyt skomplikowany. W rzeczywistości jednak tworzy go szereg zasad ogólnych odnoszących się do infrastruktury, poszczególnych elementów jej architektury a nawet etapów procesu jej kształtowania oraz korzystania z niej. W pierwszym rzędzie, są to wprost nazwane i wysłowione przez prawodawcę zasady ogólne dotyczące wdrażania, rozbudowy i modernizacji oraz użytkowania systemów teleinformatycznych[46] oraz ustanowione przez organizacje zasady ogólne stosowania wymogów określonych w normach[47]. Należą do nich adresowane do podmiotów publicznych, sformułowane na poziomie ustawowym, dwie fundamentalne zasady ogólne: zasada neutralności technologicznej/zasada równego traktowania różnych rozwiązań informatycznych oraz zasada jawności używanych standardów i specyfikacji[48], uzupełnione na poziomie norm, zwłaszcza o zasadę kompletności wymagań oraz zasadę równoważności wymagań[49]. W dalszej kolejności, są to zasady ogólne wynikające z celów lub całokształtu regulacji prawnej (lecz nie nazwane), jak przykładowo: zasada spójności

preparation of specifications for designed infrastructure, or at making available the data of public registers, and detailed requirements, especially identifying the parameters, characteristics or properties of particular components of infrastructure having both the technological and organisational character. The catalogue of these first ones, the general principles, perceived literally by the wording of legal regulations, seems to be only apparently not too much complicated. In reality it contains a series of general principles relating to infrastructure and particular components of its architecture, and even to the stages of its building and using. In the first, they are general principles, directly named and expressed by the legislator, relating to implementation, enlargement, and upgrading, and using of tele-informative systems[61], and general principles established by organisations for application of specific requirements in the normalising standards[62]. They include two fundamental principles addressed to the public subjects formulated on the statutory level: the principle of technological neutrality/principle for equal treatment of different informative solutions, and the principle of openness for used standards and specifications[63], supplemented by the principle of completeness on the level of norms, especially by the principle of completeness of requirements and the principle of equivalency of requirements[64]. In the next turn, they are the general principles resulting from the objectives or the overall form of the legal regulation (but not named), such as

[46] Zob. np. art. 1 pkt 2 i pkt 3, art. 13 ust. 2 ustawy o informatyzacji podmiotów publicznych oraz § 3 ust. 1 pkt 2 czy § 4 ust. 3 rozporządzenia w sprawie KRI.
[47] Tak pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN nr PN-ISO/IEC 27001, s. 7.
[48] 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 KRI.
[49] Zob. np. pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN nr PN-ISO/IEC 27001, s. 7.

działania systemów teleinformatycznych i rejestrów publicznych (zasada zintegrowanej informatyzacji, zasada zintegrowanej platformy analitycznej)[50], zasada sformalizowania danych, jak formaty danych, wzory dokumentów elektronicznych oraz formularze elektroniczne[51] oraz zasady ogólne udostępniania danych z rejestrów publicznych, jak zasada wnioskowości czy uwierzytelniania[52]. Wymagania szczegółowe natomiast - ujęte kazuistycznie i w dużej mierze określane poprzez odwołanie do konkretnych norm technicznych, standaryzujących, w tym norm jakościowych (ISO/IEC), a także przyjmowanego przez zindywidualizowanego producenta technologii oprogramowania (*Microsoft Corporation*) - obejmują wymagania (minimalne) dla systemów teleinformatycznych[53], wymagania dla interoperacyjności systemów teleinformatycznych i rejestrów publicznych, określone w Krajowych Ramach Interoperacyjności[54], wymagania (minimalne) dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[55], wymagania dla sys-

for instance: the principle of cohesion on operation of tele-informative systems and public registers (principle of integrated informatisation, principle of integrated analytical platform)[65], the principle of formalisation of data, such as data formats, patterns of electronic documents and electronic forms[66]; and general principles on providing access to public register data such as the principle of applicability or approval[67]. And on the other side, the detailed specifications – presented casuistically and determined in a great degree by reference to specific normalising technical standards, including quality standards (ISO/IEC), and also to the software accepted by an individual manufacturer of technology (*Microsoft Corporation*) – include the requirements (minimal) for tele-informative systems[68], requirements for interoperability of tele-informative systems and public registers determined in the Country Interoperability Frames[69], the requirements (minimal) for public registers and exchange of information in the electronic

[61] See for instance art. 1 point 2 and 3, art. 13 pos. 2 of the law on informatisation of public subjects and § 3 pos. 1 point 2 or § 4 pos. 3 of disposition on CIF.
[62] Also point 1 entitled the Scope of Norm, and point 0 entitled Introduction subpoint 01 paragraph five PN nr PN-ISO/IEC 27001, p. 7.
[63] See especially art. 1 point 2 and 3, art. 13 pos. 2 and art. 18 point 1 of the law on informatisation of public subjects and § 3 pos. 1 point 2 of disposition on CIF.
[64] See for instance point entitled the Scope of Norm and point 0 entitled Introduction, subpoint 01 paragraph five PN nr PN-ISO/IEC 27001, p. 7.
[50] Zob. art. 12b czy art. 1 pkt 9c ustawy o informatyzacji podmiotów publicznych.
[51] Zob. np. art. 3 pkt 24 i pkt 25 ustawy o informatyzacji podmiotów publicznych.
[52] Zob. art. 15a ustawy o informatyzacji podmiotów publicznych.
[53] 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, a także § 1 pkt 3 oraz rozdział IV rozporządzenia w sprawie KIR.
[54] Jest to zawarty w Krajowych Ramach Interoperacyjności „zestaw wymagań semantycznych, organizacyjnych oraz technologicznych dotyczących interoperacyjności systemów teleinformatycznych". Zob. np. art. 1 pkt 2 , art. 3 pkt 9 i pkt 21 oraz art. 13 ust. 1 ustawy o informatyzacji podmiotów publicznych oraz rozdział II, a zwłaszcza § 3 - § 5 rozporządzenia w sprawie KRI.
[55] 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. rozdział III rozporządzenia w sprawie KRI i art. 1 pkt 2 i pkt 3 oraz art. 3 pkt 9 i pkt 10 ustawy o informatyzacji podmiotów publicznych.

temów zarządzania bezpieczeństwem informacji[56] oraz wymagania dla użytkowników systemu[57]. Wymagania dla systemów teleinformatycznych stanowią przy tym zbiorczą grupę różnych zestawów wymagań. Są to odrębne zestawy wymagań dla formatów danych oraz protokołów komunikacyjnych i szyfrujących, możliwych do zastosowania w oprogramowaniu interfejsowym; sposoby zapewnienia bezpieczeństwa przy wymianie informacji, standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej oraz sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych[58]. Nie sposób też nie odnotować, że prawodawca eksponuje już na poziomie ustawowym rozróżnienie normatywnych wymagań dla systemów teleinformatycznych, Krajowych Ram Interoperacyjności tych systemów oraz rejestrów publicznych, wskazując wymagania organizacyjne i techniczne (technologiczne) a dla dwu ostatnio wymienionych także wymagania semantyczne[59]. Tym sa-

form[70], the requirements for systems governing the security of information[71] and requirements for the system users[72]. And the requirements for tele-informative systems constitute an accumulated group of different specifications of requirements. They are the separate specifications of requirements for data formats, and for communication and coding protocols which can be used in interface software; the methods warranting the security at exchange of information, technical standards providing the exchange of information with participation of public subjects and consideration of a transborder exchange, and the methods securing the access of handicapped persons to information resources of the public subjects[73]. It has to be also noted that the legislator stresses just on the statutory level the distinction of normative requirements for tele-informative systems, the Country Interoperability Frames of these systems and public registers, indicating the organisational and technical (technological) requirements, and for two recently mentioned also the semantic requirements[74].

[65] See art. 12b or art. 1 point 9c of the Act on informatisation of public subjects.
[66] See for instance art. 3 point 24 and point 25 of the Act on informatisation of public subjects.
[67] See art. 15a of the Act on informatisation of public subjects.
[68] It is „a specification of organisational and technical requirements which have to be met by tele-informative system used for performance of public assignments to data exchange with other tele-informative systems used for execution of public assignments, and to provide the access to information resources available in these systems". See art. 3 point 9 of the Act on informatisation of public subjects, and also § 1 point 3 and chapter IV of disposition on CIF.
[69] It is "a specification of semantic, organisation and technology requirements for interoperability of tele-informative systems" included in Country Interoperability Frames. See for instance art. 1 point 2 , art. 3 point 9 and point 21 and art. 13 pos. 1 of the Act on informatisation of public subjects, and chapter II, and particularly § 3 - § 5 of disposition on CIF.
[56] Zob. § 20 rozporządzenia w sprawie KIR.
[57] Zob. np. art. 14, art. 15a ust. 1, art. 16a, art. 19b ust. 2 i ust. 3, art. 19f, art. 20i ustawy o informatyzacji podmiotów publicznych oraz § 8 rozporządzenia w sprawie KIR.
[58] Zob. § 1 pkt 3 rozporządzenie w sprawie KIR.
[59] Por. art. 3 pkt 9 i pkt 21 ustawy o informatyzacji podmiotów publicznych.
[70] It is a specification of information characteristics, including identity markers and corresponding to them characteristics of structural components of information transfer, such as the contend of data field, securing the cohesion of operation for the public registers and the exchange of information in the electronic form with the public subjects. See chapter III of disposition on CIF and art. 1 point 2 and point 3, and art. 3 point 9 and point 10 of the Act on the informatisation of public subjects.
[71] See § 20 of disposition on CIF.

mym wskazuje na odmienny charakter poszczególnych zespołów wymagań oraz ich znaczenie dla zapewnienia bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa oraz rejestrów publicznych i zawartych w nich informacji. Nie sposób oprzeć się wrażeniu, że takie rozróżnienie stanowi zarazem podstawowy podział normatywnych wymagań bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa i informacji.

5. Interoperacyjność systemów teleinformatycznych i rejestrów publicznych oraz Krajowe Ramy Interoperacyjności

Interoperacyjność – generalny ustawowy wymóg dla systemów teleinformatycznych i rejestrów publicznych, składających się na infrastrukturę informacyjno-komunikacyjną państwa – wyraża, zgodnie z jej definicją legalną, „zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych”[75]. W ujęciu doktrynalnym „interoperacyjność to zdolność systemów teleinformatycznych do bezpośredniego współdziałania ze sobą (bez udziału człowieka jako tzw. interfejsu białkowego). Systemy (…) mogą sobie wzajemnie udostępniać dane, jednak pod warun-

It indicates by the same on a different character of particular specifications of requirements, and on their meaning for provision of security to the state information-communication infrastructure, and to the public registers and the information contained in them. It suggests that such distinction is by the same a basic division of the security normative requirements to the information and the state information-communication infrastructure.

5. Interoperability of Tele-informative Systems and Public Registers and Country Interoperability Frames

The interoperability – general statutory requirement for tele-informative systems and public registers being part of the state information-communication infrastructure – expresses, according with its legal definition, “the ability of different subjects and used tele-informative systems and public registers to work together in favour of mutually beneficial and agreed objectives, with regard for sharing the information and knowledge by the business processes they assist, and performed by exchange of data via tele-informative systems used by these subjects”[80]. In the doctrinal aspect “interoperability is the ability of tele-informative systems for direct cooperation between them (without human participation as the so called protein interface). The systems (…) may mutually share the data provided that the data are not forged, transformed in uncontrolled way, lost, get changed by putting them into another context, etc. (…).

[72] See for instance art. 14, art. 15a pos. 1, art. 16a, art. 19b pos. 2 and pos. 3, art. 19f, art. 20i of the Act on informatisation of public subjects, and § 8 of disposition on CIF.
[73] See § 1 point 3 of disposition on CIF.
[74] Compare art. 3 point 9 and point 21 of the Act on informatisation of public subjects.
[75] Zob. art. 3 pkt 18 ustawy o informatyzacji podmiotów publicznych.
[80] See art. 3 point 18 of the Act on informatisation of public subjects.

kiem, że dane te nie będą ulegały zafałszowaniu, niekontrolowanym przekształceniom, utracie, zmianie znaczenia przez umieszczenie ich w innym kontekście itd. (…) Interoperacyjność w praktyce pozwala na łączenie dotychczasowych odrębnych procesów, dzięki bezpośredniemu współdziałaniu również odrębnych dotychczas systemów teleinformatycznych w oparciu o identyfikatory obiektów, takich jak człowiek (PESEL), podmiot (instytucja, przedsiębiorstwo – REGON) czy obiekt w przestrzeni (punkt adresowy w oparciu o TERYT)"[76]. Tak rozumianą interoperacyjność osiąga się na trzy normatywnie i rozłącznie wskazane w Krajowych Ramach Interoperacyjności sposoby, a mianowicie poprzez ujednolicenie, wymienność lub zgodność[77]. Wyrażają one kolejno – w myśl ich definicji normatywnych – „zastosowanie kompatybilnych norm, standardów i procedur przez różne podmioty realizujące zadania publiczne"; „możliwość zastąpienia produktu, procesu lub usługi bez jednoczesnego zakłócenia wymiany informacji pomiędzy podmiotami realizującymi zadania publiczne lub pomiędzy tymi podmiotami a ich klientami, przy jednoczesnym spełnieniu wszystkich wymagań funkcjonalnych i pozafunkcjonalnych współpracujących systemów" oraz „przydatność produktów, procesów lub usług przeznaczonych do wspólnego użytkowania, pod specyficznymi warunkami zapewniającymi spełnienie istotnych wymagań i przy braku niepożądanych oddziaływań"[78]. Podmiot publiczny wdrażający dany system teleinformatyczny dla realizacji zadań publicznych posiada zatem pewną dozę dowolności wyboru sposobu zapewnienia interope-

In practice, the interoperability allows for connection of processes which were separated in the past, due to direct cooperation the tele-informative systems, which were also separated up to now, by using the identity markers of objects such as human being (PESEL), subject (institution, enterprise – REGON), or an object in the space (address point on the base of TERYT)"[81]. The interoperability understood in such way can be achieved by three normative and distinctive ways indicated in the Country Interoperability Frames, and namely the unification, exchangeability, or compliance[82]. They successively express – according to their normative definitions – „the application of compatible norms, standards, and procedures by different subjects performing the public assignments"; „possibility for replacing the product, process or service without any simultaneous harm to exchange of information between the subjects performing the public assignments, or between these subjects and their customers, at simultaneous fulfilment of all functional and by-functional requirements for cooperating systems", and "the usefulness of products, processes, or services designated for a common use, in the frame of specific conditions providing the fulfilment of essential requirements, and at the lack of any adverse actions"[83]. A public subject implementing a given tele-informative system for the execution of public assignments has a certain degree of freedom in selection of a way for provision of interoperability to this system, and the circumstances resulting from the estima-

[76] G. Szpor, K. Wojsyk, op. cit., wersja z Lex.
[77] Zob. § 4 rozporządzenia w sprawie KRI.
[78] Zob. § 4 rozporządzenia w sprawie KRI.
[81] G. Szpor, K. Wojsyk, op. cit., version with Lex.
[82] See § 4 of disposition on CIF.
[83] See § 4 of disposition on CIF.

racyjności temu systemowi, a kryteriami pomocnymi w dokonaniu tego wyboru są okoliczności wynikające z szacowania ryzyka oraz właściwości projektowanego systemu teleinformatycznego, jego zasięg oraz dostępne na rynku rozwiązania informatyczne. Granicę tej swobody zakreśla natomiast nakaz przestrzegania zasady neutralności technologicznej. Co niezwykle interesujące interoperacyjność ma – z woli prawodawcy - trzy poziomy: organizacyjny, semantyczny oraz technologiczny[79]. Każdemu z tych poziomów odpowiada zestaw wymogów, które podmiot publiczny obowiązany jest uwzględnić projektując czy modernizując system teleinformatyczny lub rejestr publiczny. Zestaw tych wymagań na poziomie ustawy o informatyzacji podmiotów publicznych, a technologicznych także na poziomie rozporządzenia w sprawie KIR został przy tym przyjęty na minimalnym poziomie.

Zakończenie

Rodzima regulacja prawna standardu bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa jest – jak dowiodła przeprowadzona analiza - rozproszona w wielu aktach prawnych i to o różnej randze w konstytucyjnej hierarchii źródeł prawa, począwszy od ustaw, poprzez akty do nich wykonawcze, a skończywszy na normach i dyrektywach technicznych. Regulacja ta jawi się jako „wielopoziomowa" i często blankietowa, skoro odwołuje się do norm technicznych, które kształtowane są na poziomie międzynarodowym przez organizacje i instytucje standaryzujące lub normalizujące, a niekiedy przez producentów technologii o uznanej pozycji na rynku. Mimo tak dużego zróżnicowania źródeł normatywnych, czę-

tion of a risk, and characteristics of the designed tele-informative system with its range and informative solutions accessible in the market, are the criteria which can be helpful to make this choice. The limit of this freedom is outlined by the ordinance for following the principle of technological neutrality. It is highly interesting that according with the legislator's will, the interoperability has three levels: organisational, semantical, and technological[84]. Each of these levels has a corresponding specification of requirements which has to be regarded by a public subject at designing or upgrading a tele-informative system or public register. The specification of these requirements on the level of the law on informatisation of public subjects, and also technological requirements on the level of disposition for CIF, was at the same time accepted on the minimal level.

Summary

The domestic legal regulation on the security standard of state information-communication infrastructure is dispersed, as it was proved by the performed analysis, throughout many legal acts of various ranks in the constitutional hierarchy of origins of the law starting from the acts of law, through the executive acts to them, and ending on technical standards and directives. This regulation looks like a "multilateral", and often as a formalistic one, as it refers to technical standards which are formed on the international level by standardising or normalising organisations and institutions, and sometimes by the manufacturers of technology with reputable position in the market. Despite the high differentiation of norma-

[79] Zob. § 5 rozporządzenia w sprawie KRI.
[84] See § 5 of disposition on CIF.

stokroć również mało klarownych, jak i niejednorodnego charakteru samych norm prawnych możliwe jest odkodowanie normatywnego wzorca standardu bezpieczeństwa tej infrastruktury. Niewątpliwie taki stan regulacji nie ułatwia ustalenia katalogu normatywnych wymagań składających się na ten standard. W praktyce działania podmiotów realizujących zadania publiczne przy użyciu infrastruktury informacyjno-komunikacyjnej państwa rodzi to niebezpieczeństwo wadliwego zrekonstruowania wzorca tego standardu w odniesieniu do poszczególnych elementów składowych tej infrastruktury, co w efekcie stwarza groźbę dla bezpieczeństwa samej infrastruktury i przetwarzanych przy jej użyciu informacji. Groźba ta jest tym bardziej realna, gdy zważymy na dynamiczny rozwój technologii i związane z nim nowe „możliwości" nieuprawnionej ingerencji w infrastrukturę oraz powszechnie znane trudności interpretacyjne norm prawnych, zwłaszcza w tak specyficznym interdyscyplinarnym obszarze normatywnym. To wymaga dużej ostrożności i czujności tych podmiotów przy projektowaniu, wdrażaniu i modernizacji rzeczonej infrastruktury. Trudno byłoby chyba normodawcy w inny sposób ująć tę tak skomplikowaną problematykę. Wobec tego zabieg prawodawcy odesłania do powszechnie uznawanych i stanowionych przez międzynarodowe i krajowe organizacje normalizujące (standaryzujące) wymogów i standardów urządzeń i sieci teleinformatycznych – mając na uwadze technologiczną naturę infrastruktury – jest jak najbardziej uzasadniony. Te uwzględniają wszak rozwój technologiczny w tym obszarze i – aktualne do najnowszej wiedzy i rozwoju ICT - warunki bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa.

Normatywny standard bezpieczeństwa infrastruktury informacyjno-komunikacyjnej

tive sources, often a bit unclear, and the inhomogeneous character of the alone legal norms, it is possible to decode a normative pattern of the security standard for this infrastructure. Undoubtedly, such state of regulations does not facilitate the establishment of a catalogue of normative requirements constituting this standard. In practice, the activities of subjects performing the public assignments with the use of the state information-communication infrastructure can be jeopardised by a faulty reconstruction of the pattern of this standard relating to particular components of this infrastructure what in effect creates a threat to this infrastructure and to the processed information. This threat is more realistic when we consider the dynamical development of technology and connected with it new "possibilities" of unauthorised interference with the infrastructure, and the widely known problems with interpretation of legal norms, especially in such specific and interdisciplinary normative domain. It demands a high care and sensitivity of these subjects at the designing, implementation, and upgrading of the said infrastructure. It would be rather difficult for the lawmakers to present these complex questions in other way. In this regard, the legislator's move of referring to the requirements and standards for hardware and tele-informative networks, which are commonly acceptable and constituted by international and national normalising (standardising) organisations, is highly substantiated. Anyway, they pay regard to the technological development in this domain and to the conditions of security of the state information-communication infrastructure which are the state of the art in present knowledge and the progress of CIF.

The normative security standard of the state information-communication infrastruc-

państwa jest zatem złożony, wieloelementowy i skomplikowany. Na standard ten składają się: wymagania normatywne samej infrastruktury, zasady jej tworzenia, modyfikacji oraz korzystania oraz reguły postępowania użytkowników, w tym podmiotów realizujących zadania publiczne przy użyciu tej infrastruktury. Występuje przy tym szeroka gama różnorakich wymagań bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa, niekiedy dedykowanych określonym elementom tej infrastruktury; a katalog warunków bezpieczeństwa infrastruktury do pewnego stopnia tylko ma charakter uniwersalny. W tym obszarze normatywnym można zaobserwować widoczną korelację między złożonością infrastruktury a złożonością standardu jej wymagań. A różnorodność występujących w obrocie gospodarczym rozwiązań technologicznych i technicznych ma swoje konsekwencje w postaci ustanowionej przez prawodawcę zasady neutralności technologicznej systemów teleinformatycznych używanych przez podmioty realizujące zadania publiczne oraz przyznanej tym podmiotom swobody stosowania różnych rozwiązań teleinformatycznych wraz z przyjętym dla nich standardem. Nie dziwi zatem, że standard bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa ma charakter mieszany. Tworzą go normatywne wymagania o różnorodnym charakterze - zarówno zasady ogólne, jak i wymagania szczegółowe, stanowione przez upoważniony organ państwa, ale też przyjmowane przez organizacje standaryzujące, a nawet narzucone przez wiodących na rynku producentów rozwiązań technologicznych. W gruncie rzeczy w obrocie prawnym funkcjonuje szereg zestawów wymagań (kryteriów, cech, właściwości, parametrów), które są dedykowane różnym systemom teleinformatycznym i rozwiązaniom technologicznym stosowanym przez po-

ture is then a complex, multi-componential and complicated one. The standard contains: normative requirements of the alone infrastructure, principles of its building, modification, and using, and the principles of users procedure including the subjects performing the public assignments with the use of this infrastructure. At the same time there is a great scale of different requirements for the state information-communication infrastructure security, which are sometimes dedicated to specific components of this infrastructure; and the catalogue of conditions for infrastructure security has a universal character only in certain degree. In this normative area a visible correlation may be observed between the complexity of the infrastructure and the complexity of standard for its requirements. And the variety of technological and technical solutions existing in the economic trading has its consequences in the form of the principle of technological neutrality established by the legislator for teleinformative systems used by the subjects performing the public assignments, and in form of freedom assigned to these subjects on the application of different teleinformative solutions with the standard accepted for them. Therefore, it is nothing strange that the standard of the state information-communication infrastructure security has a mixed character. It is created anyway by normative requirements of different character – the general principles, and also the detailed requirements established by the state authorised institution, but also accepted by the standardising organisations, and even enforced by the market leading manufacturers of technological solutions. In reality there is a series of requirements (criteria, characteristics, properties, parameters) functioning in the legal circulation which are dedicated to different tele-informative systems and

szczególne ogniwa organizacyjne infrastruktury – organy państwa, a także określonym elementom infrastruktury informacyjno-komunikacyjnej państwa. Niektóre z wymagań przy tym same w sobie stanowią powszechnie uznawany standard technologiczny lub jakościowy.

technological solutions used by particular organisational units of the infrastructure – state institutions, and to specific components of the state information-communication infrastructure. And some requirements by themselves create a commonly accepted technological or quality standard.

Bibliografia / *Bibliography*

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

Cisowska-Sakrajda E., Prawne aspekty bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa, Problemy Techniki Uzbrojenia 2022, zeszyt 162, nr 4.

Kitler W., Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe, Toruń 2018.

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

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

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

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

Wyporska-Frankiewicz J., Cisowska-Sakrajda E., Dostęp do informacji publicznej a bezpieczeństwo państwa, Wiedza Obronna 2022, vol. 278, nr 1.

Żebrowski A., Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kolegium Analiz Ekonomicznych 2013, nr 29.