

*Dominika Skoczylas**

Determinanty cyfryzacji a instrumenty prawnofinansowe wspierające wzrost poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego – analiza projektu „Cyberbezpieczny Samorząd”

**Determinants of Digitalization and Legal and Financial
Instruments Supporting the Increase in the Level of
Cybersecurity in Local Government Units – Analysis of the
“Cybersecure Local Government” Project**

STUDIA I ANALIZY

Słowa kluczowe: administracja publiczna, cyberbezpieczeństwo, cyfryzacja, e-administracja, jednostki samorządu terytorialnego

Key words: public administration, cybersecurity, digitization, e-administration, local government units

Abstrakt: Nie ulega wątpliwości, że technologie informacyjno-komunikacyjne zmieniły klasyczny sposób realizacji zadań publicznych. W kręgu zainteresowania pozostaje przede wszystkim zagadnienie informatyzacji administracji samorządowej. Z uwagi na aktualne wyzwania występujące w obszarze cyfryzacji, zdecydowano się na opracowanie i wdrożenie projektu „Cyberbezpieczny Samorząd”, którego celem jest zwiększenie poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Niniejszy artykuł pozwoli na scharakteryzowanie instrumentów prawnofinansowych, które mogą przyczynić się do poprawy jakości, efektywności, transparentności świadczenia e-usług przez administrację samorządową oraz odporności sieci i systemów teleinformatycznych na cyberzagrożenia.

Abstract: There is no doubt that information and communication technologies have changed the classic way of implementing public tasks. The issue of computerization of local government administration remains of primary interest. Due to the current challenges in

* ORCID ID: <https://orcid.org/0000-0003-1231-8078>; dr, adiunkt na Wydziale Prawa i Administracji Uniwersytetu Szczecińskiego. E-mail: dominika.skoczylas@usz.edu.pl.

the area of digitalization, it was decided to develop and implement the "Cybersecure Local Government" project, which aims to increase the level of cybersecurity in local government units. This article will characterize legal and financial instruments that can contribute to improving the quality, efficiency and transparency of the provision of e-services by local government administration and the resilience of networks and ICT systems to cyberthreats.

Wprowadzenie

W istocie środki komunikacji elektronicznej znalazły szerokie zastosowanie zarówno w działaniach administracji państwowej, jak i samorządowej. Zważywszy na zasadę decentralizacji¹ oraz to, że kluczowe usługi publiczne realizowane są przede wszystkim na poziomie lokalnym, przedmiotem zainteresowania stały się kwestie dotyczące zapewnienia cyberbezpieczeństwa systemów teleinformatycznych oraz ich użytkowników – mieszkańców gmin, powiatów i województw. Podniesienie poziomu odporności na cyberzagrożenia stało się kluczowym zadaniem jednostek samorządu terytorialnego. Należy stwierdzić, że z uwagi na „wykonywanie zadań, wykorzystywanie w tym celu uprawnień i zasobów w sposób samodzielny, niezależny (...)”² na samorządach spoczywa niebagatelna odpowiedzialność co do zapewnienia efektywnych i dostosowanych do potrzeb społeczeństwa warunków świadczenia e-usług.

Niepodważalnie informatyzacja pozwoliła na wprowadzenie nowoczesnych standardów w zakresie realizacji zadań publicznych, zarządzania informacją (e-informacją) oraz przetwarzania danych osobowych (w e-zbiorach). Pierwotne założenia dotyczące funkcjonowania elektronicznej administracji opierały się na dostępności informacyjnej i umożliwieniu nieograniczonej komunikacji on-line pomiędzy urzędem a obywatelem oraz w ramach wewnętrznych struktur administracji. Jako cechy charakterystyczne e-administracji wskazywano wówczas szybkość i efektywność załatwiania spraw publicznych, personalizację i interoperacyjność e-usług³. Istotnym etapem informatyzacji administracji publicznej było stworzenie koncepcji e-partycypacji. Obecnie „e-administracja, jako jeden z elementów e-demokracji, rede-

¹ Zgodnie z art. 15 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm.), dalej: Konstytucja RP, ustrój terytorialny Rzeczypospolitej Polskiej zapewnia decentralizację władzy publicznej.

² D. Sieklucki, *Decentralizacja – podstawowe zagadnienia teoretyczne*, «Politeja» 2022, nr 2(77), s. 23.

³ A. Dudzińska, M. Gontarczyk, *E-administracja w Polsce*, «Studia Politologiczne» 2013, vol. 27, s. 241–242.

finiuje rolę rządów, tak aby stały się bardziej zorientowane na obywateli⁴. Transformacja cyfrowa administracji publicznej znajduje się w gronie czynników mających wpływ na rozwój społeczno-gospodarczy i dobrostan obywateli. Pozytywnie należy zatem ocenić działania sektora publicznego mające na celu m.in. poprawę dostępności cyfrowej, wzmocnienie kompetencji cyfrowych użytkowników e-administracji oraz wykorzystanie systemów sztucznej inteligencji w sektorze administracji publicznej. Jednocześnie na znaczeniu zyskuje koncepcja tzw. administracji inteligentnej (ang. *smart administration*)⁵. W świetle zasady subsydiarności, jednostki samorządu terytorialnego uzyskały samodzielność i niezależność w zakresie wykonywania zadań publicznych na rzecz określonych społeczności lokalnych. Innymi słowy idea subsydiarności przejawia się przez pryzmat potrzeb mieszkańców danej wspólnoty samorządowej, jednocześnie przypisuje odpowiedzialność za załatwianie spraw publicznych właściwym organom administracji samorządowej⁶. Bez cienia wątpliwości należy stwierdzić, że nowe technologie znalazły szerokie zastosowanie w administracji publicznej, również (a może – przede wszystkim) w jednostkach samorządu terytorialnego. Transformacja cyfrowa administracji samorządowej wymaga jednak dalszego udoskonalenia, szczególnie w takich kwestiach jak dostępność i kompetencje cyfrowe użytkowników oraz ochrona sieci i systemów teleinformatycznych przed cyberzagrożeniami. Z uwagi na wyzwania w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni i ograniczone możliwości organizacyjne, technologiczne oraz finansowe zdecydowano się wprowadzić określone instrumenty prawnofinansowe wspierające wzrost poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Decentralizacja i subsydiarność powodują wzrost roli administracji samorządowej w działaniach z zakresu cyberbezpieczeństwa.

Celem artykułu jest przedstawienie problematyki cyfryzacji i cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Przedmiot badania odnosi się do wskazania podstawowych czynników cyfryzacji usług publicznych, ze szczególnym uwzględnieniem obowiązków administracji samorządowej w zakresie zapewnienia cyberbezpieczeństwa. W opracowaniu zostanie podniesiona kwestia konieczności wdrożenia odpowiednich instrumentów prawnofinansowych wspierających wzrost poziomu cyberbezpieczeństwa

⁴ D. E. Harasimiuk, T. Braun, *Nowa złożoność. Dialog demokratyczny w warunkach transformacji cyfrowej*, «Przegląd Konstytucyjny» 2021, nr 4, s. 65.

⁵ K. Pilarz, *System planowania przestrzennego wobec procesów informatyzacji i cyfryzacji administracji publicznej*, [w:] P. Lisowski (red.), *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, Wrocław 2024, s. 779–780.

⁶ G. Dutkiewicz, *Samorząd terytorialny w kontekście zasady pomocniczości w nauczaniu społecznym Kościoła katolickiego*, «The Religious Studies Review» 2019, nr 3(273), s. 152.

w jednostkach samorządu terytorialnego. Artykuł został przygotowany według schematu od ogółu do szczegółu. Na potrzeby niniejszej pracy posłużono się przykładem (analizą) rozwiązań zawartych w projekcie „Cyberbezpieczny samorząd”⁷. Szczegółowej oceny przedmiotowego projektu dokonano w rozdziale pt. „Przegląd instrumentów prawnofinansowych wspierających wzrost poziomu cyberbezpieczeństwa w administracji samorządowej – projekt „Cyberbezpieczny Samorząd”. W rezultacie ustalono, że projekt „Cyberbezpieczny Samorząd” może w pewnym stopniu wzmocnić odporność na cyberzagrożenia, w tym zwiększyć poziom bezpieczeństwa informacji w samorządach. Temat wydaje się szczególnie interesujący z uwagi na dynamiczny rozwój technologii, a co za tym idzie popularyzację świadczenia usług na odległość oraz znaczenie polityk cyberbezpieczeństwa w dobie cyberzagrożeń. Metody badawcze obejmują analizę podstawowych aktów prawnych z wykorzystaniem literatury przedmiotu.

Determinanty cyfryzacji w jednostkach samorządu terytorialnego

Korzyści wynikające z zastosowania środków komunikacji elektronicznej w działaniach administracji publicznej obejmują trzy podstawowe obszary: e-usług, e-zarządzania oraz e-demokracji. Trzeba przy tym dodać, że wszystkie z nich przyczyniają się do uproszczenia procedur administracyjnych, przy jednoczesnym zachowaniu standardów efektywności i personalizacji świadczenia usług. Z aprobatą należy przyjąć to, że cyfryzacja sektora publicznego umożliwiła (bądź wzmocniła) powszechny dostęp do informacji publicznej, bieżącą weryfikację procesów i procedur administracyjnych, redukcję kosztów, partycypację społeczną oraz transparentność działań administracji publicznej⁸. Modernizacja administracji publicznej uwarunkowana postępem technologicznym oraz potrzebami społeczeństwa informacyjnego stała się także katalizatorem zmian w administracji samorządowej. Idea elektronicznego samorządu stanowi pokłosie ogólnej koncepcji elektronicznej administracji. Za determinanty cyfryzacji w jednostkach samorządu terytorialnego należy uznać te o charakterze

⁷ Projekt został zrealizowany przez Centrum Projektów Polska Cyfrowa w Partnerstwie z NASK Państwowym Instytutem Badawczym w ramach Funduszy Europejskich na rozwój cyfrowy 2021–2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa; zob. Centrum Projektów Polska Cyfrowa, *Cyberbezpieczny samorząd*, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (1.07.2024).

⁸ K. Jastrzębska, *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, Warszawa 2018, s. 47–48.

stricte technologicznym (rozwój infrastruktury teleinformatycznej, pełne usieciowienie), organizacyjno-prawnym (zmiana modelu zarządzania sprawami publicznymi, wzrost kompetencji cyfrowych urzędników, wprowadzenie stosowanych rozwiązań legislacyjnych) oraz społecznym (poprawa jakości usług, e-dostępność, e-partycypacja). Wszystkie z nich umożliwiają realizację funkcji informacyjnej, komunikacyjnej, integracyjnej i transakcyjnej⁹. Wykonywanie przez samorząd terytorialny zadań z zakresu użyteczności publicznej (administracja świadcząca) współcześnie zyskało nowy tj. cyfrowy wymiar. Bezsporne jest to, na co zresztą uwagę zwraca Irena Lipowicz, że „legitymizacji administracji świadczącej należy poszukiwać w społecznej zasadzie gospodarki rynkowej, a także zasadach sprawiedliwości społecznej, solidarności i równości”¹⁰. Wszystkie z powyższych zasad znajdują swoje uzasadnienie również w działaniach elektronicznej administracji. Można pokusić się o stwierdzenie, że są one determinantami cyfryzacji w jednostkach samorządu terytorialnego.

W ramach e-zarządzania na poziomie lokalnym kluczową kwestię odgrywa załatwienie spraw mieszkańców danej wspólnoty samorządowej. Stąd też od organów jednostek samorządu terytorialnego oczekuje się wprowadzenia określonych programów i strategii działania w zakresie nieprzerwanego, efektywnego a przede wszystkim bezpiecznego świadczenia usług na odległość. Należy przyznać, że katalog działań, które samorządy wykonują za pomocą środków komunikacji elektronicznej jest szczególnie istotny z perspektywy petentów, są to m.in. doręczenia elektroniczne, możliwość składania pism, wniosków i deklaracji on-line, udostępnianie informacji publicznej (np. za pomocą Biuletynu Informacji Publicznej¹¹) czy szeroki katalog e-usług. W tym momencie warto odnotować, że rozwój e-administracji nie jest możliwy bez „wspierania inwestycji w dziedzinie informatyzacji (...) przeciwdziałania wykluczeniu cyfrowemu”, istotne jest „stanowienie przepisów prawnych pozwalających na rozwój usług elektronicznych, a także wdrażanie rozwiązań elektronicznych będących alternatywą do tradycyjnego załatwiania spraw urzędowych”¹². Podstawowe czynniki cyfryzacji usług publicznych na poziomie

⁹ E. Kuzionko-Ochrymiuk, *Koncepcje tradycyjnej i nowoczesnej administracji publicznej*, [w:] M. Romanowska (red.), *Współczesne problemy ekonomii: między teorią a praktyką gospodarczą w aspekcie różnorodności*, Częstochowa 2017, s. 27–28.

¹⁰ I. Lipowicz, *Samorząd terytorialny jako podmiot administracji świadczącej*, «Ruch Prawniczy, Ekonomiczny i Socjologiczny» 2015, t. 77, nr 3, s. 127.

¹¹ Zgodnie z art. 8 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902), Biuletyn Informacji Publicznej jest urzędowy publikator teleinformatyczny utworzonym w celu powszechnego udostępniania informacji publicznej, w postaci ujednoliconego systemu stron w sieci teleinformatycznej.

¹² P. Śwital, *Elektroniczne usługi publiczne dla obywateli – zarys problematyki*, «Przegląd Prawa Administracyjnego» 2022, nr 5, s. 143.

samorządowym uwarunkowane są polityką rządu w przedmiotowym zakresie. Oczywiście samorządy z uwagi na zasadę decentralizacji oraz subsydiarności, a także przysługujące im władztwo administracyjne posiadają możliwość samodzielnej realizacji e-usług i kształtowania stosownych polityk cyberbezpieczeństwa. Prowadzone działania mają na celu stworzenie specyficznych standardów funkcjonowania cyberprzestrzeni – odpowiednich dla tzw. warunków lokalnych. Intensyfikacja działań na polu informatyzacji oprócz świadczenia usług wysokiej jakości powinna zatem uwzględniać kwestie bezpieczeństwa informacji, systemów i sieci teleinformatycznych, zapewniać ochronę danych osobowych oraz wzmacniać kompetencje cyfrowe użytkowników¹³. Można zresztą zauważyć regularny wzrost zainteresowania problematyką informatyzacji i cyberbezpieczeństwa, do czego niewątpliwie przyczyniła się również pandemia COVID-19¹⁴. Zidentyfikowane powyżej czynniki cyfryzacji w jednostkach samorządu terytorialnego prowadzą do wspólnego mianownika, którym jest ustalenie potencjalnych cyberzagrożeń dla środowiska on-line a następnie przygotowanie działań ochronnych, polegających na wdrożeniu polityk cyberbezpieczeństwa. Ze względu na samodzielność i samorządność jednostek samorządu terytorialnego, warto podkreślić niemałą odpowiedzialność tych podmiotów w materii zapewnienia bezpiecznego środowiska on-line, a co za tym idzie w obszarze ochrony przedmiotowej (sieć, systemy, usługi) i podmiotowej (użytkownicy e-administracji). Przemysław Mijał wskazuje, że „zakres zadań musi być zatem dostosowany do wielkości i zdolności korporacji terytorialnej, która powinna zadania te wykonywać”¹⁵. Nie może zatem dziwić, że w pewnych przypadkach, z uwagi na ograniczone możliwości technologiczne, organizacyjne czy finansowe, cyberbezpieczeństwo na poziomie samorządów wymaga wsparcia podmiotów państwowych.

Cyberbezpieczeństwo a cyberzagrożenia w sektorze administracji publicznej

Standardem prawidłowego funkcjonowania administracji publicznej w kontekście realizacji zadań za pomocą środków komunikacji elektronicznej stało się

¹³ D. Cendrowicz, *Pomoc społeczna wobec zjawiska cyfryzacji. Wybrane zagadnienia*, [w:] P. Lisowski (red.), *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, Wrocław 2024, s. 796–797.

¹⁴ J. Maciejewski, *Dział administracji rządowej „informatyzacja” – aspekty strukturalno-ustrojowe*, «Folia Iuridica Universitatis Wratislaviensis» 2021, vol. 10, nr 1, s. 114.

¹⁵ P. Mijał, *Zasada pomocniczości jako wyznacznik roli prawotwórczej samorządu terytorialnego*, «Przegląd Prawa Konstytucyjnego» 2014, nr 2(18), s. 225.

włączenie zagadnień z zakresu cyberbezpieczeństwa. Powyższe ma świadczyć o wysokim poziomie bezpieczeństwa cyberprzestrzeni. Ustawodawca jasno wskazuje, że cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania, które mogą naruszyć poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy¹⁶. Dla sektora administracji publicznej oznacza to, że wszelkie czynności podejmowane w obszarze ochrony cyberprzestrzeni mają zapewnić w równym stopniu bezpieczeństwo informacyjne (treści cyfrowych), w tym ochronę danych osobowych, a także infrastruktury krytycznej, sieci, systemów i urządzeń. Warto przy tym zauważyć, że ochrona przed cyberzagrożeniami dotyczy całego procesu komunikacyjnego czyli wszystkich użytkowników e-administracji, do których należą zarówno podmioty administrujące (urzędnicy) jak i te znajdujące się poza nią (petenci). Z uwagi na różnorodny charakter cyberzagrożeń, do których zaliczają się w szczególności zagrożenia bezpieczeństwa informacyjnego, cyberprzestępczość czy cyberinwigilacja warunkiem *sine qua non* jest wskazanie instrumentów prawnych wspierających wzrost poziomu cyberbezpieczeństwa¹⁷. Informatyzacja zadań publicznych doprowadziła do zwiększenia kompetencji jednostek samorządu terytorialnego, przypisano im bowiem nowe zadania z zakresu elektronicznej administracji. Faktycznie, co zauważa Aleksandra Monarcha-Matlak, technologie informacyjno-komunikacyjne zmodernizowały administrację publiczną. Autorka trafnie wskazuje, że „sensowne z punktu widzenia prawa konstytucyjnego i administracyjnego, będzie rozbudowanie kontaktów na linii obywatel – urząd elektroniczny, gdzie zadania urzędów będą dopasowane do indywidualnych potrzeb obywateli”¹⁸. Cyberprzestrzeń jest niezwykle atrakcyjnym miejscem przeprowadzania ataków zarówno w skali mikro, jak i w skali makro. Uniwersalny charakter cyberprzestrzeni i cyberbezpieczeństwa determinuje sposób wykonywania zadań przez organy administracji samorządowej. Umiejętność zarządzania informacją i uwrażliwienie na wszelkiego rodzaju incydenty stanowią podstawowe elementy polityki cyberbezpieczeństwa. Ponadto, nie ulega również wątpliwości to, że ze względu na potencjalne ryzyko cyberzagrożeń oraz ich faktyczne skutki wymagana jest konkretyzacja bądź modyfikacja obowiązków na rzecz cyberbezpieczeństwa i ulepszanie systemów zapewniających

¹⁶ Zob. art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2024 r. poz. 834, dalej u.k.s.c.

¹⁷ K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, «Cybersecurity and Law» 2019, vol. 2, nr 2, s. 20–21.

¹⁸ A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, «Lingwistyka Stosowana» 2017, t. 24(4), s. 144.

ochronę środowiska on-line¹⁹. To z kolei wiąże się z koniecznością wsparcia finansowego podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa cyberprzestrzeni.

W odniesieniu do specyfiki zadań administracji samorządowej związanych *stricte* z zapewnieniem cyberbezpieczeństwa, fundamentalne znaczenie należy przypisać rozwiązaniom zawartym w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne. Powyższe stwierdzenie wydaje się w pełni uzasadnione z uwagi na rolę i zadania administracji w takich obszarach jak m.in.: ustalanie minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i określanie Krajowych Ram Interoperacyjności systemów teleinformatycznych, wymiana informacji drogą elektroniczną, w tym dokumentów elektronicznych, pomiędzy podmiotami publicznymi a podmiotami niebędącymi podmiotami publicznymi, funkcjonowania elektronicznej platformy usług administracji publicznej i publicznego systemu identyfikacji elektronicznej oraz świadczenia usługi podpisu zaufanego²⁰. Powyższe umożliwia stworzenie bezpiecznych warunków świadczenia e-usług, automatyzację procedur administracyjnych, buduje pozytywny wizerunek e-administracji. Fundamentalnym warunkiem jest również kwestia kompetencji cyfrowych, ponieważ „obie strony, czyli urząd i obywatel, muszą chcieć aktywnie korzystać z systemów informatycznych, a także posiadać przy tym niezbędne techniczne umiejętności do korzystania z elektronicznych platform załatwianych spraw²¹”. Z pewnością określenie priorytetów informatyzacji sprzyja wskazaniu kluczowych elementów cyberbezpieczeństwa, zarówno tych o organizacyjno-prawnym, jak i technologicznym znaczeniu.

Adresatami ustawy o krajowym systemie cyberbezpieczeństwa są również jednostki samorządu terytorialnego. Przypisanie obowiązków z zakresu cyberbezpieczeństwa wynika z dwóch podstawowych kwestii, tj. z intensyfikacji zadań w ramach elektronicznej administracji (e-wnioski, e-formularze, doręczenia elektroniczne, dedykowane platformy usług elektronicznych) oraz wzroście incydentów²² i cyberzagrożeń, m.in. cyberprzestępczości. Zdecydowany

¹⁹ E. Żywucka-Kozłowska, R. Dziembowski, *Wokół definicji cyberbezpieczeństwa*, «Cybersecurity and Law» 2023, vol. 10, nr 2, s. 130–131.

²⁰ Zob. art. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. z 2019 r. poz. 60, 534.

²¹ P. Romaniuk, *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, «Studia Prawnoustrojowe» 2022, nr 58, s. 449–450.

²² Incydem jest zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo; u.k.s.c. wyróżnia incydenty krytyczne, poważne, istotne i w podmiocie publicznym; zob. art. 2 pkt 5–9 u.k.s.c.

wzrost cyberataków nastąpił w dobie pandemii COVID-19. Zaobserwowana wówczas intensyfikacja takich cyberzagrożeń jak oszustwa internetowe, ataki typu *phishing*, złośliwe oprogramowania (np. ransomware czy DDoS) skłania do refleksji nad aktualizacją polityk cyberbezpieczeństwa (szczególnie pod kątem działań operacyjno-technicznych). Ochrona zasobów informacyjnych powinna skupiać się na uniemożliwieniu osobom trzecim dostępu do sieci i systemów teleinformatycznych (treści cyfrowych). Bezskuteczność działań administracji samorządowej może skutkować włamaniem do e-zbiorów, następnie nielegalnym wykorzystaniem informacji – ich udostępnieniem, sfałszowaniem czy nawet zniszczeniem²³.

Wolą ustawodawcy, jednostki samorządu terytorialnego oraz ich związki zaliczono do podmiotów krajowego systemu cyberbezpieczeństwa²⁴. W praktyce oznacza to, że szereg obowiązków (o charakterze obligatoryjnym bądź fakultatywnym) związanych m.in. z możliwością wyznaczenia jednej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne (art. 21 ust. 3 u.k.s.c.) oraz z zakresu zarządzania²⁵, zgłaszania i obsługi²⁶ incydentu (art. 22 u.k.s.c.) został ściśle przypisany samorządom. Ewa Maria Włodyka podkreśla ważną rolę działań władzy centralnej w kwestii poprawy cyberbezpieczeństwa na poziomie samorządowym. Nie oznacza to jednak odebrania kompetencji, ale jak wskazuje Autorka przyznanie wsparcia infrastrukturalnego i edukacyjnego, istotnego zarówno w kontekście działań zapobiegawczych i naprawczych „na rzecz bezpiecznego funkcjonowania JST w cyberprzestrzeni”²⁷. Wsparcie, o którym mowa ma wydźwięk prawny, organizacyjny, społeczny i finansowy, co można zauważyć na przykładzie rozwiązań zawartych w projekcie „Cyberbezpieczny Samorząd”.

²³ D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, «Prawo w działaniu. Sprawy karne» 2023, nr 53, s. 101–102.

²⁴ Zob. art. 4 pkt 7 u.k.s.c. w z art. 9 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. z 2024 r. poz. 858.

²⁵ Art. 2 pkt 18 u.k.s.c. stanowi że zarządzanie incydentem oznacza obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu.

²⁶ Zgodnie z art. 2 pkt 10 u.k.s.c. obsługa incydentu to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.

²⁷ E. M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, «Cybersecurity and Law» 2022, vol. 7, nr 1, s. 218.

Przegląd instrumentów prawnofinansowych wspierających wzrost poziomu cyberbezpieczeństwa w administracji samorządowej – projekt „Cyberbezpieczny Samorząd”

W wywodzie na temat cyberbezpieczeństwa w administracji samorządowej, należy wskazać na istotne znaczenie władztwa administracyjnego. Władczy charakter działań pozwala na przyjęcie określonej strategii w zakresie zapewnienia transparentności i skuteczności funkcjonowania elektronicznej administracji, innowacyjności i interoperacyjności e-usług. W przypadku pojawienia się cyberzagrożenia organy administracji publicznej mogą (i to w trybie natychmiastowym) podjąć stosowne działania natury faktycznej i prawnej. Jednocześnie e-administracja ma na względzie standardy wynikające z prawa do dobrej administracji²⁸. Cyfryzacja usług publicznych wymagała zatem konkretyzacji obowiązków administracji w zakresie zapewnienia cyberbezpieczeństwa. W odniesieniu do administracji samorządowej zaistniała również konieczność wdrożenia odpowiednich instrumentów prawnofinansowych wspierających wzrost poziomu cyberbezpieczeństwa. Jednym z nich jest projekt „Cyberbezpieczny Samorząd”, który ma w pewnym stopniu wzmocnić odporność na cyberzagrożenia, w tym zwiększyć poziom bezpieczeństwa informacji w samorządach. Głównym założeniem projektu jest „zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego”, które ma nastąpić poprzez „wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych”²⁹. Cyberbezpieczeństwo stało się komponentem zarządzania bezpieczeństwem publicznym na poziomie samorządowym. Co za tym idzie, oprócz wymogów formalno-prawnych jednostki samorządu terytorialnego zostały zobligowane do wprowadzenia kosztownych zmian natury organizacyjnej i technologicznej, co wiąże się ze wzrostem kosztów obsługi i utrzymania systemów i sieci teleinformatycznych, a także innych działań z zakresu cyberbezpieczeństwa (np. doskonalenia kompetencji miękkich pracowników urzędów). Tak więc „dość często kwestie finansowe nie sprzyjają samodzielności władz lokalnych i regionalnych” co prowadzi do tego, że „dość duża część środków na realizację zadań z zakresu bezpieczeństwa publicznego, niestety, jest rozłożona z pominięciem szczebla samorządowego”³⁰. Celem projektu „Cyberbezpieczny Samo-

²⁸ D. Skoczylas, *Krajowy system cyberbezpieczeństwa*, Warszawa 2023, s. 343–344.

²⁹ Centrum Projektów Polska Cyfrowa, *Cyberbezpieczny...*, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd> (1.07.2024).

³⁰ P. Romaniuk, *Wybrane elementy konstrukcji zarządzania bezpieczeństwem publicznym w jednostkach samorządu terytorialnego*, «Cybersecurity and Law» 2024, vol. 12, nr 2, s. 172.

rząd” jest wsparcie gmin, powiatów i województw w zakresie wdrożenia lub aktualizacji polityk bezpieczeństwa informacji, środków zarządzania ryzykiem w cyberbezpieczeństwie oraz mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni³¹. Pozytywny wydzźwięk projektu dotyczy także ograniczenia ekskluzji cyfrowej, problemu wykluczenia cyfrowego, do którego oprócz braku stosownej wiedzy i umiejętności należą również kwestie indywidualne, takie jak „biegłość poruszania się w wirtualnej rzeczywistości, niechęć do internetu jako takiego (tzw. autowykluczenie)”³². Z perspektywy administracji publicznej, projekt ma przysłużyć się do wzrostu poziomu wiedzy, umiejętności i kompetencji personelu. Projekt kładzie również nacisk na konieczność przeprowadzenia w jednostkach samorządu terytorialnego audytów Systemu Zarządzania Bezpieczeństwem Informacji, które będą potwierdzały uzyskanie wyższego poziomu odporności na cyberzagrożenia.

Wychodząc naprzeciw potrzebom samorządu terytorialnego NASK – Państwowy Instytut Badawczy opracował i udostępnił w formie poradnika, publikację na temat projektu „Cyberbezpieczny Samorząd”. Poradnik zawiera opis podstawowych zagadnień formalno-prawnych, organizacyjnych i technicznych umożliwiających ocenę poziomu cyberbezpieczeństwa w danej jednostce. Przedstawiono w nim przykłady przedsięwzięć na rzecz wzmocnienia odporności, zapobiegania, wykrywania i reagowania na incydenty, odnosi się także do problematyki interoperacyjności usług, ochrony danych osobowych, wzmacniania kompetencji cyfrowych i aspektów finansowych³³. Jednym z kluczowych aspektów wskazanych w projekcie „Cyberbezpieczny Samorząd” jest kompleksowe podejście do identyfikacji, zarządzania oraz ochrony informacji dzięki wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji oraz podniesienia poziomu świadomości cyberbezpieczeństwa. Niestety, pomimo postępu technologicznego, problem ograniczonych kompetencji cyfrowych występuje zarówno wśród pracowników administracji samorządowej, którzy korzystają z e-zasobów i generują treści w formie elektronicznej, jak i pozostałych użytkowników e-administracji (petentów)³⁴. W rozdziale 6 poradnika przedstawiono wykaz wymagań bezpieczeństwa dla podmiotów publicznych. Zaliczono do nich m.in.: wdrożenie systemu zarządzania bezpieczeństwem informacji; zapewnienie zgodności

³¹ Centrum Projektów Polska Cyfrowa, *Cyberbezpieczny...*, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd> (1.07.2024).

³² A. Ziółkowska, *Wrażliwość społeczna władzy w kontekście dostępności cyfrowej administracji publicznej*, [w:] S. Dudzik, I. Kawka, R. Śliwa (red.), *Obywatel w centrum działań e-administracji w Unii Europejskiej*, Kraków 2023, s. 126.

³³ NASK – Państwowy Instytut Badawczy, *Poradnik – Cyberbezpieczny samorząd*, Warszawa 2023, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd> (1.07.2024).

³⁴ J. Gerwatowski, *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, «Studia Prawnoustrojowe» 2019, nr 44, s. 105.

Polityki Bezpieczeństwa Informacji z innymi regulacjami zewnętrznymi oraz wewnętrznymi (stały monitoring i aktualizacja w razie potrzeby); inwentaryzację aktywów (m.in. sprzętu i oprogramowania) i ich konfigurację; przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz wdrażanie odpowiednich środków ochrony przed cyberzagrożeniami; określenie roli i odpowiedzialności podmiotów zaangażowanych w działania z zakresu bezpieczeństwa informacji (w zakresie nadzoru, weryfikacji uprawnień i kwalifikacji oraz konieczności przeprowadzania szkoleń); monitorowanie zmian w organizacji (w tym nadawanie uprawnień użytkowników); wzmacnianie kompetencji cyfrowych (m.in. szkolenia, edukacja na rzecz cyberbezpieczeństwa); rejestrowanie i monitoring zdarzeń; wykrywanie zdarzeń niepożądanych w infrastrukturze IT (i zapobieganie im); pracę z urządzeniami mobilnymi; potrzebę zabezpieczenia danych (bezpieczeństwo fizyczne i technologiczne); aktualizowanie oprogramowań; politykę ochrony danych osobowych (w szczególności zasady uwierzytelniania i autoryzacji); zarządzanie podatnościami technicznymi; zgłaszanie, zarządzanie i obsługę incydentów; kwestie zapisu działań w systemach³⁵. O czym była już mowa powyżej, administracja samorządowa posiada spektrum możliwości, ale i obowiązków w materii kompleksowego zarządzania informacją i załatwiania spraw publicznych w cyberprzestrzeni. Istota zawiera się w obszarze podejmowania decyzji, *stricte* jak wskazuje Kamil Mrocza, „kluczowe wyzwania w związku z rozpowszechnianiem się mechanizmów e-decydowania dotyczą wzmocnienia z poziomu rządowego samorządów we wdrażaniu mechanizmów, narzędzi i standardów w zakresie cyberbezpieczeństwa”³⁶. Bez cienia wątpliwości takim wsparciem obok kwestii organizacyjno-prawnych są te o charakterze finansowym.

Zgodnie z przyjętą koncepcją projektu „Cyberbezpieczny Samorząd” jednostki samorządu terytorialnego mogły otrzymać dofinansowanie w formie grantu, którego wysokość wynosiła: od 200 000 zł do 850 000 zł – dla gmin oraz do 850 000 zł dla powiatów i samorządów wojewódzkich. Nabór wniosków w projekcie zakończono w dniu 14 grudnia 2023 r. o godz. 16:00³⁷. W tym miejscu należy wskazać, że podmioty administracji publicznej (na poziomie centralnym oraz regionalnym) zostały objęte dyrektywą NIS 2³⁸, co oznacza,

³⁵ NASK – Państwowy Instytut Badawczy, *Poradnik – Cyberbezpieczny*, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (1.07.2024).

³⁶ K. Mrocza, *Uwarunkowania i kierunki zmian w procesach decydowania publicznego na szczeblu samorządowym w związku z pandemią koronawirusa*, «Polityka i Społeczeństwo» 2020, nr 4(18), s. 89.

³⁷ Centrum Projektów Polska Cyfrowa, *Cyberbezpieczny*, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (1.07.2024).

³⁸ Zgodnie z art. 2 ust. 2 lit. f) ppkt (i) i ppkt (ii) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego

że został im przypisany szeroki katalog obowiązków z zakresu m.in. wdrożenia odpowiednich środków mających na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa, zarządzania ryzykiem w cyberbezpieczeństwie oraz zgłaszania incydentów. W świetle Dyrektywy NIS 2 zadaniem administracji również na poziomie samorządowym „jest zapewnianie niezakłóconego świadczenia usług kluczowych oraz odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług”³⁹. W ramach projektu „Cyberbezpieczny Samorząd” określono wydatki w trzech obszarach: organizacyjnym (m.in. opracowanie, wdrożenie i przegląd dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, przeprowadzanie audytów, wdrożenie/aktualizacja Polityk Bezpieczeństwa Informacji), kompetencyjnym (szkolenia dedykowane z zakresu cyberbezpieczeństwa i budujące świadomość cyberzagrożeń dla pracowników jednostek samorządu terytorialnego, kadry zarządzającej, informatyków; testy socjotechniczne) oraz technicznym (m.in. zakup, wdrożenie i utrzymanie urządzeń, systemów teleinformatycznych, oprogramowania, usług wsparcia, rozwiązań z zakresu monitorowania cyberbezpieczeństwa, inteligentnych systemów rozpoznawania zagrożeń w cyberprzestrzeni)⁴⁰. W istocie, z uwagi na szeroki katalog form wsparcia (instrumentów prawnofinansowych) projekt „Cyberbezpieczny Samorząd” może w pewnym stopniu wzmocnić odporność na cyberzagrożenia, w tym zwiększyć poziom bezpieczeństwa informacji w samorządach.

Zakończenie

Transformacja cyfrowa wpłynęła na sposób funkcjonowania administracji publicznej, zarówno na poziomie centralnym, jak i samorządowym. Z uwagi na zasady decentralizacji i subsydiarności jednostki samorządu terytorialnego posiadają określoną samodzielność i niezależność w zakresie kształtowania

wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE 2022, L 333/80), podmiot jest podmiotem administracji publicznej na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym lub na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą.

³⁹ K. Chałubińska-Jentkiewicz, M. Nowikowska, *Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2), «Cybersecurity and Law» 2024, vol. 12, nr 2, s. 22.*

⁴⁰ NASK – Państwowy Instytut Badawczy, *Poradnik – Cyberbezpieczny*, <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (1.07.2024).

zasad elektronicznej administracji. Modernizacja administracji samorządowej stała się faktem, niemniej jednak wymaga dalszego udoskonalenia, m.in. w obszarze rozwoju infrastruktury teleinformatycznej, wzmocnienia kompetencji cyfrowych urzędników, dostępności cyfrowej, a przede wszystkim opracowania modelowych rozwiązań w kwestii polityki cyberbezpieczeństwa. Ograniczone możliwości, wynikające z problemów natury organizacyjno-prawnej lub technologicznej być może pomogą rozwiązać instrumenty prawnofinansowe zawarte w projekcie „Cyberbezpieczny Samorząd”. Założeniem projektu jest wzmocnienie odporności na cyberzagrożenia, w tym zwiększenie poziomu bezpieczeństwa informacji w samorządach. Samorządy potrzebują zewnętrznego wsparcia prawnofinansowego w tak istotnej dziedzinie jaką jest cyberbezpieczeństwo z uwagi na kilka czynników, do których należą intensyfikacja działań w ramach e-administracji, wzrost incydentów i cyberzagrożeń oraz zaangażowanie w politykę cyberbezpieczeństwa na podstawie Dyrektywy NIS 2.

Reasumując, jednostki samorządu terytorialnego, które zdecydowały się aplikować do projektu „Cyberbezpieczny Samorząd” uzyskały szansę na ogromne wsparcie działań z zakresu cyberbezpieczeństwa. Niemniej jednak przyznanie jakichkolwiek form wsparcia, wymaga ich umiejętnego wykorzystania, wprowadzenia długofalowej strategii działania, monitoringu i aktualizacji polityk cyberbezpieczeństwa w odniesieniu do potencjalnych cyberzagrożeń. Projekt „Cyberbezpieczny Samorząd” może zatem w pewnym stopniu wzmocnić odporność na cyberzagrożenia, w tym zwiększyć poziom bezpieczeństwa informacji w samorządach. Powodzenie w przedmiotowym zakresie zależy jednak w dużym stopniu od umiejętności zarządczych kierowników jednostek samorządu terytorialnego i kompetencji cyfrowych pracowników samorządowych.

Bibliografia

- Cendrowicz D., *Pomoc społeczna wobec zjawiska cyfryzacji. Wybrane zagadnienia*, [w:] P. Lisowski (red.), *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, Wrocław 2024.
- Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, «Cybersecurity and Law» 2019, vol. 2, nr 2.
- Chałubińska-Jentkiewicz K., Nowikowska M., *Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2)*, «Cybersecurity and Law» 2024, vol. 12, nr 2.
- Dudzińska A., Gontarczyk M., *E-administracja w Polsce*, «Studia Politologiczne» 2013, vol. 27.
- Dutkiewicz G., *Samorząd terytorialny w kontekście zasady pomocniczości w nauczaniu społecznym Kościoła katolickiego*, «The Religious Studies Review» 2019, nr 3(273).

- Gerwatowski J., *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, «Studia Prawnoustrojowe» 2019, nr 44.
- Harasimiuk D. E., Braun T., *Nowa złożoność. Dialog demokratyczny w warunkach transformacji cyfrowej*, «Przegląd Konstytucyjny» 2021, nr 4.
- Jastrzębska K., *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, Warszawa 2018.
- Kuzionko-Ochrymiuk E., *Koncepcje tradycyjnej i nowoczesnej administracji publicznej*, [w:] M. Romanowska (red.), *Współczesne problemy ekonomii: między teorią a praktyką gospodarczą w aspekcie różnorodności*, Częstochowa 2017.
- Lipowicz I., *Samorząd terytorialny jako podmiot administracji świadczącej*, «Ruch Prawniczy, Ekonomiczny i Socjologiczny» 2015, t. 77, nr 3.
- Maciejewski J., *Dział administracji rządowej „informatyzacja” – aspekty strukturalno-ustrojowe*, «Folia Iuridica Universitatis Wratislaviensis» 2021, vol. 10, nr 1.
- Mijał P., *Zasada pomocniczości jako wyznacznik roli prawotwórczej samorządu terytorialnego*, «Przegląd Prawa Konstytucyjnego» 2014, nr 2(18).
- Monarcha-Matlak A., *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, «Lingwistyka Stosowana» 2017, t. 24(4).
- Mrocza K., *Uwarunkowania i kierunki zmian w procesach decydowania publicznego na szczeblu samorządowym w związku z pandemią koronawirusa*, «Polityka i Społeczeństwo» 2020, nr 4(18).
- Pilarz K., *System planowania przestrzennego wobec procesów informatyzacji i cyfryzacji administracji publicznej*, [w:] P. Lisowski (red.), *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, Wrocław 2024.
- Romaniuk P., *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, «Studia Prawnoustrojowe» 2022, nr 58.
- Romaniuk P., *Wybrane elementy konstrukcji zarządzania bezpieczeństwem publicznym w jednostkach samorządu terytorialnego*, «Cybersecurity and Law» 2024, vol. 12, nr 2.
- Sieklucki D., *Decentralizacja – podstawowe zagadnienia teoretyczne*, «Politeja» 2022, nr 2(77).
- Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, «Prawo w działaniu. Sprawy karne» 2023, nr 53.
- Skoczylas D., *Krajowy system cyberbezpieczeństwa*, Warszawa 2023.
- Śwital P., *Elektroniczne usługi publiczne dla obywateli – zarys problematyki*, «Przegląd Prawa Administracyjnego» 2022, nr 5.
- Włodyka E. M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, «Cybersecurity and Law» 2022, vol. 7, nr 1.
- Ziółkowska A., *Wrażliwość społeczna władzy w kontekście dostępności cyfrowej administracji publicznej*, [w:] S. Dudzik, I. Kawka, R. Śliwa (red.), *Obywatel w centrum działań e-administracji w Unii Europejskiej*, Kraków 2023.
- Żywucka-Kozłowska E., Dziembowski R., *Wokół definicji cyberbezpieczeństwa*, «Cybersecurity and Law» 2023, vol. 10, nr 2.