ISSN 1230-3801

Zeszyt 162 nr 4/2022, str. 89-130
Volume 162 No. 4/2022, pp. 89- 130

PRAWNE ASPEKTY BEZPIECZEŃSTWA INFRASTRUKTURY INFORMACYJNO-KOMUNIKACYJNEJ PAŃSTWA

THE LEGAL ASPECTS OF THE SECURITY OF THE STATE'S INFORMATION AND COMMUNICATION INFRASTRUCTURE

Ewa CISOWSKA-SAKRAJDA ORCID: 0000-0001-8383-6951
Szkoła Wyższa Wymiaru Sprawiedliwości w Warszawie, adiunkt w Centrum Badań Polityki Europejskiej
The Warsaw's College of Justice, lecturer in the Research Centre of the European Policy

DOI 10.5604/01.3001.0016.3027

Streszczenie: Rozważania artykułu koncentrują się wokół nowych technologii informacyjno-komunikacyjnych i ich wpływu na funkcjonowanie współczesnych państw i społeczeństw informacyjnych oraz technologicznych zagrożeń dla bezpieczeństwa informacyjnego państwa. Centralnym punktem analizy jest rodzima regulacja prawna w zakresie pojęcia infrastruktury informacyjno-komunikacyjnej państwa oraz normatywnych wymagań i standardów jej bezpieczeństwa, a także poglądy rodzimej nauki różnych dyscyplin wiedzy w obszarze bezpieczeństwa informacyjnego państwa.

Słowa kluczowe: bezpieczeństwo informacyjne państwa, bezpieczeństwo infrastruktury informacyjno-komunikacyjnej, wymagania dla infrastruktury informacyjno-komunikacyjnej, zagrożenia bezpieczeństwa infrastruktury informacyjnej państwa

Abstract: The discussion of the Article focuses on new information and communication technologies and their impact on the functioning of modern States and information societies and on technological threats to the information security of the State. The main focus of the study is the domestic legal regulation on the concept of information and communication infrastructure of the State and the normative requirements and standards of its security, as well as an analysis of the views of the local science of various disciplines of knowledge in the area of information security of the State.

Keywords: state information security, security of information and communication infrastructure, requirements for information and communication infrastructure, threats to the security of the state information infrastructure

1. Technologie informacyjno-komunikacyjne a bezpieczeństwo informacyjne państwa

Dynamiczny i burzliwy rozwój nowych technologii informacyjno-komunikacyjnych (ang. *information and communications technology*, ICT) od czasu pojawienia się koncepcji

1. Information-communication Technologies and State Information Security

Since the appearance of a concept of information society[4], the dynamic and extensive development of new information and communications technologies (ICT) has not

społeczeństwa informacyjnego[1] nie pozostał bez wpływu na funkcjonowanie państwa i jego organów. Technologie te znalazły szerokie zastosowanie także do gromadzenia, przetwarzania, przechowywania i przesyłania niezliczonej ilości danych generowanych przez państwo i jego administrację i to danych o różnorodnym charakterze i ciężarze gatunkowym, lecz ważnych z punktu widzenia niezakłóconego realizowania przez państwo jego zadań. Obecnie technologie ICT są używane we wszystkich obszarach działania państwa, a zwłaszcza przez podmioty realizujące zadania publiczne w sferze bezpieczeństwa wewnętrznego i zewnętrznego państwa. Istotny wpływ na taki stan rzeczy miało przyjęcie na poziomie unijnym w 2000 r. Strategii Lizbońskiej *e-Europa* 2002[2], w tym jednej z jej założeń - polityki *e-government* oraz e-usług (publicznych usług *online*), a następnie jej upowszechnienie na szeroką skalę w państwach członkowskich Unii Europejskiej. Wedle tej polityki – najogólniej ją charakteryzując - administracja publiczna w procesach wymiany informacji, a precyzyjnie danych, i świadczenia usług publicznych korzysta z rozwiązań technologii informacyjnych i komunikacyjnych[3].

been leaving the functionality of state and its institutions beyond its impact. The technologies are also widely used for collection, processing, storing, and transmission of huge amounts of data generated by the state and its administration, including data of different character and importance, but of great significance for undisturbed performance of tasks by the state. The ICT are used now in all domains of state activities, especially by the subjects performing public assignments in sectors of state internal and external security. Acceptation of the Lisbon Strategy *e-Europa* 2002[5] on the European union level in 2000, and one of its assumptions – policy *e-government* and e-*services* (public *online* services), had an essential impact into such situation after its wide promotion in the European Union member states. In general, according to this policy, the public administration employs the solutions of information and communication technologies[6] in processes of exchanging information, and more precisely of data, and at rendering the public services.

The infrastructure of the state infor-

[4] Despite different representations for the notion of „information society" it is commonly accepted that it is the society intensively using the information as a component of economic, social, cultural and political life. As M. Luterek, *E-government*. Systems of public information, Warsaw 2010, p. 12 and following. See also on the representations of this notion M. Gołka, What the Information Society Is?, Legislative, Economic and Sociologic Movement, year LXVII - notebook 4 – 2005, p. 253 and following.

[1] Pomimo różnych ujęć pojęcia „społeczeństwo informacyjne" powszechnie przyjmuje się, że jest to społeczeństwo, w którym informacja jest intensywnie wykorzystywana jako element życia ekonomicznego, społecznego, kulturowego i politycznego. Tak M. Luterek, *E-government*. Systemy informacji publicznej, Warszawa 2010, s. 12 i n. Zob. też na temat ujęć tego pojęcia M. Gołka, Czym jest społeczeństwo informacyjne?, Ruch Prawniczy, Ekonomiczny i Socjologiczny rok LXVII - zeszyt 4 – 2005, s. 253 i n.

[2] Szerzej na temat Strategii Lizbońskiej zob. E. Okoń-Horodyńska, Strategia Lizbońska – założenia programu rozwoju innowacyjnej Europy? [w:] E. Okoń-Horodyńska (red.), K. Piech (red.), STRATEGIA LIZBOŃSKA a możliwości budowania gospodarki opartej na wiedzy w Polsce – wnioski i rekomendacje, Warszawa 2005, s. 11 - 22. Zob. też A. Hołda-Wydrzyńska, Cyfrowo wykluczeni, czyli problem dostosowania stron internetowych administracji publicznej do standardów dostępności, Niepełnosprawność – zagadnienia, problemy, rozwiązania nr 1/2013 (6), s. 57.

[3] Szerzej zob. M. Baran, M. Flankowski, Przegląd systemów *e-Government* w wybranych krajach, *Humanities and Social Sciences HSS*, vol. XIX, 21 (2/2014), pp.9-23 *April – June*, s. 10 i n.

[5] Wider see on the subject of Lisbon Strategy at E. Okoń-Horodyńska, Lisbon Strategy – program assumptions for development of innovative Europe? [w:] E. Okoń-Horodyńska (red.), K. Piech (red.), LISBON STRATEGY and possibilities for building the economy based on the knowledge in Poland – conclusions and recommendations, Warsaw 2005, p. 11 - 22. See also A. Hołda-Wydrzyńska, Digitally excluded, or the question of adaptation of public administration internet sites to the standards of accessibility, Disability – questions and solutions, nr 1/2013 (6), p. 57.

Na przestrzeni ostatniego dwudziestolecia znacznie - a pokusić się można nawet o twierdzenie, że drastycznie - zmieniła się infrastruktura bezpieczeństwa informacyjnego państwa w kierunku infrastruktury zbudowanej na nowych technologiach informacyjno-komunikacyjnych. Za sprawą tych technologii dane przetwarzane i przekazywane są już w postaci elektronicznej, a technologia ta wypiera tradycyjne metody przetwarzania „papierowych" danych i ich transfer w postaci „papierowej".

Te ostatnie odchodzą już w zapomnienie i stają się reliktem zamierzchłej przeszłości. Tym technologicznym przeobrażeniom towarzyszą jednocześnie nowe zagrożenia dla bezpieczeństwa informacyjnego państwa, zwłaszcza w wymiarze technologicznym, a także zmiana roli danych (informacji wedle normatywnej nomenklatury). W konsekwencji wskazywanych zmian zaistniała potrzeba przyjęcia zupełnie innych warunków, mechanizmów i procedur bezpieczeństwa „technologicznego" danych i „infrastruktury informacyjnej" państwa. Niezbędne stało się ustanowienie odpowiednich regulacji prawnych normujących standardy bezpieczeństwa informacyjnego państwa we wszystkich jego wymiarach, a zwłaszcza dla kluczowych jego elementów: elektronicznych baz danych oraz infrastruktury informacyjno-komunikacyjnej, co oczywiste adekwatnych do poszczególnych elementów tej infrastruktury.

Przyjmowane niegdyś podejście do bezpieczeństwa informacyjnego państwa, a także dotychczas używana różnorodna i niekonsekwentnie terminologia w sferze bezpieczeństwa informacyjnego państwa wymaga zatem rewizji. W tej mierze rozważenia wymaga wprowadzenie do języka prawniczego, a także do obrotu prawnego, pojęcia „infrastruktura informacyjno-komunikacyjna" dla zasygnalizowania zaistniałych w tej sferze zmian technologicznych oraz uwypuklenia istoty czy natury nowej technologii. Konsekwentnie uzasadniona jest następnie próba zdefiniowania tego pojęcia

mation security has changed significantly, or even dramatically, for the last two decades towards an infrastructure based on new information-communication technologies. Due to these technologies the data has been already processed and transmitted in an electronic form, and the technology drives out traditional methods of "paper" data processing and transferring.

The last ones become negligent and relic of the past. These technological transformations are accompanied at the same time by new threats for the state information security, especially in technological aspects, and by the change of meaning of the data (information according to standard terminology). In consequence of the mentioned changes, a need has appeared for acceptation of completely new conditions, mechanisms, and procedures for "technological" safety of data and state "information infrastructure". It was necessary to settle relevant legal regulations, normalising standards of state information security in all its aspects, and especially for its key components: electronic data bases and information-communication infrastructure, obviously in forms adequate to particular components of the infrastructure.

Therefore, both the former approach to the state information security and the various and inconsequential terminology used up to now in domain of the state information security have to be revised. In this domain, the introduction of notion of "the information-communication infrastructure" into the legal language, and also to the legal circulation, has to be considered to signal technological changes which have occurred in this domain, and to stress the essence, or the nature, of the new technology. And consequently an attempt can be justified for preparing a definition of this notion and determination of its correlation to the

[6] Wider see M. Baran, M. Flankowski, Review of systems *e-Government* in selected countries, *Humanities and Social Sciences HSS*, vol. XIX, 21 (2/2014), pp.9-23 *April – June*, p. 10 and following.

oraz określenie jego korelacji do pojęcia „bezpieczeństwa informacyjnego państwa", które również nie doczekało się na gruncie rodzimej nauki jednoznacznej wykładni. Nie można też pominąć w badaniach i analizie wpływu nowej technologii ICT na funkcjonowanie współczesnych państw, w tym w obszarze bezpieczeństwa informacyjnego. Rozważenia wymagają wreszcie – będące naturalną konsekwencją zasygnalizowanego wcześniej obszaru badawczego - normatywne standardy i wymagania bezpieczeństwa infrastruktury informacyjno-komunikacyjnej, w tym poziom tego bezpieczeństwa. W tym kontekście nie obędzie się również bez analizy zagrożeń dla bezpieczeństwa tej infrastruktury i ich rodzajów, wreszcie zaś oceny aktualnego stanu regulacji prawnej i doktryny w zakresie bezpieczeństwa infrastruktury informacyjno-komunikacyjnej. Nurtujące wreszcie są czynniki wpływające na bezpieczeństwo infrastruktury.

2. Pojęcie bezpieczeństwo informacyjne państwa a jego wymiary

Bezpieczeństwo informacyjne państwa współcześnie, tym bardziej wobec ostatnich doświadczeń napaści Federacji Rosyjskiej na Ukrainę oraz toczącej się na oczach społeczności międzynarodowej okrutnej w metodach i działaniach wojny militarnej i informacyjnej, odgrywa kluczową rolę wśród podsystemów bezpieczeństwa narodowego, a konkretnie podsystemów wykonawczych (podsystemów ochronnych)[7]. Ma ono bowiem ścisły związek z bezpieczeństwem wewnętrznym i zewnętrznym państwa i – co istotniejsze - jest wszechobecne we wszystkich działaniach współczesnego państwa i społeczeństwa. Jednakże termin bezpieczeństwo informacyjne państwa nie ma charakteru normatywnego, nie występuje też w obecnie obowiązującej Strategii Bezpieczeń-

notion of "the state information security", which has also failed to get a clear interpretation of homeland scientists. Moreover, the influence of the new ICT on the functionality of existing states, including also the domain of information security, cannot be neglected. Finally the normative standards and requirements of security of information-communication infrastructure, including the level of this security, have to be also considered as a consequence of the investigation area indicated earlier. Regarding it, the analysis of threats for the safety of this infrastructure, and their categories, is necessary together with evaluation of the present state of legal regulations and doctrine over the security of information-communication infrastructure. Moreover, the factors affecting the security of infrastructure are also important.

2. Notion of State Information Security and Its Aspects

State information security has now a key meaning for the national security subsystems, and specifically for executing subsystems (protective subsystems)[26], especially in confrontation with recent experiences of invasion of the Russian Federation on Ukraine and the military and information war, cruel in methods and operations, which is waged before the international society. It is directly connected with the state internal and external security, and what's more, it is present in all activities of the modern state and society. But the term of the state information security has not any normative character, and is not present in the National Security Strategy of the Republic of Poland[27], which is currently bind-

[7] Szerzej na temat podsystemów bezpieczeństwa narodowego zob. W. Kitler, Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe, Toruń 2018, s. 328 i n., a zwłaszcza s. 459 i n.

stwa Narodowego Rzeczypospolitej Polskiej[8], która operuje sformułowaniem „przestrzeń informacyjna", wskazując jednocześnie zakładane cele, które należy w tej przestrzeni osiągnąć, również w wymiarze technologicznym. Natomiast w poprzednio funkcjonującej w obrocie prawnym doktrynie bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej uznawane było ono – wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo - za jeden z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, mający charakter transektorowy i wpływający na efektywność funkcjonowania całego systemu bezpieczeństwa[9]. Nawiązując do tej definicji przyjąć należy oczywisty obecnie fakt, iż obejmuje ono przecież swoim zakresem przedmiotowym kluczowe dla efektywnego i prawidłowego funkcjonowania państwa dane (informacje), których nieuprawnione ujawnienie może spowodować poważne zagrożenie dla funkcjonowania całego systemu bezpieczeństwa, a uczynienie z nich niewłaściwego użytku może także wpłynąć na wizerunek państwa i w konsekwencji może utrudnić realizowanie działań ważnych dla państwa i jego bezpieczeństwa. W. Kitler[10] podkreśla wręcz, że „określając strukturę Systemu Bezpieczeństwa Informacyjnego jako elementu systemu bezpieczeństwa narodowego, musimy wziąć pod uwagę", po pierwsze, że „informacja i związane z nią technologie, systemy i zasoby obejmują cały System Bezpieing, and both employs the formulation of "the information space" and indicates the assumed objectives which have to be met in this space, also in technological aspect. Nevertheless, in the information security doctrine of the Republic of Poland existing previously in the legal circulation it was recognised, with its integral part of the cybersecurity, as one of most vulnerable domains of national and international security having the trans-sectorial character and affecting the efficiency of the whole security system[28]. Regarding this definition one can agree with the fact, which is obvious now, that it encompasses in its subjective meaning the data (information) which is of key importance for an efficient and proper functionality of state, and which after an unauthorised disclosure may cause a serious threat for the functionality of the whole system of security, and which after improper use may also affect the state's image and may harm in consequence execution of tasks important for the state and its security. W. Kitler[29] stresses that „at identification of the structure for Information Security System as a component of the national security system we have to consider" first of all that „information and technologies, systems, and resources related to it encompass the whole System of National Security of the Republic of Poland (SBN RP)", and

[26] Wider about the national security subsystems see W. Kitler, Organisation of national security of the Republic of Poland. Aspects of social order, legislation-administration and system, Toruń 2018, p. 328 and following, and especially p. 459 and following.

[27] It is Strategy from 12 May, 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, accessed on 28 December, 2022. See Pillar I of the strategy, point 5, p. 21, and Pillar IV, especially point 6.3., p. 36.

[8] Jest to Strategia z dnia 12 maja 2020 r., https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, dostęp z dnia 28 grudnia 2022 r. Zob. Filar I strategii, pkt 5, s. 21 i Filar IV, zwłaszcza pkt 6.3., s. 36.

[9] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, pkt 85, oraz Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, s. 171-172.

[10] W. Kitler, Organizacja bezpieczeństwa …, s. 464/465. Projekt „Doktryna Bezpieczeństwa Informacyjnego RP", Warszawa 2015, pkt 1.

[28] Strategy of National Security of the Republic of Poland, Warsaw 2014, point 85, and White Book of the National Security of the Republic of Poland, Warsaw 2013, p. 171-172.

[29] W. Kitler, Organisation of security …, p. 464/465. Project „Doctrine of Information Security of the Republic of Poland", Warsaw, 2015, point 1.

czeństwa Narodowego RP (SBN RP)", a po drugie, że „jest to (…) dziedzina transdyscyplinarna, bo system kierowania oraz każdy system operacyjny i systemy wsparcia, z których składa się system bezpieczeństwa narodowego, zawiera w sobie elementy natury informacyjnej (we wszystkich tego wyrażenia przejawach) oraz jest silnie od nich uzależniony". Bezpieczeństwo informacyjne jest – jak też zauważa A. Żebrowski[11] - zawsze obecne w polityce bezpieczeństwa i obronności państwa, a „wszechobecna globalizacja, rozwój społeczeństwa informacyjnego i technologii telekomunikacyjnych zmieniły obecne środowisko bezpieczeństwa państw, w tym również Rzeczypospolitej Polskiej", „bezpieczeństwo będące procesem należy budować, tzn. dostosowywać istniejący system bezpieczeństwa wewnętrznego i zewnętrznego do zmieniających się warunków w otoczeniu państwa, w tym trzeba realizować konsekwentnie określone zadania, które powinny zabezpieczać spokojny i równoważny rozwój w każdej sytuacji", „bezpieczeństwo narodowe państw jest coraz bardziej uzależnione od sprawności funkcjonowania infrastruktury informacyjnej (w tym infrastruktury teleinformatycznej). Jej załamanie może spowodować katastrofę, której rozmiar jest z każdym rokiem coraz większy. (…) załamanie się funkcjonowania infrastruktury informacyjnej (w tym infrastruktury teleinformatycznej) państwa doprowadziłoby do dezorganizacji funkcjonowania państwa i zagrożenia jego interesów na świecie".

Samo pojęcie „bezpieczeństwo informacyjne państwa", określane też jako „sfera informacyjna", jest charakteryzowane w różny sposób i analizowanie przez rodzimą naukę (różnych dyscyplin wiedzy) w wielu kontekstach[12]. Wielość tych kontekstów znajduje od-

secondly that „it is (…) a transdisciplinary domain as a management system, and each operation system and supporting systems creating the national security system includes in itself the components of informative nature (in all varieties of this expression) and strongly depends on them". The informative security, as it is also noted by A. Żebrowski[30], is always present in the state's policy of security and defence, and „omnipresent globalisation, development of informative society and telecommunication technologies have changed the present security environment of states including also the Republic of Poland", and „the security is a process which has to be constructed, i.e. the existing system of internal and external security has to be adapted to changed conditions surrounding the state, and the specific assignments have to be performed consequently to secure a steady and balanced development at each circumstances", when the „national security of states depends at greater degree on the efficient functionality of information infrastructure (including tele-information infrastructure). Any failure of it can cause a disaster on the scale which increases every year. (…) failure of functionality of state information infrastructure (including tele-information infrastructure) could cause disorganisation of state functionality and could threaten its interests on the world".

The mere notion of „state information security" is also determined as „information domain" and is characterised in different ways when analysed by the homeland science (various disciplines of science) in many aspects[31]. The number of these aspects reflects its different ways of definitions[32].

[11] A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kolegium Analiz Ekonomicznych nr 29/2013, s. 452 i 450 oraz 453/454 i powołana tam literatura.

[12] G. Klein, Bezpieczeństwo informacyjne RP w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej – perspektywa teoretyczna, Studia Wschodnioeuropejskie 11/2019, s. 17. Autor ten wskazuje na piętnaście kategorii kontekstów badań rodzimej nauki nad bezpieczeństwem informacyjnym: [„komponent bezpieczeństwa narodowego, komponent kultury bezpieczeństwa, komponent kultury informacyjnej, komponent ekologii informacji, bezpieczeństwo w dobie globalizacji i społeczeństwa informacyjnego, element mię-

zwierciedlenie w różnorodności sposobów jego definiowania[13]. Z tego względu ich wszystkich nie sposób zaprezentować w tego rodzaju, z natury swojej wąskim, opracowaniu, a mającym przecież za wiodący nurt rozważań warstwę technologiczną sfery informacyjnej państwa i bezpieczeństwo tej warstwy, w tym kluczową dla tych rozważań próbę jej zdefiniowania. Bezpieczeństwo informacyjne państwa w całej jego rozciągłości różnych aspektów nie jest więc istotą prowadzonych rozważań, a odniesienie się do przykładowych jego definicji ma na celu jedynie ukazanie – poza tą różnorodnością - umiejscowienia infrastruktury informacyjno-komunikacyjnej państwa w szerszym pojęciu bezpieczeństwa informacyjnego, jak i zwrócenie uwagi na niezwykłą zawiłość i skomplikowanie sfery informacyjnej państwa (tak ważnej dla bezpieczeństwa państwa postrzeganego *sensu largo*).

Wedle jednej z reprezentatywnych definicji, którą formułuje W. Kitler[14], „sferę infor-

For this reason it is not possible to present all of them in the article of a limited volume which by the way is focused on considerations of technological issues of the state information domain and on the security of this domain, including an attempt to define it, what is a question of key importance for these considerations. The state information security in its wide spectrum of aspects is not then a main question of performed considerations and the reference to its exemplary definitions is only aimed to show, beyond its variety, the position of the state information-communication infrastructure in the wider notion of information security, and to stress high complexity of the information domain of the state (so important to state security in general).

According to one of representative definitions formulated by W. Kitler[33], „the information domain may be identified as an activity of communication between various

dzynarodowej i lokalnej polityki informacyjnej, cel polityki bezpieczeństwa informacyjnego, przedmiot technologii informatyczno-komunikacyjnych (infrastruktura teleinformatyczna – obsługa i eksploatacja), równoznacznik bezpieczeństwa informacji i ochrony danych, proces zarządzania bezpieczeństwem informacji (organizacja audytu informacji), obszar wpływu manipulacji medialnej przez środki masowego przekazu, wyznacznik organizacji i jej kultury organizacyjnej, przedmiot walki konkurencyjnej i biznesowej (gospodarka elektroniczna), element walki informacyjnej (przedmiot wojny informacyjnej, cyberwojny), część edukacji dla bezpieczeństwa"].

[30] A. Żebrowski, Information security of Poland and information fight, Annals of Economic Studies Board nr 29/2013, p. 452 and 450, and 453/454 and literature called there.

[31] G. Klein, Information security of the Republic of Poland in the context of the East-European threats in the information space – theoretical perspective, East-European Studies 11/2019, p. 17. Author points out eleven categories of researching contexts for the homeland science over the information security: [„component of national security, component of security culture, component of information ecology, security in times of globalisation and information society, component of international and local information policy, objective of information security policy, subject of information-communication technologies (tele-informative infrastructure – handling and use), equivalent of information security and data protection, security information governing process (organisation of information audit), area of influence for media manipulation by the mass media communication, determinant of an organisation and its organisational culture, subject of business competition (electronic economy), component of informative competition (subject of information warfare, cyberwar), security education sector"].

[32] These definitions are reviewed for instance by T. Aleksandrowicz. See. T. Aleksandrowicz, State information security, Political Studies 2018, notebook 49, p. 41 and following.

[13] Przeglądu tych definicji dokonuje przykładowo T. Aleksandrowicz. Zob. T. Aleksandrowicz, Bezpieczeństwo informacyjne państwa, Studia Politologiczne 2018, z. 49, s. 41 i n.

[14] W. Kitler, Organizacja bezpieczeństwa …, s. 459 oraz W. Kitler, Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne [w:] W. Kitler (red.), J. Taczkowska-Olszewska (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017, s. 31.

[33] W. Kitler, Organisation of security …, p. 459, and W. Kitler, Notion and range of the state information security, definition and systematic settlings[w:] W. Kitler (red.), J. Taczkowska-Olszewska (red.), Security of information. Administration-legal aspects, Warszawa 2017, p. 31.

macyjną określać można jako aktywność w zakresie komunikowania się różnych podmiotów (ludzi, organizacji) ze sobą, poznawania świata rzeczywistego i abstrakcyjnego, a także zbiór podmiotów przekazujących i odbierających informacje oraz narzędzi (urządzeń, sieci, systemów, baz, zbiorów) ich zbierania, gromadzenia, przechowywania oraz nośników i przetworników sygnałów służących tejże działalności". Dla P. Potejki[15] z kolei „bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem". Natomiast A. Żebrowski[16], odwołując się do formułowanych licznie w doktrynie definicji, zwraca uwagę na inne ujęcie tego pojęcia, wedle którego „bezpieczeństwo informacyjne dotyczy zagwarantowania sobie przez dany podmiot (np. państwo) integralności, kompletności oraz wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko elektronicznej. Odnosi się więc zarówno do wszelkiego rodzaju wysiłków, służących ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów)". Szeroko ujmując pojęcie bezpieczeństwa informacyjnego państwa, T. Aleksandrowicz[17] stwierdza zaś, że „jego zakres przedmiotowy obejmuje zdolność do po-

subjects (people, organisations), recognition of real and abstractive worlds, and collection of subjects transferring and receiving the information, and tools (instruments, networks, systems, bases, stores) for its collection, accumulation, storing, and the carriers and converters of signals used for these activities". In the next turn, for P. Potejko[34] „the information security is a collection of activities, methods, and procedures undertaken by the authorised subjects aimed to secure the integrity of collected, stored, and processed information resources by protecting them against unwanted, and unauthorised disclosure, modification, or destruction. On the other hand, A. Żebrowski[35] referring to numerous definitions formulated in the doctrine pays the attention to another perception of this notion saying that "the information security refers to warranting by a given subject (e.g. the state) for itself the integrity, and completeness, and the reliability of possessed information resources in every form, not exclusively electronic one. It refers then both to all types of efforts servicing to protection of possessed information, important in the context of security (therefore having influence into efficient functionality of state structures and the society), and to provision of information supremacy by getting new, or the newest data, and disinformation actions against possible enemies (states and other subjects)". T. Aleksandrowicz[36] considers the notion of state information security in wide perspective claiming that „its subjective scope encompasses capacities for acquisition of information, for its analyses, distribution, and protection of owned

[15] P. Potejko, Bezpieczeństwo informacyjne [w:] K. A. Wojtaszczyk (red.), A. Materska-Sosnowska (red.), Bezpieczeństwo państwa, Warszawa 2009, s. 194.
[16] A. Żebrowski, op. cit., s. 452.
[17] T. Aleksandrowicz, op. cit., s. 48.
[34] P. Potejko, Security of information [w:] K. A. Wojtaszczyk (red.), A. Materska-Sosnowska (red.), State security, Warsaw 2009, p. 194.
[35] A. Żebrowski, op. cit., s. 452.
[36] T. Aleksandrowicz, op. cit., p. 48.

zyskiwania informacji, jej analizowania, dystrybucji, ochrony własnych zasobów informacyjnych, a także zdolności do identyfikowania i skutecznego przeciwdziałania skutkom wrogich operacji informacyjnych mających na celu uzyskanie wpływu na politykę państwa, nastroje społeczne etc.". Swoistą, bo akcentującą materialny i proceduralny charakter, definicję bezpieczeństwa informacyjnego formułuje J. Taczkowska-Olszewska[18], która przyjmuje, że w tym pierwszym ujęciu „bezpieczeństwo informacyjne może być definiowane jako dobro prawne, które wymaga indywidualnej tj. odrębnej w stosunku do innych dóbr prawnie chronionych, ochrony prawnej", zaś w tym drugim ujęciu „stanowić będzie dyrektywę działania, a w konsekwencji normę kompetencyjną upoważniającą określone rodzaje organów państwa do podejmowania czynności kształtujących sytuację prawną innych podmiotów w sferze ich praw i obowiązków w zakresie utrzymania lub osiągnięcia stanu bezpieczeństwa a także przeciwdziałania zagrożeniom".

W oparciu o te, jedynie przykładowo przytoczone, doktrynalne ujęcia bezpieczeństwa informacyjnego państwa można już przyjąć, że ma ono wiele wymiarów: organizacyjno-ustrojowy, technologiczny, procesowy oraz materialny, a także ludzki (osobowy)[19]. Podzielając w pełni pogląd W. Kitlera[20] stwierdzić więc trzeba, że „sfera informacyjna ma niejako

information resources, and also capacities for identifying and counteracting the effects of hostile informative operations aimed to affect the state policy and social opinions, etc.". A specific definition of the information security, stressing its material and procedural character, is formulated by J. Taczkowska-Olszewska[37] who assumes that in the first outlook „the information security can be defined as a legal right which requires an individual legal protection, i.e. separated against other legally protected rights", whereas in the second approach „it will constitute an operational directive, and in consequence a competence norm entitling the specific types of state institutions for undertaking activities shaping the legal situation of other subjects in the field of their rights and obligations for maintaining or achieving the level of security, and counteracting the threats, as well".

Basing on the above, only exemplary, doctrinal formulations of the state information security, it can be just accepted that it has many aspects: organisational-political, technological, procedural, and material, and human (personal), as well[38]. And when sharing the opinion of W. Kitlera[39] in full extension, it can be stated that „the information domain has a dual meaning, as in the first hand it refers to positive or negative cooperation between people, and on the

[18] J. Taczkowska-Olszewska, Bezpieczeństwo informacyjne jako kategoria prawna. Ujęcie teoretyczne [w:] W. Kitler (red.), J. Taczkowska-Olszewska (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017, s. 47.

[19] Ujmując to nieco inaczej daje się wyróżnić cztery aspekty bezpieczeństwa informacyjnego: informacje, w tym informacje niejawne o podwyższonym poziomie ochrony (elementy informacyjne, bazy wiedzy), technologie informacyjno-komunikacyjne (narzędzia telematyczne), procedury organizacyjne (procedury korzystania z systemu teleinformatycznego, jak instrukcje) oraz zasoby ludzkie, integralnie związany z pozostałymi elementami bezpieczeństwa informacyjnego państwa.

[20] W. Kitler, Organizacja bezpieczeństwa …, s. 460.

[37] J. Taczkowska-Olszewska, Information security as the legal category. Theoretical approach [w:] W. Kitler (red.), J. Taczkowska-Olszewska (red.), Information security. Legal-administration aspects, Warsaw, 2017, p. 47.

[38] Looking at it on a bit different way four aspects of information security can be distinguished: information, including classified information at higher level of protection (information components, data bases), information-communication technologies (telematic tools), organisational procedures (procedures for using tele-informative system, such as instructions), and human resources, integrally connected with the remaining components of the state information security.

[39] W. Kitler, Organisation of security …, p. 460.

dwojakie oblicze, raz dotyczy pozytywnej lub negatywnej kooperacji między ludźmi, innym zaś razem techniczno-organizacyjnej strony zapewnienia tychże kooperacji", lecz zasadniczą kategorią bezpieczeństwa informacyjnego jest informacja. Istotnie bowiem zarówno prawodawca, jak i praktyka prawnicza, w tym judykatura, największą uwagę poświęca ochronie danych (informacji publicznej), w tym jej szczególnej kategorii – informacji niejawnych. Nie oznacza to jednak, że prawodawca w ogóle nie dostrzega potrzeby zapewnienia bezpieczeństwa technologicznego narzędziom informacyjno – komunikacyjnym oraz przyjęcia określonych wymagań i standardów dla tego bezpieczeństwa. Szybki rozwój nowych technologii ICT od czasu przyjęcia idei *e-Europa* 2000 oraz szerokie zastosowanie tych technologii w sektorze publicznym do realizacji zadań państwa i świadczenia usług publicznych *on-line* w coraz większym zakresie niejako wymusił bowiem przyjęcie i w tym zakresie odpowiednich regulacji na gruncie unijnego i rodzimego prawa[21].

Wielowymiarowość sfery informacyjnej państwa plasuje ją jako jedno z najbardziej interdyscyplinarnych, a jednocześnie szczególnie złożonych i wieloaspektowych, lecz ważkich, other hand to technical-organisational questions of securing such cooperations", but the substantial category of information security is the information. As a matter of fact, both the legislator and the legal practice, including jurisdiction, pay the greatest attention to protection of data (public information), including its specific category – classified information. Nevertheless, it does not mean that the legislator does not see any need for provision of technological security for the information-communication tools and acceptation of specific requirements and standards for this security. Rapid development of new ICT after acceptation of the idea of *e-Europa* 2000 and wide application of these technologies in the public sector for execution of state assignments and rendition of public *on-line* services at increased extension has enforced in certain degree the acceptation of relevant regulations in this matter on the basis of the union and homeland legislation[40].

Multidimensional aspect of state information domain places it as a one of the most interdisciplinary, and at the same time particularly complex and multilateral, but important domains of state activity. Securi-

[21] Prawo normuje różne aspekty bezpieczeństwa technologii ICT, jak przykładowo: usługi łączności elektronicznej, publiczna sieć łączności elektronicznej, bezpieczeństwo sieci i systemów informatycznych oraz usług, krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych, interoperacyjność usług czy w ogóle interoperacyjność, szkodliwe zakłócenia czy „Krajowe Ramy Interoperacyjności". Zob. np. art. 2 pkt 4, pkt 8 i pkt 21 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (wersja przekształcona), Dz.U.UE.L.2018.321.36 z dnia 2018.12.17, zwanej dyrektywą 2018/1972, czy art. 4 pkt 2 i pkt 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U.UE.L.2016.194.1 z dnia 2016.07.19, zwanej dyrektywą 2016/1144, art. 2 pkt 13 i pkt 40a prawa telekomunikacyjnego czy art. 3 pkt 18 i pkt 21 ustawy o informatyzacji podmiotów publicznych.

[40] The law normalises different aspects of the ICT, as for instance: electronic communication services, public network of electronic communication, security of networks and informative systems and services, homeland strategy on security of networks and informative systems, interoperability of services, or even interoperability at all, harmful disturbances or „Homeland Frames of Interoperability". See for instance art. 2, point 4, and 8, and 21 of Directive of the European Parliament and Council (EU) 2018/1972 from 11 December, 2018, establishing the European code of electronic communication (version reprocessed), Law Monitor of EU.L.2018.321.36 from 2018.12.17, named as Directive 2018/1972, or art. 4, point 2, and 3 of Directive of the European Parliament and Council (EU) 2016/1148 dated on 06 July, 2016 on assets for a high common level of security of networks and informative systems on the Union territory, Law Monitor of EU.L.2016.194.1 from 2016.07.19, named as Directive 2016/1144, art. 2, point 13, and 40a of telecommunication law, or art. 3, point 18, and 21 of the Act on informatisation of public subjects.

obszarów działania państwa. Bezpieczeństwo infrastruktury informacyjno-komunikacyjnej państwa jest też w efekcie węższym pojęciem niż bezpieczeństwo informacyjne państwa, gdyż mieści się w zakresie tego ostatniego. Infrastruktura – równie ważna dla bezpieczeństwa państwa, choć odgrywająca drugorzędną (pomocniczą, posiłkową) rolę w stosunku do informacji (danych) - jest jednym z elementów bezpieczeństwa informacyjnego państwa. Doktryna przyjmuje, że bezpieczeństwo teleinformatyczne odnosi się do tych form wymiany, przechowywania i przetwarzania informacji, ograniczonych do technicznych środków łączności (telefony stacjonarne i komórkowe, radiostacje, sieci i systemy komputerowe, itp.); bezpieczeństwo teleinformatyczne dotyczy informacji przesyłanych i przetwarzanych w sieciach i systemach teleinformatycznych[22]. Tak też technologiczny aspekt bezpieczeństwa informacyjnego państwa postrzega prawodawca, który – definiując pojęcie „system informacyjny"[23] – wymienia obok systemu teleinformatycznego dane w postaci elektronicznej przetwarzane w tym systemie; natomiast definiując pojęcia „system teleinformatyczny" czy „telekomunikacja"[24] wskazuje narzędzia, metody i sposoby przekazywania danych przy użyciu tych systemów (technologiczne narzędzia komunikowania się). W definicji pojęcia „Krajowy System Informatyczny (KSI)"[25] wręcz od-

ty of the state information-communication infrastructure is in effect a narrower notion than the state information security as it falls into the scope of the last one. The infrastructure – equally important for the state security but of secondary meaning (supportive, additional) in relation to the information (data) – is one of components of the state information security. Doctrine states that the tele-information security refers to these forms of information exchange, storing, and processing, limited to technical means of communication (stationary and mobile telephones, radio-transmitters, computer networks and systems, etc.); tele-information security refers to information transmitted and processed in tele-information networks and systems[41]. The legislator perceives the technological aspect of the state information security just in this way, and defines the notion of information system"[42] by listing beside the tele-information system the data in electronic form processed in this system; whereas at definition of the notion of „tele-information system", or "telecommunication"[43] indicates the tools, methods, and ways for transferring the data by using these systems (technological tools of communication). In definition of the "Homeland Information System (HIS)"[44] the legislator simply refers

[22] Zob. A. Myśko, E. Młodzik, Bezpieczeństwo informacji – dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833, Finanse, Rynki Finansowe, Ubezpieczenia nr 72 (2014), s. 109.

[23] Zob. art. 2 pkt 14 z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j.: Dz. U. z 2020 r. poz. 1369, zwanej ustawą o cyberbezpieczeństwie.

[24] Zob. np. art. 2 pkt 4 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego, t.j.: Dz. U. z 2021 r. poz. 268, zwanej ustawą o powiadamianiu ratunkowym, art. 2 pkt 3 z dnia 8 lipca 2002 r. o świadczeniu usług drogą elektroniczną, t.j.: Dz. U. z 2020 r. poz. 344, zwanej ustawą o świadczeniu usług drogą elektroniczną, czy art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j.: Dz. U. z 2021 r. poz. 2070, zwanej ustawą o informatyzacji działalności podmiotów publicznych oraz art. 2 pkt 42 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t.j.: Dz. U. z 2021 r. poz. 576, zwanej prawo telekomunikacyjne.

[25] Zob. art. 2 pkt 11 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym *Schengen* oraz Wizowym Systemie Informacyjnym, t.j.: Dz. U. z 2021 r. poz. 1041, zwanej ustawą o systemie informacyjnym.

[41] See A. Myśko, E. Młodzik, Security of information – dilemmas connected with obligations of internal audit in units of public finances sector, Scientific Notebooks of University of Szczecin nr 833, Finances, Financial Markets, Insurances nr 72 (2014), p. 109.

wołuje się do urządzeń, procedur przetwarzania informacji, oprogramowania oraz infrastruktury telekomunikacyjnej.

3. Doktrynalne ujęcia bezpieczeństwa informacyjnego państwa

Różne dyscypliny rodzimej nauki - z racji interdyscyplinarnego charakteru bezpieczeństwa informacyjnego państwa - zajmują się różnymi wymiarami tego bezpieczeństwa, niekiedy nawet kilkoma z nich. Nauki o bezpieczeństwie[45] rozważają najczęściej organizacyjno-ustrojowy wymiar bezpieczeństwa informacyjnego państwa oraz samą informację, nauki o zarządzaniu[46] – zarządzanie bezpieczeństwem informacji oraz audyt bezpieczeństwa informacji, zaś nauki o komunikowaniu społecznym[47] - kanały (medium) przekazywania informacji (kanały transmisyjne). Nauka informatyki[48] koncentruje się na infrastrukturze informatycznej i jej architekturze oraz standardach bezpieczeństwa poszczególnych jej technologicznych elementów i normach ujednolicających wymagania dla rozwiązań technologicznych. A nauka prawa administracyjnego[49], jako najbardziej właściwa spośród

to instruments and procedures of information processing, and to telecommunication software and infrastructure.

3. Doctrinal Definitions of State Information Security

Different disciplined of the homeland science deal with different dimensions of this security, sometimes with many of them, due to the fact of the interdisciplinary character of the state information security. The sciences on security[98] usually consider organisational-political dimension of the state information security and the mere information itself, the sciences on management[99] deal with the management of information security and the audits of information security, whereas the sciences on social communication[100] - with channels (media) of transferring the information (transmitting channels). The science on informatics[101] is focused on IT infrastructure and its architecture, and on security standards of its technological components, and standards normalising the requirements for technological solutions. And the science on administration legislation[102] as the most

[42] See art. 2, point 14 from 05 July, 2018 on homeland cybersecurity system, i.e.: Law Monitor from 2020, pos. 1369, named as the act on cybersecurity.

[43] See for instance art. 2, point 4 of the Act from 22 November, 2013 on the rescue alarming, i.e.: Law Monitor from 2021, pos. 268, named as the act on rescue alarming, art. 2, point 3 from 08 July, 2002 on rendering electronic services, i.e.: Law Monitor from 2020, pos. 344, named as the act on rendering electronic services, or art. 3, point 3 of the Act from 17 February, 2005 on informatisation of subjects conducting public activities, i.e.: Law Monitor from 2021, pos. 2070, named as the act on informatisation of activities of public subjects, and art. 2, point 42 of the Act from 16 July, 2004, telecommunication law, i.e.: Law Monitor from 2021, pos. 576, named as telecommunication law.

[44] See art. 2, point 11 of the Act from 24 August, 2007 on participation of the Republic of Poland in *Schengen* Information System and Visa Information System, i.e.: Law Monitor from 2021, pos. 1041, named as the act on information system.

[45] W. Kitler, Organizacja bezpieczeństwa …, s. 463 – 469.

[46] Zob. A. Myśko, E. Młodzik, op. cit., s. 107/108.

[47] G. Klein, op. cit., s. 16.

[48] Zob. np. M. Kuraś, System informacyjny a system informatyczny – co oprócz nazwy różni te dwa obiekty?, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie 2009, nr 770, s. 261 i n. czy D. Bogusz, Wymagania technologiczne dla bezpieczeństwa dla komercyjnych systemów teleinformatycznych, https://www.bbn.gov.pl/ download/1/1004/wymaganiatechnologiczne.pdf, s. 93 i n.

[49] Por. przykładowo K. Chałubińska-Jentkiewicz, M. Karpiuk Mirosław, Prawo nowych technologii. Wybrane zagadnienia, LEX 2015, dostęp Lex z dnia 20 lipca 2022 r., 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, dostęp z 14 lipca 2022 r., P. M. Sitniewski, Dostęp do informacji publicznej. Pytania i odpowiedzi, LEX 2014, dostęp Lex z dnia 22 lipca 2022 r., M. Ber-

nauk prawnych dla bezpieczeństwa informacyjnego państwa, najwięcej uwagi poświęca – czego dowodzą liczne opracowania naukowe – dostępie do informacji publicznej i ochronie tej informacji, w tym informacji niejawnych, oraz poszczególnym atrybutom bezpieczeństwa informacji, marginalnie i to na dość znacznym poziomie ogólności zajmuje się natomiast ochroną i bezpieczeństwem infrastruktury informacyjno-komunikacyjnej[50], a więc narzędziami telematycznymi, które służą do gromadzenia, przechowywania, przetwarzania i

relevant among the legislation sciences for the state information security pays the greatest attention - what is proved by numerous scientific publications - to the access to public information and protection of this information, including classified information, and to particular attributes of information security, and also marginally and substantially in general way to protection and security of information-communication infrastructure[103], i.e. the telematic tools used for information collection, storing, processing and transfer-

naczyk, Obowiązek bezwnioskowego udostępniania informacji publicznej, Oficyna 2008, Lex z dnia 22 lipca 2022 r., E. Darmorost, Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz, LexisNexis 2013, Lex z dnia 18 lipca 2022 r., A. Monarcha-Matlak, Obowiązki administracji w komunikacji elektronicznej, Oficyna 2008, Lex z dnia 14 lipca 2022 r., K. Świtała, Prawnoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych, PPP 2013/10/21-30, Lex z dnia 15 lipca 2022 r.

[98] W. Kitler, Organisation of security …, p. 463 – 469.

[99] See A. Myśko, E. Młodzik, op. cit., p. 107/108.

[100] G. Klein, op. cit., p. 16.

[101] See for instance M. Kuraś, Information and informative system – differences beyond the names, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie 2009, nr 770, p. 261 and following, or D. Bogusz, Technological requirements for security of commercial tele-informative systems, https://www.bbn.gov.pl/ download/1/1004/wymaganiatechnologiczne.pdf, p. 93 and following.

[102] Compare for instance K. Chałubińska-Jentkiewicz, M. Karpiuk Mirosław, Prawo nowych technologii. Wybrane zagadnienia, LEX 2015, accessed on 20 July, 2022, G. Szpor, K. Wojsyk, Tryb określenia minimalnych wymagań [w:] Cz. Martysz, G. Szpor, K. Wojsyk, the Act on informatisation of activities for subjects conducting public tasks. Komentarz, Wydanie II, Lex 2015, access on 14 July, 2022, P. M. Sitniewski, Dostęp do informacji publicznej. Pytania i odpowiedzi, LEX 2014, access Lex on 22 July, 2022, M. Bernaczyk, Obowiązek bezwnioskowego udostępniania informacji publicznej, Oficyna 2008, Lex on 22 July, 2022, E. Darmorost, Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz, LexisNexis 2013, Lex on 18 July, 2022, A. Monarcha-Matlak, Obowiązki administracji w komunikacji elektronicznej, Oficyna 2008, Lex on 14 July, 2022, K. Świtała, Prawnoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych, PPP 2013/10/21-30, Lex on 15 July, 2022.

[50] Zagadnienie bezpieczeństwa infrastruktury informacyjno – komunikacyjnej państwa na gruncie nauk prawnych, warunki bezpieczeństwa infrastruktury informacyjno-komunikacyjnej nie są przedmiotem kompleksowych i obszernych badań naukowych i analiz. Doktryna ta – pomijając incydentalne i bardzo ogólnikowe opracowania sprowadzające się zasadniczo do opisu stanu regulacji prawnej - zajmuje się natomiast i to w szerokim zakresie kontrolowanym dostępem do informacji publicznej i w tym kontekście ochroną tych informacji oraz informacji niejawnych. Zachwyt nad koncepcją „czystych rąk" i transparentności działania państwa oraz jego organów przesłonił przedstawicielom tej doktryny normatywne bezpieczeństwo infrastruktury informacyjno-komunikacyjnej państwa. Analiza tego obszaru bezpieczeństwa informacyjnego państwa – o ile jest on przedmiotem jakichkolwiek zainteresowania tej doktryny – ma charakter komentatorski do aktów normatywnych i to na dość ogólnym, lakonicznym poziomie rozważań.

[103] Question of state information-communication infrastructure security on the ground of legislation sciences, conditions of security for information-communication infrastructure are not a subject of comprehensive and extensive scientific investigations and studies. The doctrine – neglecting some incidental and of very general character elaborations focused essentially on description of the status over the legal regulations – deals instead, and in a large extension with a controlled access to the public information, and in this regard with the protection of such information and classified information, as well. Admiration over the concept of "clean hands" and transparency of activities of the state and its institutions has screened the normative security of the state information-communication infrastructure for representatives of this doctrine. Analysis of this domain of state information security – if it still is any subject of an interest for this doctrine – has a commentating character over normative acts, and on relatively general and superficial level of considerations.

przekazywania samej informacji.

W konsekwencji można w rodzimej nauce – bez względu na jej dziedzinę - odnaleźć różne ujęcia bezpieczeństwa informacyjnego państwa oraz różną terminologię dla określenia jej infrastruktury, choć – co wymaga podkreślenia – trzon tych ujęć w pewnej mierze bywa zbieżny, jeśli nie tożsamy. Rodzi to chaos terminologiczny i pojęciowy, zwłaszcza co do zakresu przedmiotowego tych pojęć i ich tożsamości. W publikacjach naukowych można zatem odnaleźć pojęcia takie jak: „bezpieczeństwo informatyczne" (a ściślej „bezpieczeństwo teleinformatyczne"), a w konsekwencji „infrastruktura informacyjna" (w tym infrastruktura teleinformatyczna") i „systemy informacyjnego komunikowania"/„system informatyczny" i „system teleinformatyczny"/ „systemy informacyjnego komunikowania"[51], a także „kanał przesyłania treści (informacji)" i „bezpieczeństwo kanału"[52], a ponadto „infrastruktura informacyjno-komunikacyjna"[53]. Nie często jednakże nauka formułuje ich definicje, ograniczając się raczej do wskazania ich korelacji do pojęcia bezpieczeństwa informacyjnego państwa. Niektórzy przedstawiciele nauki[54] formułują wręcz tezę badawczą i wyrażają przekonanie, że pojęcia: „system informatyczny" i „system teleinformatyczny" należy traktować jako synonimy, zapominając, że mają one różne zakresy znaczeniowe. Inni[55] z kolei błędnie przyjmują, że „bezpieczeństwo informatyczne" jest precyzyjnej wyrażonym pojęciem „bezpieczeństwo teleinformatyczne", podczas gdy z technologicznego punktu widzenia i nauki o nowoczesnej technologii nie są to pojęcia tożsame, to pierwsze jest wszak węższe niż to drugie. Przedstawiciele nauki informatyki[56] z kolei podnoszą, że „w ślad za

ring.

In consequence the homeland science – independently of its discipline – represents different perceptions of the state information security and different terminology describing its infrastructure, even if – what has to be stressed – the essence of these perceptions is similar, if not identical, in some degree. It brings a chaos in terminology and notions, especially on the subjective extension of these notions and their identities. Scientific publications can include then such notions as: „informatics security" (precisely „tele-informative security"), and in consequence „information infrastructure" (including "tele-informative infrastructure") and "systems of informative communication"/„informative system" and „tele-informative system"/ „systems of information communication"[104], and also "a channel for transferring the news (information)" and „channel's security"[105], and moreover „information-communication infrastructure"[106]. But the science formulates their definitions not in every case, and instead restrains rather to indicate their correlations with the notion of the state information security. Some representatives of science[107] have been just formulating a researching thesis and expressing the conviction that the notions: „informative system" and „tele-informative system" have to be treated as synonyms forgetting that they have different scopes of meaning. The others[108] on the other hand accept mistakenly that „informative security" is a „tele-informative security" expressed in more precise way, whereas from the technological point of view, and the science on new technologies, they are not identical notions, as the first one is a narrower one than the sec-

[51] Zob. A. Żebrowski, op. cit., s. 452 - 456 oraz 461 i podana tam literatura, czy A. Myśko, E. Młodzik, op. cit., s. 109 i 110.
[52] G. Klein, op. cit., s. 16.
[53] Tak J. Orłowska, „Baltophobia", czyli wojna informacyjna Rosji w państwach bałtyckich, Refleksje nr 22/2020, s. 88, oraz A. Hołda – Wydrzyńska, op. cit., s. 58.
[54] Tak A. Myśko, E. Młodzik, op. cit., s. 109.
[55] A. Żebrowski, op. cit., s. 452.
[56] Zauważa to M. Kuraś, choć kontestuje ten pogląd. Zob. M. Kuraś, op. cit., s. 260.

rozprzestrzenianiem nowych technologii na miejsce pojęcia system informacyjny (SI) pojawiło się nowe «system informatyczny» (SIt)". W literaturze można też odnaleźć pogląd, wedle którego system teleinformatyczny – ze względu na znaczny postęp technologiczny – ułatwia działanie systemu informatycznego, bowiem poszerza go o transmisję danych za pomocą elektronicznej sieci komunikacyjnej[57]. Normodawca również nie jest konsekwentny w tym zakresie, bowiem – poza szerszym zakresowo (bo obejmującym bazy danych i infrastrukturę) pojęciem „system informacyjny"[58] - posługuje się dwoma zasadniczymi pojęciami: „system teleinformatyczny"[59] lub „(inny) systemy łączności"[60] oraz „system informatyczny" (niekiedy sieć informatyczna")[61], choć niekiedy także pojęciem

ond. Representatives of science on IT[109] have been raising on the other hand a question that „following the spreading of new technologies the notion of the information system (InS) was replaced by a new notion of «informative system» (IeS)". In literature, an opinion can be also found that tele-informative system – due to significant technological progress – facilitates the operation of informative system through extending it by data transmission with electronic communication network[110]. The legislator is also not consequent in this matter as beyond a wider meaning (including data bases and infrastructure) of the notion of „information system"[111] – it uses two fundamental notions: „tele-informative system"[112], or „(other ones) communication systems"[113] and „informative system" (some-

[104] See A. Żebrowski, op. cit., p. 452 - 456 and 461 and attached literature, or A. Myśko, E. Młodzik, op. cit., p. 109 and 110.
[105] G. Klein, op. cit., p. 16.
[106] As J. Orłowska, „Baltophobia", or the Russia's information war in Baltic states, Refleksje nr 22/2020, p. 88, and A. Hołda – Wydrzyńska, op. cit., p. 58.
[107] As A. Myśko, E. Młodzik, op. cit., p. 109.
[108] A. Żebrowski, op. cit., p. 452.

[57] Zob. A. Myśko, E. Młodzik, op. cit., s. 110.

[58] Zob. np. art. 1 czy art. 3 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, t.j.: Dz. U. z 2021 r. poz. 666, zwanej ustawą o systemie informacji w ochronie zdrowia czy art. 1 ustawy o systemie informacyjnym; art. 2 pkt 4 i pkt 11 ustawy o cyberbezpieczeństwie.

[59] Zob. np. art. 5 pkt 2a ustawy z dnia 24 maja 202 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j.: Dz. U. z 2022 r. poz. 557; art. 6 ust. 1 czy art. 7 ustawy o systemie informacji o ochronie zdrowia; art. 3 pkt 3 ustawy o informatyzacji podmiotów publicznych; art. 2 pkt 3 ustawy o usługach elektronicznych; art. 2 pkt 4 ustawy o danych pasażera; art. 4 § 1 ustawy z dnia 17 listopada 1964 – Kodeks postępowania cywilnego, t.j.: Dz. U. z 2021 r. poz. 1805, zwanej k.p.c.; art. 2 pkt 4 ustawy o powiadamianiu ratunkowym; art. 2 pkt 14 ustawy o cyberbezpieczeństwa; art. 71aa i n. ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, t.j.: Dz. U. z 2022 r. poz. 1009; art. 5 pkt 32c ustawy z dnia 27 lipca 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, t.j.: Dz. U. z 2021 r. poz. 1285, art. 3 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, t.j.: Dz. U. z 2022 r. poz. 633, zwanej u.d.l.; art. 2 ust. 4 ustawy z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty, t.j.: Dz. U. z 2021 r. poz. 790, zwanej u.z.l.l.d.; art. 9 ust. 2 i ust. 4a ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, t.j.: Dz. U. z 2022 r. poz. 902; art. 2 pkt 6 i pkt 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j.: Dz. U. z 2019 r. poz. 742; art. 4a ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym, t.j.: Dz. U. z 2021 r. poz. 1709, art. 160a ustawy z dnia 23 lutego 2003 r. Prawo upadłościowe, t.j.: Dz. U. z 2020 r. poz. 1228.

[60] Np. art. 3 ust. 1 u.d.l. czy art. 2 ust. 4 u.z.l.l.d.

[61] Zob. np. rozdział 4c art. 28h i n. ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska, t.j.: Dz. U. z 2021 r. poz. 1070, zwanej u.i.ś.; art. 2 pkt 8 ustawy o cyberbezpieczeństwie; art. 2 pkt 2, art. 10 pkt 2 i pkt 3 czy art. 11 ustawy z dnia 14 lutego 2003 r. o przenoszeniu treści księgi wieczystej do struktury księgi wieczystej prowadzonej w systemie informatycznym, Dz. U. z 2003 r. nr 42 poz. 363, preambuła pkt 1 i pkt 3 oraz art. 1 ust. 1 czy art. 4 pkt 1 dyrektywy 2016/1148; art. 4 ustawy z dnia 2 kwietnia 2004 r. o systemie identyfikacji i rejestracji zwierząt, t.j.: Dz. U. z 2021 r. poz. 1542; art. 25 ust. 1 pkt 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, t.j.: Dz. U. z 2019 r. poz. 1781.

„sieć łączności elektronicznej”[62], „sieć telekomunikacyjna”[63], „sieć teleinformatyczna”[64], „krajowy system informatyczny”[65] oraz „infrastruktura telekomunikacyjna”[66] – zasadniczo wprowadzając jednocześnie ich legalną definicję, tym samym czyniąc wskazane już wątpliwości nauki pozbawionymi racji. W obrocie prawnym występuje też pojęcie „infrastruktury informacji przestrzennej”[67]. Najczęściej jednak prawo używa pierwszego pojęcia – „system teleinformatyczny”, a stosowane poprzednio na gruncie rodzimego prawa pojęcie „system informatyczny” coraz rzadziej występuje w aktach prawnych i jest stopniowo zastępowany określeniami adekwatnymi dla nowych technologii ICT, zasadniczo – z uwagi na rozpowszechnienie komunikacji informacyjnej na odległość – pojęciem „system teleinformatyczny”. To pierwsze zresztą jest – jak wynika

times informative network”)[114], but also rarely the notion „network of electronic communication”[115], „telecommunication network”[116], „tele-informative network”[117] „„homeland informative system”[118], and “telecommunication infrastructure”[119] – and actually introducing at the same time their legal definition and making by the same the indicated doubts unsubstantiated. In the legal circulation also exists the notion of “space information infrastructure”[120]. But the legislature usually employs the first notion – „teleinformative system”, and the notion of “informative system” which was previously used on the ground of the homeland law is now more rarely used in legal documents and is gradually replaced by terms which are adequate for new ICT, generally – due to the spreading of distant information communica-

[109] It is noticed by M. Kuraś, but it is contested, see M. Kuraś, op. cit., p. 260.
[110] See A. Myśko, E. Młodzik, op. cit., p. 110.
[111] See for instance art. 1, or 3 of the Act from 28 April, 2011 on the health care information system, i.e.: Law Monitor from 2021, pos. 666, named as the Act on the health care information system, or art. 1 of the Act on informative system; art. 2, point 4 and 11 of the Act on cybersecurity.
[112] See for instance art. 5, point 2a of the Act from 24 May, 2022 on the Internal Security Agency or the Intelligence Agency, i.e.: Law Monitor from 2022, pos. 557; art. 6, pos. 1, or art. 7 of the Act on the health care information system; art. 3, point 3 of the Act on informatisation of public subjects; art. 2, point 3 of the Act on electronic services; art. 2, point 4 of the Act on passenger’s data; art. 4, § 1 of the Act from 17 November, 1964 – Civil Code of Law Proceedings, i.e.: Law Monitor from 2021 pos. 1805, named as k.p.c. in Polish; art. 2, point 4 of the Act on rescue information; art. 2, point 14 of the Act on cybersecurity; art. 71aa and following of the Act from 13 October, 1998 on social insurance system, i.e. : Law Monitor from 2022, pos. 1009; art. 5, point 32c of the Act from 27 July, 2004 on provisions of health care financed from public assets, i.e.: Law Monitor from 2021, pos. 1285, art. 3, pos. 1 of the Act from 15 April, 2011 on medical treatment, i.e.: Law Monitor from 2022, pos. 633, named later u.d.l.; art. 2, pos. 4 of the Act from 05 December, 1996 on the occupation of doctor and dentist, i.e.: Law Monitor from 2021, pos. 790, named later as u.z.l.l.d.; art. 9, pos. 2, and 4a of the Act from 06 September, 2001 on the access to the public information, i.e.: Law Monitor from 2022, pos. 902; art. 2, point 6 and 9 of the Act from 05 August, 2010 on protection of classified information, i.e.: Law Monitor from 2019, pos. 742; art. 4a of the Act from 24 May, 2000 on the Homeland Penalty Record, i.e.: Law Monitor from 2021, pos. 1709, art. 160a of the Act from 23 February, 2003 on the Bankruptcy Law, i.e.: Law Monitor from 2020, pos. 1228.
[113] For instance art. 3, pos. 1 of u.d.l., or art. 2, pos. 4 of u.z.l.l.d.
[62] Zob. art. 1 pkt 1 i art. 2 pkt 1 dyrektywy 2018/1972.
[63] Zob. art. 2 pkt 35 prawa telekomunikacyjnego.
[64] Zob. art. 2 pkt 5 ustawy o powiadamianiu ratunkowym.
[65] Zob. np. art. 1 i art. 2 pkt 11 i pkt 14 czy art. 3 ust. 1 ustawy o systemie informacyjnym, oraz rozdział 10a, w tym art. 75a i n. ustawy z dnia 25 czerwca 1997 r. o cudzoziemcach, t.j.: Dz. U. z 2001 r. nr 127, poz. 1400, czy art. 2 pkt 4 ustawy z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera, t.j.: Dz. U. z 2019 r. poz. 1783, zwanej ustawa o danych pasażera.
[66] Zob. art. 2 pkt 11 ustawy o systemie informacyjnym, oraz art. 2 pkt 8 prawa telekomunikacyjnego.
[67] Zob. art. 1 czy art. 3 pkt 1 ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej, t.j.: Dz. U. z 2021 r. poz. 214, oraz pkt 6 motywów, art. 1 czy art. 3 pkt 1 dyrektywy nr 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE), Dz.U.UE.L. 2007.108.1 z dnia 2007.04.25.

z definicji przykładowo „Krajowego Systemu Informatycznego" czy samego pojęcia „system teleinformatyczny" - postrzegane przez rodzimego prawodawcę jako element tego ostatniego[68]. System informatyczny tradycyjnie, także na gruncie poprzednio obowiązującego prawa[69], jest kojarzony z systemem dedykowanym do przetwarzania danych przy użyciu urządzeń informatycznych i oprogramowania. Można więc pokusić się o tezę, że rozwój i upowszechnienie narzędzi telematycznych (technologii ICT), które umożliwiają zdalne przekazywanie danych w postaci cyfrowej (a więc przetwarzanych w systemie informatycznym), spowodowało pojawienie się nowego pojęcia „systemy teleinformatyczne". To pojęcie wchłonęło wcześniej stosowane systemy informatyczne do gromadzenia, przechowywania, przetwarzania i przekazywania danych cyfrowych, do których dodano nową wartość – możliwość zdalnego przekazywania elektronicznych danych przy użyciu ICT. Rodzimy prawodawca nie wprowadza jednakże – poza funkcjonującym już od wielu lat normatywtion – i.e. the notion of „tele-informative system". The first one is by the way – as it results for instance from definition of „Homeland Informative System", or the mere notion of „tele-informative system" – perceived by the homeland legislator as a component of the last one[121]. The informative system traditionally, and also on the ground of the previously binding law[122], is connected with a system dedicated for data processing with informative hardware and software. It can be then stated that development and spreading of telematic tools (ICT), which allow for remote transfer of data in digital form (and therefore processing in informative system), caused that the new notion of „tele-informative systems" came into existence. This notion has absorbed the earlier used informative systems for collecting, storing, processing and transferring digital data with the newly added value – possibility for distant transfer of electronic data by using ICT. The homeland legislator has not decided yet to introduce the notion of "tele-informative infrastructure", be-

[114] See for instance chapter 4c, art. 28h, and n. of the Act from 20 July, 1991 on the Environment Protection Agency, i.e.: Law Monitor from 2021, pos. 1070, named as u.i.ś.; art. 2, point 8 of the Act on cybersecurity; art. 2, point 2, art. 10, point 2 and 3, or art. 11 of the Act from 14 February, 2003 on transferring the mortgage book records to the structure of mortgage book kept in informatics system, Law Monitor from 2003, 42 pos. 363, preamble point 1 and 3, and art. 1, pos. 1, or art. 4, point 1 of Directive 2016/1148; art. 4 of the Act from 02 April, 2004 on the system for identification and registration of animals, i.e. : Law Monitor from 2021 pos. 1542; art. 25, pos. 1, point 3 of the Act from 10 May, 2018 on personal data protection, i.e.: Law Monitor from 2019, pos. 1781.

[115] See art. 1, point 1, and art. 2, point 1 of Directive 2018/1972.

[116] See art. 2, point 35 of telecommunication law.

[117] See art. 2, point 5 of the Act on rescue alarming.

[118] See for instance art. 1 and art. 2, point 11, and 14, or art. 3, pos. 1 of the Act on information system, and chapter 10a, including art. 75a and following of the Act from 25 June, 1997 on foreigners, i.e.: Law Monitor from 2001, nr 127, pos. 1400, or art. 2, point 4 of the Act from 09 May, 2018 on processing data for passenger's flight, i.e.: Law Monitor from 2019 pos. 1783, named as the Act on passenger's data.

[119] See art. 2, point 11 of the Act on the information system, and art. 2, point 8 of telecommunication law.

[120] See art. 1, and art. 3, point 1 of the Act from 4 March, 2010 about infrastructure of space information, i.e.: Law Monitor from 2021, pos. 214, and point 6 of motivations, art. 1, or art. 3, point 1 of Directive nr 2007/2/WE of the European Parliament and Council from 14 March, 2007 settling the infrastructure of the space information in the European Union (INSPIRE), Law Monitor of EU, 2007.108.1 from 2007.04.25.

[68] Zob. definicje tego pojęcia zawartą w art. 2 pkt 11 ustawy o systemie informacyjnym, art. 2 pkt 4 ustawy o systemie powiadamiania ratunkowego, art. 2 pkt 2 ustawy o usługach drogą elektroniczną i art. 3 pkt 3 ustawy o informatyzacji podmiotów publicznych.

[69] Zob. definicję systemu informatycznego zawartą w art. 7 pkt 2a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j.: Dz. U. z 2016 r. poz. 922, która została uchylona z dniem 6 lutego 2019 r. (na mocy art. 175 obecnie obowiązującej ustawy o ochronie danych osobowych z 2018 r.). Zgodnie z tym przepisem „systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych".

nym pojęciem „infrastruktura telekomunikacyjna”[70] - pojęcia „infrastruktura teleinformatyczna” ani też innego na określenie warstwy technologicznej bezpieczeństwa informacyjnego państwa. Prawodawca unijny zaś do definicji pojęcia „sieć łączności elektronicznej” wprowadza jedynie zwrot „infrastruktura” jako element definiujący tę sieć, a ściślej wymienione w jej definicji „systemy transmisyjne”[71]. Nie dodaje jednakże do pojęcia „infrastruktura” żadnego kwalifikatora, który wskazywałby na rodzaj tej infrastruktury czy ją dookreślał. Istotnym kryterium rozróżniającym pojęcia: „system teleinformatyczny”, „system informatyczny” i inny „system łączności” jest – jak można przyjąć w oparciu o definicje legalne - zastosowana w tych systemach technologia, w tym zwłaszcza technologia informacyjno-komunikacyjna oraz właściwe dla niej narzędzia technologiczne – służące wyłącznie do przetwarzania informacji bądź także do zdalnego przekazywania danych, jak i postać tych danych (cyfrowa czy papierowa, w tym głosowa, obrazowa, lub mieszana) oraz rodzaj narzędzia komunikacyjnego (transmisyjnego).

Wobec tak dużej różnorodności pojęciowej zachodzi potrzeba ujednolicenia zarówno samej terminologii, jak i desygnatów tak ujednoliconej terminologii. Termin „infrastruktura informacyjno-komunikacyjna”, wywodzony z nauk technicznych, zwłaszcza informatyki i telekomunikacji, a więc nauk właściwych dla nowoczesnych technologii informacyjno-komunikacyjnych, wydaje się jak najbardziej odpowiedni na określenie infrastruktury informacyjnej państwa używanej do przetwarzania

side the normative notion of „tele-informative infrastructure”[123] already existing for many years, or another one for determination of a technological layer of state information security. And the EU legislator has only decided to introduce the word “infrastructure” to definition of notion of „network of electronic communication” as a component defining this network, and more precisely, the “transmission systems”[124] listed in this definition. But it does not add any qualificator to the notion of “infrastructure” which could indicate the type of this infrastructure, or could define it more accurately. The essential criterium for distinguishing the notions: „tele-informative system”, „informative system” and other „communication system” is – as it can be taken from legal definitions – the technology applied in these systems, including especially the information-communication technology and technological tools relevant to it – used exclusively for processing information, or also for distant transfer of data, as the form of the data (digital, or paper like, including voice, images, or mixed) and the type of a communication (transmission) tool.

Regarding such great conceptual variety a need appears for normalisation both the terminology itself, and the designates of so normalised terminology. The term of „information-communication infrastructure” derived from technical sciences, especially of IT and telecommunication, and therefore the sciences appropriate for modern information-communication technologies, seems to be the most suitable for description of the state in-

[121] See definitions of this notion in art. 2, point 11 of the Act on information system, art. 2, point 4 of the Act on rescue information system, art. 2, point 2 of the Act on electronic services and art. 3, point 3 of the Act on informatisation of public subjects.

[122] See definition of informative system included in art. 7, point 2a of the Act from 29 August, 1997 on personal data protection, i.e.: Law Monitor from 2016, pos. 922, which was cancelled on 06 February, 2019 (on the force of art. 175 of currently biding law on the personal data protection from 2018). According to this regulation „informative system is understood as a set of devices, programs, information processing procedures and software tools used for data processing working together”.

[70] Zob. art. 2 pkt 8 prawa telekomunikacyjnego.

[71] Zob. art. 2 pkt 1 dyrektywy 2018/1972.

[123] See art. 2, point 8 of telecommunication law.

[124] See art. 2 point 1 of Directive 2018/1972.

danych w formie elektronicznej i ich transmisji za pomocą nowych technologii ICT. Jest to przy tym najszerszy zakresowo – bo obejmujący wszelkie obecnie dostępne na rynku usług online, w tym e-usług publicznych, sposoby komunikowania się i narzędzia telematyczne (narzędzia ICT) do gromadzenia, przechowywania, przetwarzania i przekazywania informacji elektronicznych (cyfrowych) danych (informacji) i komunikowania się na odległość – termin, niekiedy już stosowany w doktrynie, pomimo, że normatywnymi pojęciami są wyłącznie „system teleinformatyczny" i „system informatyczny". Proponowane pojęcie „infrastruktura informacyjno-komunikacyjna" – w przeciwieństwie do innych proponowanych przez doktrynę[72] terminów - ma też uniwersalny charakter, zwłaszcza, że w systemie teleinformatycznym – tak w praktyce, jak i na gruncie prawa - możliwe jest funkcjonalne wyodrębnienie jego mniejszych systemów (podsystemów). Żadne z najczęściej proponowanych przez przedstawicieli różnych dyscyplin nauki, zwłaszcza zaliczanych do tzw. nauk humanistycznych, oraz stosowanych obecnie przez normodawcę pojęć na określenie infrastruktury (a ściślej systemów teleinformatycznych) stosowanej do przetwarzania i transmisji danych nie oddaje zatem w pełni istoty i funkcjonalności tej infrastruktury. Można wręcz odnieść wrażenie, że różnorakie propozycje terminologiczne są wynikiem nie do końca zrozumienia subtelnych niekiedy różnic między informatyką i teleinformatyką, co jednakże usprawiedliwia wysoko specjalistyczna wiedza technologiczna, dostępna w jej całokształcie i ze wszelkimi kontekstami wyłącznie naukom z zakresu technologii. Niemniej jednak przedrostek „tele" wskazuje, wedle ogólnej i powszechnej wie-

formation infrastructure used for data processing in electronic form and its transmission via new ICT. It is moreover the term with the widest meaning as it encompasses all online services currently available in the market including public e-services, ways of communication and telematic tools (ICT tools) for collection, storing, processing, and transferring of electronic (digital) data (information), and for distant communication, and it was sometimes used in the doctrine despite that only "the tele-informative system" and "informative system" are the normative concepts. Proposed notion „information-communication infrastructure" – contrary to other terms proposed by the doctrine[125] - has also a universal character, especially that in the tele-informative system – both in practice and on the ground of law – a functional distinguishing of its smaller systems (subsystems) can be made. None of notions most often proposed by the representatives of different scientific disciplines, especially named as the arts sciences, and employed now by the legislator for determination of the infrastructure (and more strictly tele-informative systems), and used for processing and transmission of data, does not reflect faithfully the essence and functionality of this structure. One can even has an impression that different terminological proposals are caused by false understandings of subtle differences between informatics and tele-informatics, what anyway may be justified by a highly specialised technological knowledge which is exclusively available in all its contexts and completeness for the technological sciences. Nevertheless the prefix „tele" points out, according to the general and common knowledge, to a remote

[72] Por. G. Klein, op. cit., s. 22. Przykładowo doktrynalne pojęcie „kanał komunikacyjny" kładzie akcent wyłącznie na metodę komunikacji (sam proces – medium przesyłania informacji i komunikowania się), jak Internet, telefon itp., techniczne aspekty przesyłania informacji, podczas gdy analizowana infrastruktura obejmuje też inne elementy, w tym urządzenia do przetwarzania i magazynowania danych.

[125] Compare G. Klein, op. cit., p. 22. Exemplary notion of „communication channel" stresses exclusively a method of communication (the process itself – medium for transferring information and communication), such as Internet, telephone, etc., technical aspects of transmitting information, whereas the analysed infrastructure also includes other components, such as devices for data processing and storing.

dzy, na zdalny przekaz danych, tj. bez bezpośredniego kontaktu nadawcy i odbiorcy tych danych oraz przy użyciu narzędzi telematycznych (umożliwiających komunikację na odległość). Na tej podstawie można przyjąć, że istnieje zasadnicza – choć może w powszechnym społecznym odczuciu nie aż tak widoczna - różnica między informatyką a teleinformatyką. Współcześnie też to technologie zdalnej komunikacji, a więc narzędzia telematyczne, wiodą prym i odgrywają największą rolę w procesie przetwarzania danych i to one (a nie tradycyjne kanały komunikacji) w konsekwencji są najczęściej – co oczywiste poza samą informacją i bazami danych - przedmiotem ataków. W nauce[73] – choć słusznie podkreśla się, że bezpieczeństwo informatyczne (a precyzyjniej teleinformatyczne) jest węższe niż bezpieczeństwo informacyjne - to jednak wadliwie utożsamia się bezpieczeństwo informatyczne i teleinformatyczne[74], jednocześnie przy tym dostrzegając, że po pierwsze, „bezpieczeństwo informatyczne (teleinformatyczne) odnosi się do faktu szybkiego upowszechniania określonych metod przetwarzania i przesyłania informacji oraz wiążących się z tym konsekwencji w sferze bezpieczeństwa, nie zaś zwiększenia rangi informacji (niezależnie od sposobu i medium jej przechowywania, przetwarzania i przesyłania) we współczesnym świecie", oraz po drugie, że „kieruje ono uwagę na zmiany technologiczne w uzyskiwaniu, przechowywaniu, przetwarzaniu oraz przekazywaniu informacji, dokonujące się wraz z upowszechnieniem cyfrowych form prezentacji danych". Podkreśla się też niekiedy, że „na środowisko teleinformatyczne składa się infrastruktura teleinformatyczna jednostki wraz z wykorzystującymi ją systemami informatycznymi oraz eksploatowane w jednostce systemy informatyczne wspierające jego działalność, oparte na infrastrukturze teleinformatycznej zapewnianej przez podmioty ze-

transfer of data i.e. without any direct contact between sender and recipient of the data and by means of telematic tools (enabling distant communication). It can be accepted on the basis of this that there is an essential difference – which maybe is not so visible in a common social perception - between informatics and tele-informatics. And also now, the technologies of distant communication, the telematic tools, are the leading ones and have the greatest meaning in the process of data processing, and they are (but not the traditional communication channels) in consequence most often targeted – obviously beside the information itself and data bases. The science[126] – even if it reasonably notes that the informative security (and precisely tele-informative) has a narrower meaning than the information security – faulty identifies the informative and tele-informative security[127], and at the same time notices that at first „the informative (tele-informative) security refers to the fact of a rapid spreading of particular methods for processing and transferring the information, and to the consequences connected with it in the domain of security, but not to the increased importance of the information (independently on the method and medium of its storing, processing, and transferring) in the present world", and secondly that „it focuses the attention on technological changes for acquisition, storing, processing, and transferring of the information occurring along the spreading of digital forms of data presentation". It is sometimes underlined that „tele-informative environment consists of unit's tele-informative infrastructure together with informative systems using it, and the informative systems employed in the unit for supporting its operation and based on tele-informative infrastructure provided by the external subjects"[128].

[73] Zob. A. Żebrowski, op. cit., s. 452-453.

[74] Odmiennie A. Myśko, E. Młodzik, op. cit., s. 110. Według tych Autorów „między systemem informatycznym a systemem teleinformatycznym nie należy stawiać znaku równości".

wnętrzne"[75].

To różne spojrzenie rodzimych nauk na zagadnienie bezpieczeństwa informacyjnego państwa i różne do niego podejście – będące w głównej mierze wynikiem zastosowania właściwych dla tych nauk narzędzi badawczych i metodologii oraz fragmentarycznego podjęcia - jest zapewne przyczyną tak dużej różnorodności i tworzy wrażenie pewnego chaosu pojęciowego. Niemniej jednak wspólny dorobek tych nauk - zważywszy na interdyscyplinarność bezpieczeństwa informacyjnego państwa i jego wielowymiarowość – pozwala na stworzenie kompleksowego ujęcia tego zagadnienia w całokształcie jego różnorakich wymiarów. Nauki te intuicyjnie dostrzegają też różnice znaczeniowe używanych pojęć, choć następnie – co daje się dostrzec - nie zawsze konsekwentnie respektują nadane tym pojęciom znaczenia. Również prawodawca – pomimo posługiwania się różnymi terminami – dostrzega różnicę między „systemem teleinformatycznym", „systemem informatycznym" czy „infrastrukturą teleinformatyczną", a widoczne na gruncie prawa zróżnicowanie terminologiczne tylko pozornie sprawia wrażenie braku jego konsekwencji. Rozróżnia on – czego dowodzi analiza normatywnego materiału badawczego: unijnej i rodzimej regulacji prawnej z obszaru nowoczesnych technologii komunikacyjno-informacyjnych – wszak po pierwsze, pojęcia system i sieć w odniesieniu do technologii, a po drugie, pojęcia informatyka, teleinformatyka i inna łączność - odnoszone do systemów i sieci. To, że pojęcia te nie są tożsame, zamienne (synonimiczne), lecz mają inne zakresy przedmiotowe i znaczenie, prawodawca wyraża w definicjach legalnych stosowanych pojęć. Jednakże część definicji legalnych kluczowego dla prowadzonej analizy pojęcia „system teleinformatyczny", zawartych w ustawach szczegółowych, a niekiedy także w aktach wykonaw-

Such different outlooks of the homeland sciences on the question of the state information security, and different approaches to it, - effected in general by application of researching tools, and methodologies, and fragmentary approach relevant to these sciences – is surely the reason for such a great variety creating an impression of a conceptual chaos. Nevertheless, the joint output of these sciences - considering interdisciplinary and multidimensional character of state information security – can be used for preparation of a comprehensive outlook of this question for all its different dimensions. The sciences have been intuitively perceiving the differences of meanings for used notions, even if later – what can be noticed – they have not respected consequently the meanings given to these notions in each case. The legislator – despite using different terms – also notices a difference between „tele-informative system", „informative system", and „tele-informative infrastructure", and differentiation of terminology visible on the ground of the law only apparently gives an impression of a lack of its consequence. The legislator distinguishes – what can be proved by the analysis of the investigated normative material: the EU and homeland legal regulations on new communication-information technologies – by the way, firstly, the notions of system and network in reference to technology, and secondly, the notions of informatics, tele-informatics, and other communication links – referred to systems and networks. The fact that these notions are not identical and replaceable (synonymous) but have different scopes of meaning and subject is expressed by the lawmaker in definitions of legally used notions. But a part of legal definitions crucial for the present analysis of notion „tele-informative system", included in the detailed Acts, and sometimes in execu-

[126] See A. Żebrowski, op. cit., p. 452-453.
[127] Adversely A. Myśko, E. Młodzik, op. cit., p. 110. According to the authors „there is no equality between informative system and tele-informative system".
[128] See in this matter A. Myśko, E. Młodzik, op. cit., p. 110.
[75] Zob. na ten temat A. Myśko, E. Młodzik, op. cit., s. 110.

czych do ustaw[76], ma – na co trzeba zwrócić uwagę - charakter odsyłający[77] do definicji tego pojęcia, które zawierają dwie fundamentalne w tym zakresie ustawy: ustawa o świadczeniu usług drogą elektroniczną i ustawa o informatyzacji podmiotów publicznych. Wprowadzane zaś w ustawach szczegółowych[78] - na ich potrzeby własne definicje tych pojęć - zasadniczo są powtórzeniem definicji tych pojęć zawartych w ustawach podstawowych, a spotykane w nich niekiedy inne zredagowanie treści definicji nie ma istotnego znaczenia dla zakresu przedmiotowego definiowanych pojęć[79].

Dotychczasowy dorobek rodzimej nauki oraz materiał normatywny w obszarze bezpieczeństwa informacyjnego państwa (który z natury rzeczy powinien uwzględniać najnowszy poziom wiedzy w dziedzinie technologii i różnych obszarach „sfery informacyjnej" państwa) – wspólnie analizowany - stanowią doskonałą podstawę do skonstruowania prawniczej (doktrynalnej) definicji pojęcia „infrastruktura informacyjno-komunikacyjna" oraz wyróżnienia jej elementów składowych.

4. Pojęcie infrastruktura informacyjno-komunikacyjna państwa i jej elementy

Przyjmując za punkt wyjścia dla rozważań nad ujęciem w ramy prawnicze pojęcia „infrastruktura informacyjno-komunikacyjna państwa" normatywne znaczenie pojęcia „system

tive regulations for the Acts[129], has – what has to be stressed – a referential character[130] against the definitions of this notion, including two fundamental Acts for this question: the Act on rendering electronic services and the Act on informatisation of public subjects. Definitions of these notions, introduced in detailed Acts[131] to be used by them, in general repeat the definitions of these notions included in the basic Acts, and some differences of definition wordings which can be met there are without any essential meaning for the subjective scope of defined notions[132].

Present outcome of the homeland science and the normative material in domain of the state information security (which as a matter of fact has to take into account the newest level of knowledge in domain of technology and different areas of state's „information sector") can be analysed jointly, and create an excellent base for creation of legal (doctrinal) definition of notion „information-communication infrastructure" and for distinguishing its components.

4. Notion of State Information-communication Infrastructure and Its Components

Accepting the normative meaning of notion „tele-informative system" and notions linked to it: „telecommunication", „telecom-

[76] Zob. art. 2 pkt 6 ustawy o ochronie informacji niejawnych, art. 2 pkt 13 ustawy o informacji o ochronie zdrowia, czy art. 2 pkt 13 ustawy o systemie informacji o zdrowiu, a także § 2 pkt 9 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 30 maja 2011 r. w sprawie systemów teleinformatycznych stosowanych w publicznych służbach zatrudnienia, Dz. U. z 2011 r. nr 130, poz.75, czy § 2 pkt 12 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej, Dz. U. z 2007 r. nr 216, poz.1609. Por. też art. 2 pkt 14 ustawy o cyberbezpieczeństwie.

[77] Taki zabieg legislacyjny jest typowy dla prawa i jak najbardziej uzasadniony przejrzystością aktu prawnego oraz zasadami techniki prawodawczej. Regułą jest bowiem, że definicje podstawowych dla określonego obszaru unormowania zawierają akty podstawowe dla tego obszaru, natomiast inne akty prawne, które posługują się tymi pojęciami odsyłają do definicji zawartej w akcie podstawowym. Zob. np. § 4 ust. 1 czy § 9 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej", t.j.: Dz. U. z 2016 r. poz. 283, formułujące odpowiednio zakaz powtórzeń oraz zasadę konsekwencji terminologicznej w obrębie języka prawnego.

[78] Przykładowo art. 2 pkt 4 ustawy o systemie powiadamiania ratunkowego.

[79] Zob. definicje systemu teleinformatycznego zawartą w już powołanym przykładowo art. 2 pkt 4 ustawy o systemie powiadamiania ratunkowego.

teleinformatyczny" i powiązanych z nim pojęć: „telekomunikacja", „sieć telekomunikacyjna" oraz „infrastruktura telekomunikacyjna"[80] przyjąć można, że systemy teleinformatyczne to 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. Wobec tego pojęcie system teleinformatyczny jest bardzo szerokim pojęciem, mieszczącym w sobie wszelkie możliwe metody (sposoby) transmisji danych (informacji) w formie elektronicznej[81]. Jego struktura architektoniczna składa się zaś z - wymienianych w definicjach legalnych wskazanych po-

munication network" and „telecommunication infrastructure"[133] as a starting point of considerations on putting into legal frames the notion of „state information-communication infrastructure", it can be taken that tele-informative systems are the transmission systems which at first are used for processing of information in electronic (digital) form with computer hardware and software; and on second provide telecommunication, i.e. the transfer (transmission, reception, or retransmission) of information in the electronic form; on third are based on the communication (telecommunication) infrastructure; and at fourth they transfer the information via telecommunication networks by means of a terminal device relevant to given type of network. Regarding the above, the notion of tele-informative system is a very wide notion including all possible methods (ways) of data (information) transmission in the electronic form[134]. Its architectural struc-

[129] See art. 2, point 6 of the Act on protection of classified information, art. 2, point 13 of the Act on health protection, or art. 2, point 13 of the Act on the health information system, and also § 2, point 9 of Disposition of the Minister of Labour and Social Policy dated on 30 May, 2011 on tele-informative systems used by the public employment services, Law Monitor from 2011, nr 130, pos.75, or § 2, point 12 of Disposition of the Minister of Labour and Social Policy dated on 02 November, 2007 on tele-informative systems used in organisational units of social assistance, Law Monitor from 2007, nr 216, pos.1609. Also compare art. 2, point 14 of the Act on cybersecurity.

[130] Such legislative step is typical for the law and entirely substantiated by the transparency of the legal act and the rules of legislative engineering. It is because of the rule saying that the basic definitions for a specific domain of normalisation are included in the acts fundamental for this domain, whereas other legal acts using these notions have to refer to definitions included in the fundamental act. See for instance § 4, pos. 1, or § 9, of the Chair of the Board of Ministers dated on 20 June, 2002 on „Principles of Legislation Engineering", i.e.: Law Monitor from 2016, pos. 283, formulating respectively a ban of repetitions and a principle of terminological consequence in domain of legal language.

[131] For instance, art. 2, point 4 of the Act on the rescue information system.

[132] See definitions of tele-informative system included in art. 2, point 4, called as an example, of the Act on the rescue information system.

[80] Por. art. 2 pkt 1 dyrektywy 2018/1972, art. 2 pkt 3 ustawy o usługach drogą elektroniczną, art. 3 pkt 3 ustawy o informatyzacji podmiotów publicznych, art. 2 pkt 8, pkt 35, pkt 42 prawa telekomunikacyjnego.

[81] Obejmuje ono transmisję danych zarówno za pomocą przewodów, fal radiowych, optycznych, jak i innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzajów. Sygnały mogą być przekazywane przykładowo za pomocą radia, telefonów, telewizji, środków optycznych lub innych wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komputerowych i pakietowych, w tym Internetu) i sieci ruchomych, elektromagnetycznych systemów kablowych.

[133] Compare art. 2, point 1 of Directive 2018/1972, art. 2, point 3 of the Act on electronic services, art. 3, point 3 of the Act on informatisation of public subjects, art. 2, point 8, and 35, and 42 of telecommunication law.

[134] It includes both data transmission by wires, air, optics, and other means using electromagnetic energy, independently on their types. The signals may be transmitted for instance via radio, telephones, television, optical means or other using the waves, including satellite networks, and stationary (computerised and packeted, including Internet), and mobile networks, electromagnetic cable systems.

jęć - systemów informatycznych (komputerowych systemów informatycznych), sieci telekomunikacyjnej oraz infrastruktury telekomunikacyjnej.

Kluczowe dla tytułowego zagadnienia prawnych aspektów bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa technologiczne elementy stanowią – zważywszy na normatywny sposób rozumienia samego systemu teleinformatycznego - bardzo zróżnicowaną kategorię zarówno pod względem rodzaju, charakteru, jak i funkcjonalności. Zasadniczo można jednak wyróżnić dwa elementy warstwy technologiczno-technicznej bezpieczeństwa informacyjnego państwa: infrastrukturę informatyczną oraz infrastrukturę telekomunikacyjną (w tym infrastrukturę telekomunikacyjną budynku).

Ta pierwsza – infrastruktura informatyczna, określana niekiedy jako infrastruktura IT, zważywszy na doktrynalne ujęcie informatyczny system komputerowy[82], funkcjonalnie jest wykorzystywana do przetwarzania danych z wykorzystaniem sprzętu i oprogramowania komputerowego. Jest definiowana jako „zespół komponentów potrzebnych do funkcjonowania kooperacyjnych usług i środowisk informatycznych w przedsiębiorstwie, a także do zarządzania nimi”[83]. Stanowi ona wydzieloną skomputeryzowaną część systemu informacyjnego (informatyczny system komputerowy),

ture consists of informative systems (computerised informative systems), and telecommunication network, and telecommunication infrastructure, which were mentioned in the legal definitions of pointed out notions.

Technological components of crucial meaning for the question mentioned in the title over the legal aspects of the state information-communication infrastructure security constitute – considering the normative way of perception of the mere teleinformative system – very differentiated category regarding both the character and functionality. But in general two components of technological-technical level of the state information security can be distinguished: informative infrastructure and telecommunication infrastructure (including telecommunication infrastructure of a building).

The first one – informative infrastructure, named sometimes as IT infrastructure, regarding doctrinal perception of informative computer system[135], is functionally used for data processing using computer hardware and software. It is defined as „a combination of components needed for functioning of cooperating services and informative environments in the company, and for their management, as well”[136]. It creates a separate computerised part of the information system (informative computer system), and is char-

[82] Por. Sz. Konkol – Publikacje Cyfrowe, Charakterystyka informatycznych systemów komputerowych, 2 lipca 2016, https://www.slideshare.net/qwertyra/charakterystyka-informatycznych-systemw-komputerowych, dostęp z dnia 11 lipca 2022 r. Wedle tego Autora „informatyczny system komputerowy to zbiór powiązanych ze sobą elementów, którego funkcja jest przetwarzanie danych z wykorzystaniem sprzętu i oprogramowania komputerowego. (…) można go zdefiniować jako część systemu informacyjnego, którego głównym zadaniem jest przetwarzanie informacji. Pod pojęciem systemu informacyjnego należy rozumieć wielopoziomową strukturę, która pozwala użytkownikowi przekształcać dane wejściowe na pożądane informacje wyjściowe za pomocą odpowiednich modeli i procedur”.

[83] Zob. artykuł internetowy zatytułowany: Czym jest infrastruktura informatyczna?, https://www.ibm.com/pl-pl/topics/infrastructure, dostęp z dnia 19 lipca 2022 r.

[135] Compare Sz. Konkol – Digital Publications, Characteristics of informative computer systems, 2 July, 2016, https://www.slideshare.net/qwertyra/charakterystyka-informatycznych-systemw-komputerowych, accessed on 11 July, 2022. According to the author „informative computer system is a combination of linked together components aimed to data processing with computer hardware and software. (…) it may be defined as a part of information system aimed mainly to process the information. Under the notion of the information system one can understand a multi-level structure allowing for the user to transform input data into wanted output information by suitable models and procedures”.

[136] See the internet publication titled: What the informative infrastructure is?, https://www.ibm.com/pl-pl/ topics/infrastructure, accessed on 19 July, 2022.

charakteryzującą się – z uwagi na złożoność samego informatycznego systemu komputerowego - wielopoziomową strukturą, która pozwala użytkownikowi przekształcić dane wejściowe na pożądane informacje wyjściowe za pomocą odpowiednich modeli i procedur. O skomplikowanej strukturze infrastruktury informatycznej przesądza zarówno ilość jej elementów technologicznych, jak i zaawansowanie technologiczne oprogramowania, a także wielość użytkowników korzystających z tej infrastruktury oraz danych przetwarzanych przy jej zastosowaniu. Ten rodzaj infrastruktury składa się z niezależnych elementów, które można ująć w dwie zasadnicze grupy: sprzęt komputerowy (ang. *hardware*)[84], w tym urządzenia wejścia/wyjścia, oraz oprogramowanie (ang. *software*)[85]. Tak rozumiana infrastruktura informatyczna może mieć postać infrastruktury tradycyjnej, tj. składać się z typowych komponentów: sprzętu i oprogramowania, i zainstalowana w siedzibie podmiotu obrotu prawnego służyć do jego użytku wewnętrznego; lub infrastruktury chmurowej, podobnej do infrastruktury tradycyjnej, lecz umożliwiającej łączenie się użytkowników końcowych z infrastrukturą za pośrednictwem Internetu i poprzez mechanizm wirtualizacji[86] używania zasobów obliczeniowych bez instalowania ich na miejscu.

Druga z wymienionych infrastruktur – infrastruktura telekomunikacyjna funkcjonalnie

acterised – due to complexity of the informative computer system itself – by a multilevel structure which allows the transformation of input data into output information demanded by the user by employing suitable models and procedures. The complex structure of informative infrastructure is determined by both the number of its technological components, and technologically advanced computer codes, and finally by the variety of users using the infrastructure and data processed on it. This type of infrastructure consists of independent components which can be put in two main groups: computer hardware[137], including input/output devices, and software[138]. The infrastructure perceived in such way may exist in the form of conventional infrastructure, i.e. consist of typical components: hardware and software, and be installed in the premisses of the subject of legal trade for its internal use; or cloud infrastructure, similar to conventional infrastructure, but providing the connections of end users with the infrastructure via Internet and by a mechanism of virtualisation[139] on using the computing resources without installing them in the site.

The second listed infrastructure – telecommunication infrastructure is functionally employed for transferring (transmission) of data and distant communication, and includes according to its legal definition[140] „telecommunication equipment, apart from telecom-

[84] Sprzęt komputerowy stanowią różnego rodzaju urządzenia o różnej funkcjonalności, jak: urządzenia służące do przechowywania danych; urządzenia służące do zbierania danych (kamery, sensory); urządzenia służące do komunikacji między sprzętowymi elementami systemu; urządzenia służące do komunikacji między ludźmi a komputerami; urządzenia służące do odbierania danych ze świata zewnętrznego – nie od ludzi (na przykład czujniki elektroniczne, kamery, skanery). Do komponentów sprzętowych zaliczane są m.in. komputery osobiste, sieć, obejmująca: serwery (komputery umożliwiające wielu użytkownikom dostęp do zasobów i wspólne korzystanie z nich), koncentratory, routery, przełączniki; centra przetwarzania danych/serwerownie oraz infrastruktura budynku (przestrzeń dla sprzętu sieciowego, serwerów i całych centrów przetwarzania danych, okablowanie sieciowe budynków biurowych, które łączy ze sobą komponenty infrastruktury informatycznej).

[85] Obejmuje ono: oprogramowanie wbudowane (ang. *firmware*) np. sterownik urządzenia IoT; oprogramowanie systemowe (ang. *system software*) np. system operacyjny; oprogramowanie aplikacyjne (ang. *application software*) np. system zarządzania bazą danych. Do komponentów oprogramowania przykładowo zaliczane są systemy zarządzania treścią (CMS), systemy zarządzania relacjami z klientami (CRM), systemy do zarządzania zasobami przedsiębiorstwa (ERP), systemy operacyjne i serwery WWW.

[86] Wirtualizacja łączy serwery fizyczne utrzymywane przez dostawcę usług w jednym lub wielu ośrodkach. Jednocześnie wydziela i tworzy abstrakcję zasobów, takich jak pamięć masowa, aby były dostępne dla użytkowników praktycznie w dowolnym miejscu, w którym można nawiązać połączenie z Internetem.

służy do przekazywania (transmisji) danych oraz komunikacji na odległość i składa się, zgodnie z jej definicją legalną[87], „z urządzeń telekomunikacyjnych, oprócz telekomunikacyjnych urządzeń końcowych[88], oraz w szczególności linii, kanalizacji kablowych, słupów, wież, masztów, kabli, przewodów oraz osprzętu, wykorzystywanych do zapewnienia telekomunikacji", a jej część składową stanowi instalacja telekomunikacyjna budynku, która obejmuje w szczególności kable i przewody wraz z osprzętem instalacyjnym i urządzeniami telekomunikacyjnymi, począwszy od punktu połączenia z publiczną siecią telekomunikacyjną (przełącznica kablowa) lub od urządzenia systemu radiowego do gniazda abonenckiego[89]. W ramach tak normatywnie rozumianej infrastruktury telekomunikacyjnej daje się zatem – analogicznie jak w przypadku infrastruktury informatycznej - wyróżnić jej odrębne funkcjonalnie elementy, a mianowicie urządzenia przeznaczone do zapewnienia telekomunikacji, w tym umożliwiające nadawanie, odbiór lub transmisję sygnałów (za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną), jak: urządzenia elektryczne, elektroniczne czy radiowe; instalacje telekomunikacyjne, jak:

munication terminal devices[141], and especially the lines, cable channels, posts, towers, masts, cables, wires, and accessories employed for provision of telecommunication", and the telecommunication installation of the building is a component of it, consisting especially of the cables and wires with installation accessories and telecommunication devices, starting from the point of connection with the public telecommunication network (cable hub), or from the device of radiosystem to the subscriber's socket[142]. In the frame of such normatively understood telecommunication infrastructure some separate functional components can be distinguished – identically as in the case of informative infrastructure – such as devices for provision of telecommunication, enabling among others the transmission and reception of signals (by means of wires, optical or radio waves, or other means using electromagnetic energy) including: electric, electronic, or radio devices; telecommunication installations including: cables, wires with installation accessories, towers or masts; and the buildings or other constructed objects where the equipment is placed.

Basing on it, an assumption can be made

[137] Computer hardware consists of different devices of various functionalities such as: devices for storing data; for collection of data (cameras, sensors); devices for communication between system hardware components; devices for communication between people and computers; devices for reception of data from outside – not from people (for instance electronic sensors, cameras, scanners). Into the hardware components also fall between all personal computers, network encompassing: servers (computers providing access of many users to the resources and a joint use of them), concentrators, routers, switchers; data processing centres/server rooms and building infrastructure (space for network's hardware, servers, and the data processing centres, office building network cabling for connecting the informative infrastructure components).

[138] It includes: embedded software *(firmware*) e.g. controller of IoT device; system software, e.g. operational system; application software, e.g. data base management system. Components of the software include for instance contents management systems (CMS), customers relations management systems (CRM), electronic resources programming system (ERP), operating systems and servers WWW.

[139] Virtualisation connects real servers operated by the provider of services in one or many centres. At the same time it creates abstractive resources, such as mass memory, to be accessible for the users practically at any place where connection with Internet is possible.

[140] See art. 2, point 8 of telecommunication law.

[87] Zob. art. 2 pkt 8 prawa telekomunikacyjnego.

[88] Są to urządzenia telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci – art. 2 pkt 43 prawa telekomunikacyjnego.

[89] Zob. definicję zawartą w art. 2 pkt 8a prawa telekomunikacyjnego.

[141] These are the telecommunication devices dedicated for direct or undirect connection with the termination of the network – art. 2, point 43 of telecommunication law.

[142] See definition included in art. 2, point 8a of telecommunication law.

kable, przewody wraz z osprzętem instalacyjnym, wieże czy maszty; oraz budynki lub inne obiekty budowlane, w których znajdują się te urządzenia.

Na tej podstawie przyjąć można, że termin „infrastruktura informacyjno-komunikacyjna" stanowi pojęcie zbiorcze na określenie infrastruktury informatycznej i infrastruktury telekomunikacyjnej, które służą odpowiednio do przetwarzania danych (informacji) oraz ich przekazywania i odczytu, lecz razem współdziałające spełniają funkcję informacyjno-komunikacyjną państwa. Obejmuje ona - w zależności od zastosowanych narzędzi komunikacji i celu zastosowania - wyodrębnione organizacyjno-technicznie struktury (systemy), które tworzą razem funkcjonalną całość, ale też jednocześnie mogą funkcjonować jako samodzielne elementy infrastruktury informacyjno-komunikacyjnej[90].

Obok tak skonstruowanej infrastruktury informacyjno-komunikacyjnej państwa w doktrynie pojawia się znaczeniowo zbliżone pojęcie „infrastruktura teleinformatyczna". Tę ostatnią doktryna definiuje – adaptując stanowisko Komisji Nadzoru Finansowego w zakresie tej infrastruktury - jako zespół urządzeń i łączy transmisyjnych, obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: rutery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę tych zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), a także te wykorzystywane w ośrodkach zapasowych jednostki[91]. Pojęcie

that the term „information-communication infrastructure" is a collective notion describing the informative infrastructure and telecommunication infrastructure which are used respectively for data (information) processing and transmitting, and for reading it out, but when working together they are fulfilling the information-communication function of the state. It encompasses – depending on applied communication tools and dedicated application – selected organisational-technical structures (systems) which taken together create a functional integrity, but can also operate as independent components of information-communication infrastructure[143].

Beside the state information-communication infrastructure constructed in such way the doctrine includes a notion of "tele-informative infrastructure" with similar meaning. This last one is defined by the doctrine as a system of devices and transmitting links – adapting the opinion of the Commission of Financial Survey concerning this infrastructure – especially including hardware platforms (with: servers, matrixes, working stations), tele-informative network (with routers, switchers, network barriers, and other network devices), system software (with operating systems, and data base management systems), and other components providing undisturbed and safe operation of these resources (with power supplies UPS, electric power generators, air condition devices), and also those which are used in reserve centres of the unit[144]. The notion of „tele-informative infrastructure" – linked directly with the term „tele-informative system" and associated with this system – may be regarded as an alternative (and replacing)

[90] W jej ramach w ujęciu normatywnym mogą występować odrębne, stanowiące pewną funkcjonalną całość systemy jak: system zarządzania usługami IT, system zarządzania bezpieczeństwem informacji, system dedykowany użytkownikom usług sieciowych - które ze sobą powiązane współdziałają dla prawidłowego działania systemu informacyjnego państwa jako całości.

[91] Zob. A. Myśko, E. Młodzik, op. cit., s. 110.

[143] Some separate systems can exist in its frame, in normative aspects, creating a functional entity, such as: systems for governing IT services, system for information security management, system dedicated to users of

cie „infrastruktura teleinformatyczna" - nawiązujące wprost do terminu „system teleinformatyczny" i kojarzone z tym systemem - można uznać za alternatywne (i zamienne) dla proponowanego w opracowaniu terminu „infrastruktura informacyjno-komunikacyjna" określenia dla technologicznej warstwy bezpieczeństwa informacyjnego państwa. Tym bardziej, że w odniesieniu do telekomunikacji i sieci telekomunikacyjnej prawodawca stosuje pojęcie „infrastruktura telekomunikacyjna".

Infrastruktura informacyjno-komunikacyjna (czy infrastruktura teleinformatyczna) państwa jest dość złożonym i skomplikowanym układem różnorakich technologicznych elementów o różnej funkcjonalności, które razem połączone (i współpracujące) umożliwiają przetwarzanie i przekazywanie danych w postaci elektronicznej oraz komunikowanie na odległość. Złożoność ta jest sumą złożoności i wieloskładnikowości infrastruktury informatycznej i telekomunikacyjnej, w tym infrastruktury budynkowej. Architektura infrastruktury informacyjno-komunikacyjnej składa się z różnych składników systemów teleinformatycznych, w tym systemów wyodrębnionych funkcjonalnie, powiązań i relacji między tymi składnikami. Prawodawca dopuszcza wszak projektowanie i wdrażanie systemów teleinformatycznych „sektorowych" (dla spraw należących do właściwości jednego działu administracji rządowej) i „ponadsektorowych" (dla spraw należących do właściwości więcej niż jednego działu administracji rządowej)[92], a także przewiduje odrębne systemy do zarządzania bezpieczeństwem informacji czy zarządzania usługami IT[93]. W ujęciu doktrynalnym „infra-

one for the term proposed in the paper „information-communication infrastructure" identifying the level of the state information security. And much more, the legislator uses the notion "telecommunication infrastructure" referring to telecommunication and telecommunication network.

The state information-communication infrastructure (or tele-informative infrastructure) is a relatively complicated and complex system of different technological components with different functionalities which after combining (and working together) provide data processing and transferring in electronic form and distant communication. The complexity is a sum of complexity and multicomponent character of informative and telecommunication infrastructure, including the building infrastructure. The architecture of information-communication infrastructure consists of different components of tele-informative systems, including the systems which were functionally integrated, and mutual connections and relations between these components. The legislator permits anyway the designing and implementation of "sectorial" tele-informative systems (for the matters falling into competence of one section of the government administration) and „over-sectorial" ones (for matters falling to competence of more than one section of the government administration)[145], and also predicts separate systems for managing the security of information, or managing the IT services[146]. In the doctrinal outlook „the information infrastructure of the public administration in the state, and in

network services - which linked together work jointly for proper operation of the state information system as the whole.

[144] See A. Myśko, E. Młodzik, op. cit., p. 110.

[92] Zob. art. 3 pkt 7 i pkt 8 ustawy o informatyzacji podmiotów publicznych.

[93] Zob. np. § 15 ust. 2 i § 20 ust. 2 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, zwanego rozporządzeniem w sprawie Krajowych Ram Interoperacyjności lub rozporządzeniem w sprawie KRI.

[145] See art. 3, point 7 and 8 of the Act on informatisation of public subjects.

struktura informacyjna administracji publicznej w państwie, a w niektórych dziedzinach także w skali międzynarodowej, stanowi kompleks systemów ściśle ze sobą powiązanych i współdziałających systemów teleinformatycznych. Współdziałanie to polega na wymianie informacji, wspomaganiu kontroli jakości i integralności informacji, korzystaniu ze wspólnych zasobów informacyjnych i metainformacyjnych, minimalizacji refundancji, a dzięki temu optymalizacji kosztów infrastruktury informacyjnej całej administracji publicznej, innych jednostek sektora publicznego i podmiotów społecznych i ekonomicznych: przedsiębiorstw, jednostek społecznych, gospodarstw domowych"[94]. Istotną cechą infrastruktury informacyjno-komunikacyjnej jest więc to aby po pierwsze, wszystkie jej technologiczne elementy, jak i wyodrębnione funkcjonalnie systemy były częścią procesów funkcjonujących w organizacji oraz ogólnej struktury tej infrastruktury i były z nimi zintegrowane, a po drugie, aby bezpieczeństwo poszczególnych elementów składowych, w tym zwłaszcza danych i usług IT, było uwzględniane przy projektowaniu i wdrażaniu systemów teleinformatycznych.

Dla systemów teleinformatycznych służących do realizacji zadań publicznych rodzimy prawodawca przyjął, jako zasadniczy, model usługowy architektury, dopuszczając jednakże wyjątkowo stosowanie innego modelu architektury - w przypadkach uzasadnionych specyfiką podmiotu publicznego lub świadczonych przez niego usług[95]. Model usługowy[96] architektury systemu teleinformatycznego - system zorientowany na usługi (Service Oriented Ar-

some domains also in the international scale, constitutes a complex of tele-informative systems strictly linked and working together. The cooperation refers to exchange of information, to support of the quality control and information integrity, to use of joint resources of information and metainformation, and to minimisation of re-foundation and in consequence to it to optimisation of the costs of the information infrastructure for the whole public administration, and to other units of the public sector and social and economic subjects: companies, social units, the households"[147]. The essential feature of the information-communication infrastructure is firstly that all its technological components and functionally separated systems were a part of processes functioning in the organisation and in the general structure of the infrastructure, and were integrated with them, and secondly that the security of particular components, especially IT data and services, were regarded at designing and implementing tele-informative systems.

The homeland legislator has accepted for tele-informative systems, used for execution of public assignments, a service oriented model of architecture as the basic one, permitting anyway on exceptional basis the use of other model of architecture – in the cases substantiated by the specificity of the public subject or the services rendered by it[148]. Service oriented model[149] of architecture of tele-informative system (Service Oriented Architecture - SOA) is character-

[146] See for instance § 15, pos. 2, and § 20, pos. 2 of Disposition of the Ministers' Board dated on 12 April, 2012 on the Homeland Frames of Interoperability (HFI), and minimal requirements for public records and exchange of electronic information, and minimal requirements for tele-informative systems, i.e.: Law Monitor from 2017, pos. 2247, named as disposition on the Homeland Frames of Interoperability, or disposition on HFI.

[94] J. Oleński, Standardy informacyjne w administracji publicznej - wybrane tezy i zagadnienia (w:) Z. Olejniczak, J.S. Nowak, J.K. Grabara, Systemy informatyczne w administracji, Warszawa 2004, s. 29.

[95] Zob. § 8 ust. 1 i ust. 4 lub rozporządzeniem w sprawie KRI.

[96] Zob. § 2 pkt 8 rozporządzenia w sprawie KRI.

[147] J. Oleński, Information Standards in public administration – selected thesis and questions, (w:) Z. Olejniczak, J.S. Nowak, J.K. Grabara, Informative systems in administration, Warsaw 2004, p. 29.

[148] See § 8, pos. 1 and 4 of Disposition on HFI.

[149] See § 2, point 8 of Disposition on HFI.

chitecture - SOA) charakteryzuje się zaś tym, że dla użytkowników definiuje się stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisuje się sposób korzystania z tych funkcji, jak wskazany przykładowo system zarządzania bezpieczeństwem informacji. Usługi sieciowe są przy tym rozumiane tu jako „właściwość systemu teleinformatycznego polegającą na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze”[97].

5. Normatywne wymagania bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa

Normatywne wymagania bezpieczeństwa infrastruktury informacyjo – komunikacyjnej (systemów teleinformatycznych) – unormowane na gruncie aktualnego stanu prawnego dwupoziomowo: na poziomie ustawowym i poziomie rozporządzenia wykonawczego[151] – są znacznie zróżnicowane tak co do szczegółowości i kategoryczności ich sformułowania, jak i charakteru prawnego. Sama konstrukcja systemów teleinformatycznych opiera się zaś na wymogu zapewnienia im interoperacyjności[152], stosownie do Krajowych Ramach Interoperacyjności[153].

Nie wnikając w szczegółowe rozwiązania prawne, pozostawione - z uwagi na obszerność i kazuistyczność regulacji prawnej, złożoność samej problematyki wymagań i standardów bezpieczeństwa tej infrastruktury - odrębnemu opracowaniu[154] można zasadniczo

ised by definition of functions of tele-informative system, constituting a separated integrity (network services), for the users, and by description of methods for using these functions, as for instance the pointed out system for information security management. The network services are regarded here as “a feature of tele-informative system for repeated execution of predefined functions by the system after receiving the data arranged according to a specific structure by means of tele-informative network system”[150].

5. Normative Requirements for State Information-communication Security

Normative requirements of security for information-communication infrastructure (tele-informative systems) – normalised on the ground of the present legal status and on two levels: on the level of the law and on the executive level[161] – are largely differentiated, both concerning the details and categorical aspect of their formulations, and the legal character. The mere construction of tele-informative systems is based on a requirement for provision of interoperability to them[162], in compliance with the Homeland Frames of Interoperability[163].

Leaving apart details of legal solutions, which due to their volume and casuistic character of legal regulations, and complexity of questions concerning the requirements and standards for security of this infrastructure can be presented in a separate work[164],

[97] Zob. § 2 pkt 19 rozporządzenia w sprawie KRI.
[150] See § 2, point 19 of Disposition on HFI.
[151] Zob. art. 1 pkt 2 i pkt 3 oraz art. 18 ustawy o informatyzacji podmiotów publicznych.
[152] Interoperacyjność – najogólniej to ujmując – oznacza zdolność systemów teleinformatycznych do bezpośredniego współdziałania ze sobą (bez udziału człowieka jako tzw. interfejsu białkowego). Tak G. Szpor., K. Wojsyk, op. cit., wersja Lex.
[153] Zob. np. art. 1 pkt 2 , art. 3 pkt 9 czy art. 13 ust. 1 ustawy o informatyzacji podmiotów publicznych oraz § 3 rozporządzenia w sprawie KRI.
[154] Szerzej na temat wymogów zob. E. Cisowska – Sakrajda, Normatywne wymagania bezpieczeństwa infrastruktury informacyjno – komunikacyjnej, Problemy Techniki Uzbrojenia (w druku).
[161] See art. 1, point 2 and 3, and art. 18 of the Act on informatisation of public subjects.

wyróżnić dwie ich zasadnicze grupy. Są to, po pierwsze, unormowane ustawowo wymagania prawno-organizacyjne: zasady ogólne adresowane do podmiotów realizujących zadnia publiczne, a zawierające wskazówki przy ustalaniu wymagań dla systemów teleinformatycznych i Krajowych Ram Interoperacyjności (KIR) oraz dostosowania tych systemów do wymagań ustanowionych w KIR, jak: zasada neutralności technologicznej i zasada jawności używanych standardów i specyfikacji[155]; wskazane wymagania dla systemów teleinformatycznych, interoperacyjności i Krajowych Ram Interoperacyjności, jak: wymagania organizacyjne, technologiczne i semantyczne[156]; oraz katalog skonkretyzowanych obowiązków podmiotów publicznych w zakresie zapewnienia bezpieczeństwa systemów teleinformatycznych[157]. Po drugie, są to, wskazane na poziomie rozporządzenia w sprawie KIR a stanowiące dorobek społeczności międzynarodowych, wymagania prawno-techniczne, to jest konkretne (zindywidualizowane) normy i standardy stosowane w rozwiązaniach technologicznych, a w razie ich braku standardy uznawane przez organizacje międzynarodowe lub przez nie rekomendowane. Wymagania te – uwzględniające tak szybko zmieniającą się technologię teleinformatyczną i telekomunikacyjną, specyfikę postępu technologicznego i praw rządzących tym postępem oraz samą technologią – obejmują w szczególności wy-

in general two main groups of them may be distinguished. First of all, they are the legal-organisational requirements normalised in the Acts: general principles addressed to the subjects performing the public assignments with the guidelines for preparation of requirements for tele-informative systems and the Homeland Frames of Interoperability (HFI), and adaptation of these systems to the requirements set in the HFI, such as: the principle of technological neutrality, and the principle of openness for used standards and specifications[165]; recommended requirements for tele-informative systems and the interoperability and the Homeland Frames of Interoperability with organisational, technological and semantical requirements[166]; and the catalogue of identified obligations for the public subjects on provision of security to the tele-informative systems[167]. And secondly, they are the legal-technical requirements, indicated on the level of disposition concerning the HFI and prepared by international societies, including the precise (individualised) normalisations and standards employed for technological solutions, and in the case of lacking the such ones, the standards recognised or recommended by the international organisations. These requirements – regarding the rapidly changing tele-informative and telecommunication technologies, the specificity of technological

[162] Interoperability – in general outlook – is the capacity of tele-informative systems for working together (without a human factor as the so called protein interface). As G. Szpor., K. Wojsyk, op. cit., version Lex.

[163] See for instance art. 1, point 2 , art. 3, point 9, or art. 13, pos. 1 of the Act on informatisation of public subjects and § 3 of Disposition for HFI.

[164] Wider in the question of requirements see E. Cisowska – Sakrajda, Normative requirements for security of information-communication infrastructure, Problemy Techniki Uzbrojenia *(Issues of Armament Technology)* (under printing).

[155] Zob. art. 1 pkt 2 i 3 ustawy o informatyzacji podmiotów publicznych.

[156] Zob. art. 3 pkt 18 ustawy o informatyzacji podmiotów publicznych.

[157] Zob. np. art. 13 ust. 2 pkt 1 w zw. z ust. 3, ust. 2 pkt 2, ustawy o informatyzacji podmiotów publicznych oraz § 5 ust. 2, § 6, § 8 ust. 3, § 9 pkt 1, § 10 ust. 5, ust. 6, ust. 11 i ust. 12, art. 13 ust. 2 pkt 2 i § 16 ust. 3 rozporządzenia w sprawie KRI, a także G. Szpor, K. Wojsyk, op. cit., wersja z Lex.

[165] See art. 1, subpoints 2 and 3 of the Act on informatisation of public subjects.

[166] See art. 3, point 18 of the Act on informatisation of public subjects.

[167] See for instance art. 13, pos. 2, point 1 in reference to pos. 3, and 2, point 2, of the Act on informatisation of public subjects, and § 5, pos. 2, § 6, § 8 pos. 3, § 9, point 1, § 10, pos. 5, 6, 11 and 12, art. 13, pos. 2, point 2 and § 16, pos. 3 of Disposition on HFI, and also G. Szpor, K. Wojsyk, op. cit., version with Lex.

magania techniczne czy normalizujące (standaryzujące) dla systemów teleinformatycznych (infrastruktury informacyjno-komunika-cyjnej) - w tym zwłaszcza architektury tego systemu i jej modelu, kompatybilności, a także normy, standardy i procedury dla podmiotów realizujących zadania publiczne oraz reguły „użyteczności" systemu. Spełnienie przez system wszystkich tych zasad jest przy tym - stosownie do zasady kompletności wymagań oraz zasady równoważności wymagań[158] - konieczne dla zapewnienia normatywnego poziomu bezpieczeństwa technologicznej warstwy informacyjnej państwa.

Tak ukształtowane wymagania dla systemów teleinformatycznych - pomijając odrębne unormowanie, w pewnym zakresie, wymagań dla sieci telekomunikacyjnej[159] - oraz wymagania techniczne dla interoperacyjności tych systemów zostały przyjęte przez ustawodawcę na poziomie minimalnym[160]. Jednocześnie katalog wymagań dla interoperacyjności jest szersze niż dla samych systemów, gdyż obejmują one – poza wymaganiami organizacyjnymi i technologicznymi – dodatkowo wymagania semantyczne. Pomimo zauważalnych między nimi definicyjnych różnic – tworzą one spójny zespół czy zestaw określonych parametrów czy wartości, gwarantujących prawidłowe funkcjonowanie systemów teleinformatycznych – przetwarzanie i transfer/wymianę danych. Wymagania te łącznie – bez względu czy odnoszą się do systemu teleinformatycznego, czy do interoperacyjności tego systemu – stanowią zarazem uniwersalny standard dla systemów teleinformatycznych, które stosują

progress and the rules governing the progress and the technology itself – include especially technical, or normalising (standard) requirements for tele-informative systems (information-communication infrastructure) – with the system's architecture and its model, compatibility, and the norms, standards, and procedures for subjects performing the public assignments, and the rules of system's "usefulness". Fulfilment of all these principles by the system is anyway – according to the principles of completeness and equality of requirements[168] - a necessary step for provision of a normative security level for the state information technological layer.

The requirements formulated in this way for tele-informative systems – omitting separate normalisation, in some degree, of requirement for telecommunication network[169] - and technical requirements for interoperability of these systems were accepted by the legislator on the minimal level[170]. At the same time the catalogue of requirements for interoperability is larger than for the systems themselves, as it additionally comprises – besides organisational and technological requirements – the semantical requirements. Despite differences noticed in their definitions – they create a coherent complex or system of specific parameters or values warranting proper functionality of tele-informative systems – data processing and transfer/exchange. These requirements together – regardless if they refer to tele-informative system or to the interoperability of this system – constitute at the same time a universal standard for tele-informative systems used by

[158] Przykładowo zob. pkt 1 zatytułowany Zakres normy oraz pkt 0 zatytułowany Wprowadzenie ppkt 01 akapit piąty PN nr PN-ISO/IEC 27001, s. 7.

[159] Por. art. 132 ust. 1, art. 137 ust. 1, art. 175 ust. 1, art. 17c ust. 1, art. 175d czy art. 182 prawa telekomunikacyjnego.

[160] Por. rozdział III i IV 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.

[168] For instance see point 1 titled *Scope of the norm,* and point 0 titled *Introduction* subpoint 01, paragraph five PN nr PN-ISO/IEC 27001, p. 7.

[169] Compare art. 132, pos. 1, and art. 137, pos. 1, and art. 175, pos. 1, and art. 17c, pos. 1, and. 175d, or art. 182 of telecommunication law .

[170] Compare chapters III and IV of Disposition on HFI, and art. 1, points 2 and 3, and art. 3, points 9 and 10 of the law on informatisation of public subjects.

podmioty realizujące zadania publiczne. Określają one bowiem powszechnie przyjmowany model, wzorzec dla projektowania, wdrażania i eksploatacji systemów teleinformatycznych, systemów zarządzania usługami realizowanymi przez systemy teleinformatyczne, prezentacji danych w systemach teleinformatycznych oraz systemów zarządzania bezpieczeństwem informacji. Z założenia mają one z jednej strony zapewniać bezpieczeństwo infrastruktury informacyjno – komunikacyjnej państwa (bezpieczeństwo systemów teleinformatycznych), z drugiej zaś kompatybilność i zdolność różnych systemów do wzajemnej „współpracy".

6. Zagrożenia dla bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa

Zastosowanie nowoczesnej technologii informacyjno-komunikacyjnej w procesie przetwarzania i transmisji danych, generowanych przez podmioty realizujące zadania publiczne, stwarza niezliczone możliwości atakowania tak infrastruktury informacyjno-komunikacyjnej, jak i danych przetwarzanych i transmitowanych przy jej użyciu. Nawet najlepsze zabezpieczenia (w tym oprogramowanie antywirusowe), normatywne mechanizmy ochrony infrastruktury oraz procedury szybkiego i skutecznego reagowania na pojawiające się zagrożenia, a nade wszystko ich respektowanie, jak i najwyższej klasy standardy (zasady i procedury) bezpieczeństwa systemów teleinformatycznych nie są w stanie zapobiec naruszeniu funkcjonalności czy użyteczności tej infrastruktury, a tym bardziej je wyeliminować całkowicie. Mogą natomiast - co wymaga uświadomienia - jedynie zminimalizować ryzyko powstania zagrożeń dla tego obszaru bezpieczeństwa państwa. W sposób ewidentny dowodzą tego doniesienia medialne o spektakularnych (o globalnym zasięgu) i skutecznych atakach międzynarodowej grupy hakerów na rządowe strony Federacji Rosyjskiej po dokosubjects performing the public tasks. It is because they determine a commonly accepted model, or pattern, for designing, and implementing and using of tele-informative systems, and the systems managing the services provided by tele-informative systems, and for presentation of data in the tele-informative systems, and for the information security management systems. It is assumed, from one side, that they have to provide the security of the information-communication infrastructure (security of tele-informative systems), and on the other side, the compatibility and ability of different systems to "work together".

6. Threats to State Information-Communication Infrastructure Security

Application of modern information-communication technology in the process of data processing and transmission generated by the subjects performing the public tasks creates numerous occasions for attacking both the information-communication infrastructure, and the data processed and transmitted with its use. Even the best protections (including anti-virus software), and normative mechanisms of infrastructure security and the procedures for quick and efficient reaction against appearing threats, and most of all the observance of them, and the standards of the highest rank (rules and procedures) for tele-informative systems security cannot prevent any infringements in functionality or usability of this infrastructure, or to eliminate them entirely. They may instead – and it has to be realised – minimise the risk of posing the threats for this sector of state security. It is proved by media news about spectacular (with global range) and efficient attacks of international groups of hackers on the governmental sites of the Russian Federation after the aggression

naniu agresji na Ukrainę. W obszarze bezpieczeństwa informacyjnego państwa istnieje bowiem pewna doza niepewności nieuprawnionego – zamierzonego (celowego) lub przypadkowego – dostępu do infrastruktury, wywołania destrukcyjnych działań przez podmioty zewnętrzne, jak i wewnętrzne w stosunku do państwa, czy też tylko zaistnienia prozaicznych zagrożeń i pułapek związanych z nieodpowiednim użytkowaniem narzędzi technologicznych (Internetu i systemów informatycznych) lub brakiem świadomości użytkowników potencjalnych zagrożeń technologicznych. Zagrożenia te mogą jednakże, w szczególności powodować utratę płynności funkcjonowania państwa lub jego poszczególnych organów, kreować negatywny wizerunek państwa na arenie międzynarodowej i/lub w środowisku wewnętrznym państwa, w szerszej skali mogą skutkować powstaniem zakłóceń w świadczeniu usług publicznych, strategicznych dla zaspokojenia podstawowych potrzeb całego lub części społeczeństwa (tzw. usług użyteczności publicznych) czy choćby spowodować paraliż w ich realizacji. Sprawne funkcjonowanie technologii informacyjno-komunikacyjnych stanowi zatem niezaprzeczalnie fundament niezakłóconego działania współczesnego państwa i funkcjonowania społeczeństwa informacyjnego.

Dostrzegając wagę analizowanego zagadnienia unijny i rodzimy prawodawca definiuje odpowiednio pojęcia „szkodliwe zakłócenia" i „incydent związany z bezpieczeństwem"[171] oraz „zagrożenie sytemu teleinformatycznego"/„szkodliwe zakłócenia"[172], a także powiązane z nimi pojęcia „zagrożenie cyberbezpieczeństwa", „ryzyko" i „incydent" („incydent krytyczny", „incydent poważny", „incydent istotny" i „incydent w podmiocie publicznym")[173]. Na podstawie tych definicji oraz ję-

against Ukraine. Anyway, there is a piece of uncertainty in domain of the state information security for unauthorised - intentional (deliberate) or casual – access to the infrastructure, triggering destructive actions by the external and internal subjects against the state, or presence of simple threats and traps connected with improper use of technological tools (Internet and informative systems) or the lack of users awareness about potential technological threats. But these threats can specifically cause the loss of continuity in functionality of the state or its institutions and create a negative image of the state or its particular institutions on the international arena and/or in the state internal environment, and in the larger scale they may effect in arising disturbances for rendering public services which are strategically important for meeting the basic demands of the whole or a part of the society (so called publicly used services), or even may jeopardise their performance. The efficient operation of information-communication technologies is undoubtedly a foundation for undisturbed existence of the modern state and the informative society.

Noticing the weight of the considered question the EU and homeland lawmakers define respective notions of „harmful interferences", and „ an incident connected with the security"[181], and „tele-informative system threat"/„harmful interferences"[182], and also linked to them notions of „cybersecurity threats", „risk" and „incident" („critical incident", „serious incident", „important incident" and „incident in the public subject")[183]. On the basis of these definitions and linguistical meaning of the notion „damage" a legal definition of notion

[171] Zob. art. 2 pkt 20 i pkt 42 dyrektywy 2018/1972.
[172] Zob. § 2 pkt 22 rozporządzenia w sprawie KRI oraz art. 2 pkt 40a prawa telekomunikacyjnego.
[173] Zob. art. 2 pkt 17, pkt 12, pkt 5, pkt 6, pkt 7, pkt 8 i pkt 9 ustawy o cyberbezpieczeństwie, art. 4 pkt 9 i pkt 7 dyrektywy 2016/1144 i art. 2 pkt 15 ustawy o ochronie informacji niejawnych.
[181] See art. 2, point 20 and 42 of Directive 2018/1972.
[182] See § 2, point 22 of Disposition on HFI and art. 2, point 40a of telecommunication law.

zykowego rozumienia pojęcia „szkoda" można skonstruować prawniczą definicję pojęcia „zagrożenia bezpieczeństwa infrastruktury informacyjno-komunikacyjnej" – co istotne odnoszonego jedynie do infrastruktury działającej zgodnie z obowiązującymi przepisami międzynarodowymi, unijnymi lub krajowymi, a więc skonstruowanej w oparciu o normatywne wymagania. W tym ujęciu pojęcie to należy identyfikować jako potencjalną przyczynę (źródło) niepożądanego zdarzenia lub okoliczności (incydentu, zakłócenia) i ich konsekwencje, które: po pierwsze, mogą wywołać szkodę w tej infrastrukturze, tj. spowodować stratę lub uszczerbek w jej działaniu[174], lub po drugie, mogą zagrozić jej normalnemu funkcjonowaniu lub poszczególnych jej elementów, lub po trzecie, mogą poważnie pogorszyć, utrudnić, przerwać lub wielokrotnie zakłócić jej funkcjonowanie, lub po czwarte, mogą mieć (wywrzeć) niekorzystny wpływ na jej bezpieczeństwo, lub po piąte, mogą powodować poważne obniżenie jakości lub przerwać ciągłość świadczenia przez podmioty publiczne usług za pomocą systemów teleinformatycznych lub realizowania zadań przez ten podmiot. Pojęcie „zagrożenia dla bezpieczeństwa infrastruktury informacyjno-komunikacyjnej" obejmuje zatem szerokie spektrum przyczyn, które mogą spowodować różnej wagi konsekwencje dla funkcjonowania tej infrastruktury, a w następstwie i bezpieczeństwa państwa. W ujęciu doktrynalnym zagrożeniem bezpieczeństwa państwa – wiązanym ściśle z samym bezpieczeństwem państwa - jest natomiast „taki splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w którym z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych – w wyniku zastosowania przemocy politycznej, psycholo-

„threats to information-communication infrastructure security" can be prepared – what is essentially referred only to the infrastructure operating according to the binding international, homeland and the EU regulations, i.e. prepared on the basis of normative requirements. In this perspective the notion has to be identified as a potential cause (source) of an unwanted event or circumstances (incident, disturbances) and their consequences which, at first, may cause a damage in the infrastructure, i.e. cause a loss or detriment to its operation[184], or secondly, may threat normal functionality of it or its particular components, or thirdly, may seriously worsen, harm, interrupt, or disturb its operation many times, or fourthly, may exert unfavourable impact into its security, or fifthly, may cause serious reduction of quality, or interrupt the continuity of rendering the services by the public subjects via tele-informative systems, or the execution of tasks by the subject. The notion of „threat to information-communication infrastructure security" includes then the wide spectrum of reasons which can trigger consequences with different weight for operation of this infrastructure, and finally for the security of the state. In the doctrinal perspective, the threat for state security – strictly linked with the state's own security – is „such combination of internal events, or in international relations, when it is highly likely that a limitation or loss of conditions can occur for undisturbed existence of state or its partner-like treatment in international relations – in effect of applied political, or psychological, or economical, or military violence, etc."[185]. Following this way of thinking and at the same time referring to the EU definitions of „security of network and ser-

[183] See art. 2, point 17, points 12, 5, 6, 7, 8 and 9 of the Act on cybersecurity, art. 4, points 9 and 7 of Directive 2016/1144, and art. 2, point 15 of the Act on protection of classified information.
[174] Zob. M. Szymczak (red.), op. cit., s. 413/414.

gicznej, ekonomicznej, militarnej itp."[175]. Podążając tym tokiem rozumowania i jednocześnie sięgając do unijnych definicji „bezpieczeństwo sieci i usług" /„bezpieczeństwo sieci i systemów informatycznych"[176] czy rodzimej definicji „cyberbezpieczeństwo"[177] zagrożeniem dla bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa w ujęciu normatywnym będzie splot takich zdarzeń, które z dużym prawdopodobieństwem mogą wystąpić, powodując utratę lub ograniczenie zdolności tej infrastruktury do odpierania, na przyjętym dla niej poziomie bezpieczeństwa, wszelkich działań naruszających jej dostępność, autentyczność, integralność oraz poufność.

W wymiarze technologicznym zagrożenia dla bezpieczeństwa informacyjnego państwa wykazują się szczególną specyfiką i są – z uwagi na ich zasięg, szybkość rozprzestrzeniania się, a niekiedy „ciche" oraz „powolne" działanie i w konsekwencji powodowane szczególnie groźne dla państwa skutki – wyjątkowo niebezpieczne i szkodliwe. Postęp technologiczny nie tylko bowiem stwarza warunki (przy braku odpowiedniej ochrony) nieograniczonego dostępu do zasobów informacyjnych państwa, w tym kluczowych dla zapewnienia jego bezpieczeństwa w różnych jego obszarach (nie tylko militarnym). Powoduje on też – jak słusznie zauważa doktryna - zmianę natury zagrożeń dla systemów teleinformatycznych państwa, a „w czasach powszechnego dostępu do technik informatycznych, rodzą się nowe niebezpieczeństwa, ściśle powiązane z użytkowaniem sieci informatycznych i systems"/„security of network and informative systems"[186], or the homeland definition of „cybersecurity"[187], a threat for the state information-communication infrastructure security in the normative perspective will be created by such combination of these events which could happen with a high probability, and may cause the loss or limitation of infrastructure's capacities for repelling, at a level of security accepted to it, all actions breaching its accessibility, authenticity, integrity and confidentiality.

Threats to state information security in the technological dimension show a particular specificity and are exceptionally dangerous and harmful due to their range, speed of spreading, and sometimes to a "quiet" and a "slow" action what in consequence generates exceptionally threatening effects for the state. Technological progress creates not only conditions (at the lack of proper protection) for unrestricted access to state information resources, including those of crucial importance for provision of its security in different sectors (not only the military one), but also causes – as it is justly noted by doctrine – the change in the nature of threats for the state teleinformative systems, and „in the times of common access to informative techniques the new dangers arise strictly connected with the use of informative networks and information systems"[188].

Technological threats – as one of numerous categories distinguished in the

[184] See M. Szymczak (red.), op. cit., p. 413/414.

[185] As in Zb. Ciekanowski, Types and sources of threats, Arts and Social Sciences in Favour of Security, https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BGPK-2860-1288/c /httpwww_bg_utp_edu_plartbtp2012010bezpieczef1stwo-zc.pdf, accessed on 20 July, 2022 and literature called there.

[175] Tak Zb. Ciekanowski, Rodzaje i źródła zagrożeń bezpieczeństwa, Nauki Humanistyczne i Społeczne na Rzecz Bezpieczeństwa, https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BGPK-2860-1288/c /httpwww_bg_utp_edu_plartbtp2012010bezpieczef1stwo-zc.pdf, dostęp z dnia 20 lipca 2022 r. i powołana tam literatura.

[176] Zob. art. 2 pkt 21 dyrektywy 2018/1972 oraz art. 4 pkt 2 dyrektywy 2016/1144.

[177] Zob. art. 2 pkt 4 ustawy o cyberbezpieczeństwie.

temów informacyjnych"[178].

Zagrożenia technologiczne - jako jedna z licznie wyróżnianych w rodzimej doktrynie kategorii zagrożeń dla bezpieczeństwa państwa[179] - charakteryzują się tym, że ingerują one w stosowaną przez państwo technologię informacyjno-komunikacyjną a ingerencja ta następuje w sposób zdalny przy użyciu atakowanej technologii poprzez zaatakowanie całości lub poszczególnych elementów (systemów, baz danych) infrastruktury informacyjno-komunikacyjnej państwa. Zagrożenia te, nazywane jako techniki włamań do systemów teleinformatycznych, obejmują różne działania[180].

homeland doctrine of threats for the state security[189] - are characterised by their intervention into the information-communication technology used by the state, and this intervention is occurring in a remote way by employing the attacked technology through attacking the whole, or particular components (systems, data bases), state information-communication infrastructure. These threats are also named as techniques for breaking into teleinformative systems, and comprise different actions[190].

[186] See art. 2, point 21 of Directive 2018/1972 and art. 4, point 2 of Directive 2016/1144.

[187] See art. 2, point 4 of the Act on cybersecurity.

[188] As J. Gerwatowski, Information security in territorial self-governing units, Legislation Studies, UWM 2019 nr 44, p. 91/92 and literature called there.

[178] J. Gerwatowski, Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego, Studia Prawno-ustrojowe UWM 2019 r. nr 44, s. 91/92 i powołana tam literatura.

[179] Szerzej na temat klasyfikacji tych zagrożeń zob. J. Gerwatowski, op. cit., s. 96 i n., Zb. Ciekanowski, op. cit., wersja internetowa, W. Kitler, Pojęcie i zakres bezpieczeństwa informacyjnego …, s. 35 i n. oraz T. Aleksandrowicz, op. cit., s. 45 i n.

[180] Doktryna właściwa dla zarządzania bezpieczeństwem informacyjnym wskazuje na: zdalne wprowadzanie do sieci informatycznych wirusów komputerowych (czy robaków, koni trojańskich lub innych aplikacji), dostosowanych programowo do samopowielania i szybkiego rozprzestrzeniania i destabilizowania sprawności systemu; lokowanie w systemach informatycznych tzw. bomb logicznych, które jako odpowiednio opracowane aplikacje programowe będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych wcześniej reżimów czasowych; blokowanie wymiany danych w torach transmisyjnych, deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem środków masowego przekazu, kanałów łączności rządowej i wojskowych systemów dowodzenia; wprowadzanie wirusów komputerowych do rządowych oraz komercyjnych sieci i systemów informatycznych, jak również układów zdalnego sterowania tymi systemami; wytwarzanie impulsów wielkiej mocy, zaprogramowanych na niszczenie urządzeń elektronicznych, a także środków biologicznych – specjalnych mikrobów – do niszczenia obwodów elektronicznych i materiałów izolacyjnych; stosowanie broni elektronicznej przeciwko wybranym elementom infrastruktury i przemysłu, powodujące np. paraliżowanie łączności, transportu, dopływu energii elektronicznej, czyli paraliżowanie życia w danym regionie; wprowadzanie programów wykorzystujących błędy w systemach operacyjnych i oprogramowaniu użytkowym; wywoływanie fałszywych alarmów czy celowe inicjowanie awarii. Tak np. A. Żebrowski, op. cit., s. 457, tabela nr 4 oraz podana tam literatura, a także J. Gerwatowski, op. cit., s. 97 i podana tam literatura.

[189] Wider about classification of these threats see J. Gerwatowski, op. cit., p. 96 and following, Zb. Ciekanowski, op. cit., internet version, W. Kitler, Notion and range of informative security …, p. 35 and following and T. Aleksandrowicz, op. cit., p. 45 and following.

[190] Doctrine which is relevant for information security management indicates: the remote introduction of computer viruses to informative networks (or worms, Trojan horses or other applications), adapted to self-reproduction in the software and to rapid scattering and destabilisation of systems efficiency; login of the so called logic bombs in informative systems which as a suitably prepared software applications will be adapted for activation under earlier specified signals or according to preprogramed time sequences; blocking of data exchange in transmission busses, deformation of contents, and introduction of false logic contents via the mass media into informative systems, channels of government communication and military command systems; introduction of computer viruses into the government and commercial networks and informative systems, as well as the systems for remote control over these systems; generation of high power pulses programmed for destruction of electronic equipment, and also biological assets – special microbes – for destruction of electronic circuits and insulation materials; use of electronic weapons against selected components of infrastructure and industry effecting for instance the interruption of communication, transport, supply of elec-

7. Bezpieczeństwo infrastruktury informacyjno-komunikacyjnej państwa – podsumowanie

Zagadnienie technicznego wymiaru bezpieczeństwa informacyjnego państwa, tj. infrastruktury informacyjno-komunikacyjnej, tak kluczowego w toczonej obecnie walce informacyjnej na arenie międzynarodowej między różnymi jej uczestnikami, nie zostało – pomimo przyjęcia przez rodzimego prawodawcę na przestrzeni kilkunastu ostatnich lat szeregu aktów prawnych – unormowane w sposób kompleksowy i spójny. W tym obszarze rodzima regulacja prawna jest znacznie rozproszona, chociaż kluczowe kwestie zostały zawarte w trzech podstawowych aktach prawnych: ustawie o informatyzacji podmiotów publicznych i rozporządzeniu w sprawie Krajowych Ram Interoperacyjności oraz prawie telekomunikacyjnym. Poza nimi obowiązuje wiele norm technicznych i standaryzujących, przyjętych przez międzynarodowe, unijne i krajowe organizacje normalizacyjne, a także wiele krajowych uregulowań w mniejszym czy większym stopniu odnoszących się do tej problematyki, jak: ustawa o świadczeniu usług drogą elektroniczną.

Rodzimy prawodawca nie wprowadza też jednolitej terminologii dla określenia infrastruktury informacyjnej państwa, zachowując funkcjonujące w poprzedniej epoce technologicznej pojęcie „systemy informatyczne", które stosuje obok pojęć: „systemy teleinformatyczne", „telekomunikacja" i „infrastruktura telekomunikacyjna" oraz „sieć telekomunikacyjna". Stosowana przez niego terminologia nie jest też spójna z unijną terminologią, która jest stosowana dla nowych technologii informacyjno-komunikacyjnych stosownie do idei *e-Europa* 2000 i jej aktualizacji, a którą wyrażają pojęcia takie jak: „bezpieczeństwo sieci i

7. State Information-communication Infrastructure Security – Summary

The question of technical dimension of state information security, i.e. information-communication infrastructure, having a key meaning at present information war in the international arena between different sides, was not normalised in comprehensive and coherent way despite acceptation of many legal acts by the homeland lawmakers within a dozen of last years. The homeland legal regulation in this domain is significantly scattered even if the basic questions were included in three basic legal acts: the Act on informatisation of public subjects, and disposition on the Homeland Frame of Interoperability, and the telecommunication law. Besides them, there is a lot of binding technical and normalising standards accepted by international, the EU, and homeland normalisation organisations, and many homeland regulations relating to these questions in certain degree, for instance the Act on rendering services by electronic means.

The homeland legislator has not introduced any uniformed terminology for description of the state information infrastructure, as well, leaving the notion of "informative systems", originating from former technological epoch, which is used beside the notions: „tele-informative systems", „telecommunication" and „telecommunication infrastructure" and „telecommunication network". Terminology used by the legislator is a bit uncoherent with the EU terminology used for new information-communication technologies following the idea of *e-Europe* 2000 and its updating, and which is expressed by such notions as: „security of network and services", or „security of networks and informa-

tric energy, or paralysation of life in a given region; introduction of programs exploiting the errors in operational systems and used software; launching false alerts or intentional initiation of faults. As e.g. A. Żebrowski, op. cit., p. 457, table nr 4 and literature given there, and also J. Gerwatowski, op. cit., p. 97 and literature given there.

usług" czy „bezpieczeństwo sieci i systemów informatycznych". W konsekwencji na poziomie krajowym prawodawca również nie definiuje używanych już w doktrynie, a jak najbardziej adekwatnych dla nowej technologii, pojęć jak: „infrastruktura informacyjno-komunikacyjna" czy alternatywnego do niego pojęcia „infrastruktura teleinformatyczna". Wprowadza natomiast szereg z nimi powiązanych pojęć jak: „zagrożenia systemu teleinformatycznego", „szkodliwe zakłócenia" czy „zagrożenie cyberprzestępstwa", które także nie są w pełni spójne z definicjami adekwatnych unijnych pojęć.

Także rodzima doktryna różnych dyscyplin nauki nie prezentuje kompleksowego i spójnego stanowiska wobec zagadnienia bezpieczeństwa informacyjnego państwa i jego technologicznego wymiaru, koncentrując się jedynie na poszczególnych aspektach bezpieczeństwa informacyjnego państwa. Z kolei doktryna prawa administracyjnego – dostrzegając regulację prawną w zakresie technologicznych warunków bezpieczeństwa informacyjnego państwa (infrastruktury informacyjno-komunikacyjnej państwa/systemów teleinformatycznych) – nie poświęca jej wiele uwagi.

To wszystko razem wzięte pod rozwagę prezentuje obraz rodzimej doktryny i rodzimego prawa w obszarze bezpieczeństwa informacyjnego państwa jako chaotycznego i pozbawionego kompatybilności, a parafrazując normatywne pojęcie jako „nie – interoperacyjnego", w zakresie terminologii i precyzji pojęciowej, a ściślej braku dostatecznej precyzji. W efekcie nie ma kompleksowych interdyscyplinarnych badań i opracowań monograficznych, które objęłyby wszystkie aspekty bezpieczeństwa informacyjnego państwa i to w sposób kompleksowy, tj. uwzględniający wiedzę i doświadczenie różnych dyscyplin nauki, a mających za przedmiot jakikolwiek wycinek bezpieczeństwa informacyjnego państwa.

Z zadowoleniem należy przyjąć wprowadzenie do rodzimego prawa regulacji w zakresie technologicznych aspektów bezpieczeństwa

tive systems". In effect, the legislator also does not define the notions on the homeland level, which were already used in the doctrine and are well adequate for the new technology, such as: „information-communication infrastructure", or the alternative notion „tele-informative infrastructure". The legislator introduces instead a series of notions connected with them such as: „threats to tele-informative system", „harmful disturbances", or „threats of cybercrimes", which are also not entirely coherent with definitions of the EU adequate notions.

The homeland doctrine of different disciplines of science also lacks a comprehensive and coherent stand against the question of state information security and its technological dimension, focusing exclusively on particular aspects of the state information security. On the other hand, the doctrine of administration law – noticing the legal regulation for technological conditions of state information security (state information-communication infrastructure) – does not pay too much attention to it.

Considering all the above mentioned, it represents a picture of the homeland doctrine and the law in domain of the state information security as a chaotic one and deprived of compatibility, and paraphrasing a normative notion as „non – interoperative" in the aspect of terminology and precision of formulation, and more precisely as lacking a sufficient precision. In effect there is a lack of any comprehensive and interdisciplinary investigations and monographic proceedings which could include all aspects of the state information security in a comprehensive way, i.e. regarding the knowledge and experience of different disciplines of science, and focused on any sector of state information security.

The introduction of a regulation to the homeland law on technological aspects of state information security, including requirements for information-communication

informacyjnego państwa, w tym wymogów dla bezpieczeństwa infrastruktury informacyjno-komunikacyjnej. Przyczyni się to – niewątpliwie - do zwiększenia bezpieczeństwa tak zasobów informacyjnych państwa, jak i stosowanej do ich przetwarzania i transmisji infrastruktury. Pewien niedosyt regulacji wywołuje jednakże wskazywany chaos pojęciowy i definicyjny, a także dość skomplikowane i przez to mało czytelne (dwupoziomowe i poprzez odesłania) zaprezentowanie wymagań dla systemów teleinformatycznych. W praktyce wiele problemów może też rodzić próba dookreślenia zastosowanych przez normodawcę – choć koniecznych – pojęć nieostrych, a będących elementem niektórych wymagań.

Waga bezpieczeństwa informacyjnego państwa uzasadnia wobec tego podjęcie przez władzę legislacyjną pilnych działań, które po pierwsze, ujednolicą i uporządkują funkcjonującą nadal na gruncie rodzimego prawa w różnych aktach prawnych różnorodność pojęciową, a stosowaną na określenie technicznego wymiaru bezpieczeństwa informacyjnego państwa; a po drugie, doprowadzą do skonstruowania jednej definicji kluczowych dla tego obszaru pojęć, jak: „infrastruktura informacyjno-komunikacyjna" czy „infrastruktura teleinformatyczna", oraz jednolitej siatki pojęciowej dla szeregu powiązanych z „bezpieczeństwem technologicznym państwa" zjawisk, zdarzeń, jak: „zagrożenie dla bezpieczeństwa infrastruktury informacyjno-komunikacyjnej państwa".

infrastructure security, can be noted with satisfaction. It can contribute inevitably to increased security for both the state information resources, and the infrastructure used for their processing and transmission. But indicated chaos in the notions and definitions shows some shortages in the regulations, together with relatively complex, and due to it insufficiently legible (in two levels and with references), presentation of requirements for tele-informative systems. In practice some problems can be also created by an attempt for precising ambiguous notions used by the legislator – which anyway are necessary – as the components of some requirements.

The meaning of the state information security justifies then taking the urgent actions of legislative authorities to unification and putting in order, at first, the wide notional selection still existing in different legal acts of the homeland law and used for description of technical dimension of the state information security; and to preparation, at second, of one definition of key notions in this domain, such as: „information-communication infrastructure", or „tele-informative infrastructure", and a unified notional diagram for many effects, or events, related with „state technological security", such as: „threat to the state information-communication infrastructure security".

Bibliografia / *Bibliography*

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

[2] M. Baran, M. Flankowski, Przegląd systemów *e-Government* w wybranych krajach, *Humanities and Social Sciences* HSS, vol. XIX, 21 (2/2014), pp.9-23 *April – June.*

[3] M. Bernaczyk, Obowiązek bezwnioskowego udostępniania informacji publicznej, Oficyna 2008, Lex 2022.

[4] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013.

[5] D. Bogusz, Wymagania technologiczne dla bezpieczeństwa dla komercyjnych systemów teleinformatycznych, https://www.bbn.gov.pl/download/1/1004/wymaganiatechnologiczne.pdf

[6] K. Chałubińska-Jentkiewicz, M. Karpiuk Mirosław, Prawo nowych technologii. Wybrane zagadnienia, LEX 2015.

[7] Zb. Ciekanowski, Rodzaje i źródła zagrożeń bezpieczeństwa, Nauki Humanistyczne i Społeczne na Rzecz Bezpieczeństwa, https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BGPK-28601288/c/ httpwww_ bg_utp_edu_plartbtp2012010bezpiec zef1stwo-zc.pdf

[8] Czym jest infrastruktura informatyczna?, https://www.ibm.com/pl-pl/ topics/infrastructure.

[9] E. Darmorost, Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz, LexisNexis 2013, Lex 2022.

[10] J. Gerwatowski, Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego, Studia Prawnoustrojowe UWM 2019 r. nr 44.

[11] M. Gołka, Czym jest społeczeństwo informacyjne?, Ruch Prawniczy, Ekonomiczny i Socjologiczny rok LXVII - zeszyt 4 – 2005.

[12] A. Hołda-Wydrzyńska, Cyfrowo wykluczeni, czyli problem dostosowania stron internetowych administracji publicznej do standardów dostępności, Niepełnosprawność – zagadnienia, problemy, rozwiązania nr 1/2013 (6).

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

[14] W. Kitler, Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne [w:] W. Kitler (red.), J. Taczkowska-Olszewska (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017.

[15] G. Klein, Bezpieczeństwo informacyjne RP w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej – perspektywa teoretyczna, Studia Wschodnioeuropejskie 11/2019.

[16] Sz. Konkol – Publikacje Cyfrowe, Charakterystyka informatycznych systemów komputerowych, 2 lipca 2016, https://www.slideshare.net/qwertyra/charakterystyka-informatycznych-systemw-komputerowych.

[17] M. Kuraś, System informacyjny a system informatyczny – co oprócz nazwy różni te dwa obiekty?, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie 2009, nr 770.

[18] M. Luterek, *E-government*. Systemy informacji publicznej, Warszawa 2010.

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

[20] A. Myśko, E. Młodzik, Bezpieczeństwo informacji – dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833, Finanse, Rynki Finansowe, Ubezpieczenia nr 72 (2014).

[21] E. Okoń-Horodyńska, Strategia Lizbońska – założenia programu rozwoju innowacyjnej Europy? [w:] E. Okoń-Horodyńska (red.), K. Piech (red.), STRATEGIA LIZBOŃSKA a możliwości budowania gospodarki opartej na wiedzy w Polsce – wnioski i rekomendacje, Warszawa 2005.

[22] J. Oleński, Standardy informacyjne w administracji publicznej - wybrane tezy i zagadnienia [w:] Z. Olejniczak, J.S. Nowak, J.K. Grabara, Systemy informatyczne w administracji, Warszawa 2004.

[23] J. Orłowska, „Baltophobia", czyli wojna informacyjna Rosji w państwach bałtyckich, Refleksje nr 22/2020.

[24] P. Potejko, Bezpieczeństwo informacyjne [w:] K. A. Wojtaszczyk (red.), A. Materska-Sosnowska (red.), Bezpieczeństwo państwa, Warszawa 2009.

[25] Projekt „Doktryna Bezpieczeństwa Informacyjnego RP", Warszawa 2015.

[26] P. M. Sitniewski, Dostęp do informacji publicznej. Pytania i odpowiedzi, LEX 2014.

[27] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014.

[28] 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.

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

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

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

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