UNIWERSYTET ZIELONOGÓRSKI

DYSKURS PRAWNICZY I ADMINISTRACYJNY 1/2025 ISSN 2657-926X

Dominika Skoczylas
Uniwersytet Szczeciński
ORCID 0000-0003-1231-8078
dominika.skoczylas@usz.edu.pl

Dyrektywa NIS 2 a cyberbezpieczeństwo administracji publicznej

Słowa kluczowe: administracja publiczna, cyberbezpieczeństwo, dyrektywa NIS 2, krajowy system cyberbezpieczeństwa, podmioty kluczowe

Streszczenie. Artykuł poświęcony jest problematyce cyberbezpieczeństwa administracji publicznej. Celem jest scharakteryzowanie działań podejmowanych przez podmioty administracji publicznej w zakresie zapewnienia cyberbezpieczeństwa usług świadczonych w sektorze publicznym. Nie ulega wątpliwości, że zwiększenie odporności sektora administracji publicznej na cyberzagrożenia stanowi kluczowy element efektywności i skuteczności realizacji zadań publicznych. Rozważania w przedmiotowym zakresie przeprowadzono, opierając się na przepisach obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa oraz dyrektywy NIS 2, na podstawie której podmioty administracji publicznej uznano za tzw. podmioty kluczowe dla utrzymania krytycznej działalności społecznej lub gospodarczej. W związku z wprowadzeniem przedmiotowej dyrektywy niezbędna stała się nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. Przedmiotem artykułu jest przedstawienie i ocena aktualnych regulacji prawnych dotyczących cyberbezpieczeństwa administracji publicznej oraz wskazanie zasadności zmian wprowadzonych na podstawie dyrektywy NIS 2. Analiza tematu pozwoli odpowiedzieć na pytania, czy dyrektywa NIS 2 zapewni wprowadzenie jednolitych środków mających na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii oraz jakie kwestie powinna uwzględniać polityka cyberbezpieczeństwa administracji publicznej. Mając na uwadze powyższe, w artykule zostaną przedstawione możliwości zastosowania nowych technologii w administracji publicznej. Wyjaśnione zostaną również podstawowe pojęcia wprowadzone na mocy dyrektywy NIS 2. Autorka pracy zgadza się z aktualną polityką Unii Europejskiej, zgodnie z którą podmioty administracji publicznej uznano za tzw. podmioty kluczowe, tym samym popiera wskazanie skoordynowanych ram w zakresie cyberbezpieczeństwa administracji publicznej. W pracy wykorzystano metodę dogmatycznoprawną.

The NIS 2 Directive and the cybersecurity of public administrations

Keywords: public administration, cybersecurity, NIS 2 Directive, national cybersecurity system, essential entities

Summary. This article is devoted to the issue of cybersecurity of public administration. The aim is to characterise the actions taken by public administration entities in ensuring the cybersecurity of public sector services. There is no doubt that increasing the resilience of the public administration sector to cyberthreats is a key element in the efficiency and effectiveness of public tasks. The discussion in this regard is based on the provisions of the current Act on the National Cybersecurity System and the NIS 2 Directive, under which public administration entities are recognised as so-called essential entities for maintaining critical social or economic activities. Following the introduction of this

Directive, it became necessary to amend the National Cybersecurity System Act. The subject of this article is to present and assess the current legal regulations on public administration cybersecurity and to indicate the rationale for the changes introduced on the basis of the NIS 2 Directive. The analysis of the topic will allow answering the questions: will the NIS 2 Directive allow the introduction of uniform measures to achieve a high common level of cybersecurity across the Union? and secondly, what issues should be taken into account in a public administration's cybersecurity policy? With the above in mind, the article will present the possibilities of applying new technologies in public administration. The basic concepts introduced by the NIS 2 Directive will also be explained. The author of the paper agrees with the current policy of the European Union, according to which public administration entities have been recognised as so-called „essential entities", thus supporting the identification of a coordinated framework for public administration cybersecurity. The paper uses a dogmatic-legal method.

Wprowadzenie

Niekwestionowanie powszechne zastosowanie środków komunikacji elektronicznej ukształtowało nowy model administracji publicznej. Modernizacja sektora publicznego nie jest jednak utożsamiana wyłącznie ze zmianami na płaszczyźnie technologicznej, ale przede wszystkim organizacyjno-prawnej. Elektroniczna administracja poprzez zastosowanie nowoczesnych technologii informacyjno-komunikacyjnych (dalej: ICT) może w sposób łatwy, a jednocześnie efektywny świadczyć usługi użyteczności publicznej na odległość. Tym samym, na co zwraca uwagę Maciej Błażewski, szczególna zaleta e-administracji przejawia się w jej powszechności, nieskrępowanej komunikacji pomiędzy organami administracji publicznej a organami administracji publicznej (komunikacja wewnątrz struktur administracji) oraz podmiotami publicznymi a obywatelami (komunikacja zewnętrzna). Autor dodaje, że „zasada powszechności dotyczy dwóch aspektów działania administracji publicznej: stosowania systemów teleinformatycznych oraz zapewnienia spójności tych systemów"[1]. Powyższe stwierdzenie wydaje się zasadne, biorąc pod uwagę takie cechy administracji, jak jej dostępność, fachowość, efektywność, skuteczność czy poszanowanie interesu publicznego. W tym miejscu należy zaznaczyć, że równie istotny wpływ na informatyzację życia publicznego miały (i mają) potrzeby społeczeństwa informacyjnego. Można sformułować tezę, że środki komunikacji elektronicznej w znaczącym stopniu kształtują relacje społeczeństwa z instytucjami publicznymi, jednocześnie kreują wizerunek otwartej i przyjaznej administracji, zapewniają transparentność i skuteczność działań[2].

Jednakże obok niewątpliwie pozytywnych aspektów zastosowania nowych technologii w administracji publicznej należy zwrócić uwagę na czynniki ograniczające bądź uniemożliwiające świadczenie e-usług, takie jak: nieodpowiednio przygoto-

[1] M. Błażewski, *Zasada powszechności elektronicznej administracji*, „Folia Iuridica Universitatis Wratislaviensis" 2018, vol. 7(1), s. 230-231.

[2] J. Ejdys, *Zaufanie do technologii w e-administracji*, Białystok 2018, s. 16.

wana infrastruktura teleinformatyczna czy niskie kompetencje cyfrowe pracowników administracji publicznej. Aktualnie warunkiem *sine qua non* funkcjonowania administracji publicznej jest cyberbezpieczeństwo. Cyberprzestrzeń jest „nową jakościowo płaszczyzną zagrożeń"[3], a metody, którymi posługują się hakerzy, cyberprzestępcy czy cyberterroryści są coraz bardziej różnorodne. W efekcie zakłócenia sieci i systemów informatycznych uniemożliwiają realizację zadań publicznych. Polityka cyberbezpieczeństwa ma kluczowe znaczenie w kontekście bezpieczeństwa e-usług publicznych, nie dziwi zatem, że na mocy dyrektywy NIS 2 rozszerzono krąg podmiotów, które świadczą usługi o kluczowym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Podmioty administracji publicznej uznano za tzw. podmioty kluczowe i przypisano im istotne zadania w obszarze cyberbezpieczeństwa. Celem artykułu jest scharakteryzowanie działań podejmowanych przez podmioty administracji publicznej w zakresie zapewnienia cyberbezpieczeństwa usług świadczonych w sektorze publicznym. Ponadto przedmiotem rozważań jest analiza aktualnych regulacji prawnych dotyczących cyberbezpieczeństwa administracji publicznej oraz wskazanie najważniejszych zmian wprowadzonych na mocy dyrektywy NIS 2.

1. O modernizacji administracji publicznej – zastosowanie nowych technologii i informatyzacja życia publicznego

Bez cienia wątpliwości informatyzacja wpłynęła na modernizację administracji publicznej. Popularyzacja wykorzystywania środków komunikacji elektronicznej w sektorze publicznym pozwoliła ukształtować zasady cyfryzacji i informatyzacji w skali makro, zarówno w państwach członkowskich Unii Europejskiej, jak i na poziomie międzynarodowym. Fundamentalne znaczenie miało w tym przypadku przygotowanie określonych kanałów komunikacji wewnętrznej (pomiędzy organami administracji publicznej) oraz zewnętrznej (stosunki administracyjnoprawne pomiędzy instytucjami publicznymi a przedsiębiorcami albo obywatelami). Niewątpliwie do zalet e-administracji obok interoperacyjności, powszechności czy transgraniczności należy również prostota i szybkość świadczenia różnorodnego rodzaju usług na odległość, dzięki temu „e-usługi rozumiane są jako nowoczesna metoda dystrybucji usług publicznych, które stają się dość popularne i zastępują tradycyjną formę załatwiania spraw administracyjnych"[4]. Działania w zakresie informatyzacji życia publicznego promowane są przez Unię Europejską. Warto w tym miejscu

[3] P. Lubiewski, *Szczególna dynamika zmian współczesnych zagrożeń w sferze bezpieczeństwa publicznego na przykładzie cyberprzestrzeni*, „Zeszyty Naukowe SGSP" 2020, nr 76/4, s. 54.

[4] P. Romaniuk, *Tradycje i przyszłość administracji publicznej w zakresie rozwoju e-usług*, „Journal of Modern Science" 2020, t. 1/44, s. 271.

wspomnieć o programie „Cyfrowa Europa" (2021-2027)[5]. W motywie 51 programu wskazano, że modernizacja europejskich administracji publicznych stanowi jeden z zasadniczych priorytetów w dążeniu do udanego wdrożenia jednolitego rynku cyfrowego, podkreślono również potrzebę intensyfikacji transformacji administracji publicznych oraz konieczność zapewnienia obywatelom łatwego, zaufanego i bezproblemowego dostępu do usług publicznych. Dodatkowo zaakcentowano cele szczegółowe transformacji cyfrowej, takie jak m.in. cyberbezpieczeństwo i zaufanie, rozwój kompetencji cyfrowych czy interoperacyjność usług, które stanowią istotne determinanty funkcjonowania sektora administracji publicznej[6]. Dostęp do wysokiej jakości usług cyfrowych jest kluczowym zadaniem organów administracji publicznej. Jednakże należy podkreślić, że nie będzie on możliwy w pełni, gdy nie zostaną wprowadzone kompleksowe rozwiązania prawne w zakresie cyberbezpieczeństwa. Współcześnie bowiem to właśnie cyberzagrożenia stanowią czynniki ograniczające czy wręcz uniemożliwiające efektywne i skuteczne świadczenie usług na odległość. Niezbędne będą w tym aspekcie nie tylko zmiany o charakterze legislacyjnym czy te związane z dostępnością cyfrową, ale również podniesienie kompetencji cyfrowych urzędników[7].

Stosownie do powyższych rozważań, trafny wydaje się pogląd przedstawiony przez Aleksandrę Monarchę-Matlak, która wskazuje, że „prawo komunikacji elektronicznej powoduje, że powstaje nowa jakość działania, nowy sposób pracy i nowe zmiany organizacyjne"[8]. W ślad za Autorką należy przyznać, że w odniesieniu do warunków technologicznych musi istnieć odpowiednia infrastruktura teleinformatyczna. Natomiast struktury administracji publicznej powinny być tak zorganizowane, aby kompetencje cyfrowe poszczególnych pracowników były „kompatybilne" z zakresem zadań, które będą realizowane za pomocą ICT. Innymi słowy, kwestie technologiczne i organizacyjne są równie ważne co uwarunkowania prawne w materii informatyzacji. W polskim systemie prawnym już od dawna obowiązują przepisy, które określają m.in. minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych, funkcjonowanie elektronicznej platformy usług administracji (ePUAP), publicznego systemu iden-

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 (Tekst mający znaczenie dla EWG), Dz.Urz. UE L Nr 166, s. 1).

[6] Art. 3 ust. 2 Programu Cyfrowa Europa określa pięć wzajemnie powiązanych celów szczegółowych, do których należą: obliczenia wielkiej skali, sztuczna inteligencja, cyberbezpieczeństwo i zaufanie, zaawansowane umiejętności cyfrowe, wdrażanie i optymalne wykorzystanie zdolności cyfrowych i interoperacyjność.

[7] D. Skoczylas, *Dostępność cyfrowa determinantą zmian w funkcjonowaniu administracji publicznej*?, „Studia Administracji i Bezpieczeństwa" 2022, nr 13, t. 13, s. 124-125.

[8] A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, „Lingwistyka Stosowana" 2017, issue 24, s. 144.

tyfikacji elektronicznej czy zasady świadczenia usługi podpisu zaufanego[9], krajową infrastrukturę zaufania, w tym działalność dostawców usług zaufania, oraz krajowy schemat identyfikacji elektronicznej, zasady określania i wykorzystywania standardu usługi rejestrowanego doręczenia elektronicznego[10]. W obszarze informatyzacji pojawiły się jednak nieznane dotychczas problemy, mianowicie cyberzagrożenia, które stanowią przeszkodę dla ciągłego świadczenia usług publicznych (załatwiania spraw urzędowych przez internet) oraz mogą negatywnie wpłynąć na sposób przetwarzania danych osobowych i informacji publicznych, ograniczyć przepustowość sieci czy prawidłowe funkcjonowanie infrastruktury teleinformatycznej. Przedstawione problemy nierzadko mają charakter transgraniczny. W odniesieniu do badanego przypadku rację należy przyznać Grażynie Szpor, która stwierdza, że „ekspansja Internetu zmniejsza rolę prawa krajowego w regulowaniu stosunków informacyjnych. Istotne staje się oddziaływanie na legislację unijną i prawo międzynarodowe oraz sposób transpozycji tych aktów do prawa krajowego"[11]. Tak też było w przypadku wprowadzenia do polskiego porządku prawnego ustawy o krajowym systemie cyberbezpieczeństwa (dalej: u.k.s.c.)[12]. We wskazanej ustawie w katalogu usług kluczowych próżno jednak szukać usług administracji publicznej. To zmieni się zasadniczo ze względu na regulacje zaproponowane na mocy dyrektywy NIS 2[13]. Nie oznacza to jednak, że aktualnie administracja nie ma swoich własnych polityk cyberbezpieczeństwa.

2. Dyrektywa NIS 2 szansą na osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa administracji publicznej

E-administracja stanowi potencjalne źródło cyberataków[14]. Ochrona przed różnego typu cyberzagrożeniami jest obowiązkiem organów administracji publicznej.

[9] Zob. art. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j. Dz.U. z 2024 r. poz. 1557.

[10] Zob. art. 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, t.j. Dz.U. z 2024 r. poz. 1725.

[11] G. Szpor, *Problemy administracyjnoprawne związane z ekspansją Internetu*, [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W.R. Wiewiórowski, Warszawa 2012, s. 79.

[12] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz.U. z 2024 r. poz. 1077 ze zm.

[13] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego 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 L Nr 333, s. 80.

[14] Cyberatakiem określa się atak dokonany za pomocą środków cyfrowych poprzez cyberprzestrzeń; celem cyberataku jest najczęściej uszkodzenie, zablokowanie dostępu, zniszczenie lub złośliwe przejęcie środowiska obliczeniowego albo naruszenie integralności danych lub przechwycenie informacji. Zob. P. Wiszniewski, *Cyberatak*, [w:] *Wielka Encyklopedia Prawa. Prawo Informatyczne*, red. B. Hołyst, R. Hauser, G. Szpor, L. Grochowski, t. 22, Warszawa 2021, s. 88.

Zakres bezpieczeństwa e-administracji obejmuje kilka komponentów, do których należą cyberbezpieczeństwo informacji i danych osobowych, infrastruktury krytycznej państwa, sieci i systemów teleinformatycznych oraz stabilność świadczenia e-usług[15]. Analiza aktów prawnych dotyczących funkcjonowania elektronicznej administracji prowadzi do wniosku, że ustawodawca bardziej skupił się na komponentach techniczno-organizacyjnych niż tych związanych z zapewnieniem cyberbezpieczeństwa. Być może wynika to z faktu, że na mocy dyrektywy NIS[16] nie wskazano w wykazie operatorów usług kluczowych podmiotów administracji publicznej. Ustawa o krajowym systemie cyberbezpieczeństwa, która stanowi implementację dyrektywy NIS, może znaleźć zastosowanie co do działań podejmowanych przez administrację publiczną w kontekście przygotowania i wdrożenia zasad polityki cyberbezpieczeństwa.

W odpowiedzi na pytanie, jakie kwestie powinna uwzględniać polityka cyberbezpieczeństwa w administracji publicznej, należy odwołać się do u.k.s.c. Kluczowe znaczenie ma definicja cyberbezpieczeństwa zawarta w art. 2 pkt 4 u.k.s.c., w świetle której przez cyberbezpieczeństwo należy rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Innymi słowy, ustawodawca wyraża przekonanie, że skuteczna polityka cyberbezpieczeństwa zapewnia ochronę danych, stabilność świadczenia e-usług oraz bezpieczeństwo teleinformatyczne (infrastrukturalne, systemowe). Co ciekawe, w u.k.s.c. dokonano klasyfikacji incydentów[17], w ramach której wymienione zostały tzw. incydenty w podmiocie publicznym[18]. W wyniku analizy przepisów jednoznacznie można stwierdzić, że pomimo tego, iż podmioty administracji publicznej[19] nie znalazły się w wykazie operatorów usług kluczowych, to przepisy dotyczące zgłaszania czy obsługi incydentów mogą znaleźć zastosowanie również

[15] D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu. Sprawy Karne" 2023, nr 53, s. 103.

[16] Dyrektywa 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.Urz. UE L Nr 194, str. 1. Zob. motyw 45 dyrektywy NIS: niniejsza dyrektywa ma zastosowanie wyłącznie do tych administracji publicznych, które zostały zidentyfikowane jako operatorzy usług kluczowych. Państwa członkowskie pozostają jednak odpowiedzialne za zapewnienie bezpieczeństwa sieci i systemów informatycznych administracji publicznych niewchodzących w zakres stosowania niniejszej dyrektywy.

[17] Art. 2 pkt 5 u.k.s.c. stanowi, że incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

[18] Art. 2 pkt 9 u.k.s.c. stanowi, że incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7-15 u.k.s.c.

[19] Nadmienić należy, że krajowy system cyberbezpieczeństwa obejmuje podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz organy właściwe do spraw cyberbezpieczeństwa (zob. art. 4 pkt 16 i 17 u.k.s.c.).

w administracji publicznej. Powyższe wymaga jednak dookreślenia elementów polityki cyberbezpieczeństwa, dostosowania jej do zakresu działań podejmowanych przez określony organ. Wydaje się, że owa polityka powinna regulować następujące kwestie: sposób klasyfikacji incydentów, działania prewencyjne i następcze związane z potencjalnym bądź faktycznym zagrożeniem świadczenia e-usług, zakres ochrony danych i informacji, wzrost kompetencji cyfrowych pracowników administracji publicznej. Polityka cyberbezpieczeństwa rozpatrywana przez pryzmat ww. czynników stanowi istotny komponent zarządzania kryzysowego. Należy odnotować, że w związku z coraz szerszym zastosowaniem rozwiązań sztucznej inteligencji (SI) w administracji publicznej zwiększa się ryzyko złośliwego wykorzystywania SI, pojawiają się także działania przestępcze[20]. Skala cyberzagrożeń jest ogromna, niemniej jednak polityka cyberbezpieczeństwa powinna być tak przygotowana, aby działania podejmowane przez e-administrację sprzyjały nie tylko modernizacji usług, ale również pozytywnie wpływały na zrównoważony rozwój i sprzyjały włączeniu społecznemu (dostępność cyfrowa). Osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa administracji publicznej to główny cel dyrektywy NIS 2.

Różnice w implementacji dyrektywy NIS w poszczególnych państwach członkowskich UE, wzrost incydentów (cyberzagrożeń), a także niedoskonałości prawne to przyczyny, z uwagi na które zdecydowano się wprowadzić dyrektywę NIS 2. W odróżnieniu od swojej poprzedniczki dyrektywa NIS 2 obejmuje swoim zakresem również podmioty administracji publicznej, które uznano za tzw. podmioty kluczowe[21]. Jednocześnie usługi administracji publicznej zostały określone jako te, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. W dodatku nie ma znaczenia, czy podmiot administracji publicznej świadczy usługi na poziomie centralnym czy regionalnym. Zarówno w jednym, jak i w drugim przypadku traktowany jest jako podmiot kluczowy[22]. W dyrektywie NIS 2 wymieniono warunki uznania za podmiot administracji publicznej, a zatem jest nim taki, który m.in.: został utworzony w celu zaspokajania potrzeb leżących w interesie ogólnym i nie ma charakteru przemysłowego ani handlowego, ma osobowość prawną lub zgodnie z przepisami jest uprawniony do działania w imieniu innego podmiotu mającego osobowość prawną, spełnia określone warunki

[20] J. Cytowski, *Przestępcze i złośliwe wykorzystywanie sztucznej inteligencji*, [w]. *Internet. Hacking*, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2023, s. 200-203.

[21] Zob. art. 3 ust.1 lit. d dyrektywy NIS 2.

[22] Zgodnie z art. 2 ust. 2 lit. f dyrektywy NIS 2, który stanowi, że 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.

finansowania i nadzoru, ma możliwość kierowania do osób fizycznych lub prawnych decyzji administracyjnych lub regulacyjnych, mających wpływ na ich prawa w transgranicznym przepływie osób, towarów, usług lub kapitału[23].

Właśnie z racji umieszczenia podmiotów administracji publicznej w wykazie usług kluczowych na znaczeniu zyskał pomysł utworzenia i wdrożenia skoordynowanych ram w zakresie polityki cyberbezpieczeństwa administracji publicznej. Powyższe ramy w przypadku administracji obejmują przede wszystkim obowiązki wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz procedury zgłaszania incydentów. W przypadku pierwszego z nich, art. 21 dyrektywy NIS 2 stanowi wprost, że podmioty administracji publicznej zostały zobowiązane do wprowadzenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych, niezbędnych do zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, za pomocą których świadczą usługi. Celem takiego działania jest zapobieganie bądź minimalizowanie wpływu incydentów na usługi i otoczenie. W tym celu dyrektywa NIS 2 wprowadza następujące elementy zarządzania ryzkiem, takie jak m.in.: polityka analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługa incydentu, zarządzanie kryzysowe, bezpieczeństwo łańcucha dostaw, podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa, bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami[24]. Niezwykle istotne w tym aspekcie obok zagadnień o charakterze prawnym i technologicznym są szkolenia i bezpieczeństwo zasobów ludzkich. Grażyna Szpor wskazuje wprost na istotę wsparcia rozwoju umiejętności i kompetencji cyfrowych, zwiększenia świadomości w zakresie ryzyka oraz edukacji cyfrowej[25].

Dyrektywa NIS 2 formułuje obowiązki w aspekcie zgłaszania incydentów mających istotny wpływ na świadczenie usług (poważny incydent) bez zbędnej zwłoki do właściwego CSIRT, organu oraz odbiorców usług. Bardzo ważne jest również powiadamianie o transgranicznym wpływie incydentu. Samo zgłoszenie nie nakłada jednak na podmiot zgłaszający zwiększonej odpowiedzialności[26]. Oprócz wskazanych powyżej obowiązków dyrektywa NIS 2 formułuje jeszcze inne, takie jak: przyjęcie krajowych strategii cyberbezpieczeństwa oraz wyznaczenie lub powołanie właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa, zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), zasady

[23] Zob. art. 6 pkt 35 dyrektywy NIS 2.
[24] Zob. art. 21 dyrektywy NIS 2.
[25] G. Szpor, *Modele podnoszenia kompetencji cyfrowych*, [w:] *Internet. Hacking…*, s. 326-329.
[26] Zob. art. 23 dyrektywy NIS 2.

i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie oraz w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

Konkluzje

Czy dyrektywa NIS 2 pozwoli na wprowadzenie jednolitych środków mających na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii? Na powyższe pytanie nie ma jednoznacznej odpowiedzi. Wiele zależy od tego, jakie środki zarządzania ryzykiem w cyberbezpieczeństwie zostaną uwzględnione w ramach polityki cyberbezpieczeństwa poszczególnych państw członkowskich UE. Nie można jednak zaprzeczyć, że obecnie w obliczu wzrastającej liczby cyberzagrożeń (również w sektorze publicznym) determinantę skutecznego, efektywnego, a przede wszystkim bezpiecznego świadczenia e-usług stanowi cyberbezpieczeństwo. Pozytywnie należy ocenić działania UE w obszarze osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego – wprowadzenie dyrektywy NIS 2, która kładzie akcent na stworzenie jednolitych standardów cyberbezpieczeństwa. Słusznie zresztą na mocy dyrektywy NIS 2 podmioty administracji publicznej uznano za tzw. podmioty kluczowe i przypisano im obowiązki w zakresie stworzenia skoordynowanych ram w zakresie cyberbezpieczeństwa.

W ślad za dyrektywą NIS 2 polityka cyberbezpieczeństwa administracji publicznej stanowi istotny komponent zarządzania kryzysowego. Cyberbezpieczeństwo administracji publicznej dotyczy ochrony danych i informacji, systemów, sieci oraz infrastruktury teleinformatycznej. Dyrektywa NIS 2 wskazuje wprost najważniejsze obowiązki podmiotów kluczowych (w tym również podmiotów administracji publicznej) w ramach zapewnienia cyberbezpieczeństwa, takie jak wdrożenie środków zarządzania ryzykiem w cyberbezpieczeństwie oraz procedur zgłaszania incydentów. Polityka cyberbezpieczeństwa administracji publicznej oprócz zapewnienia bezpieczeństwa łańcucha dostaw, prowadzenia analizy ryzyka i bezpieczeństwa systemów, zgłaszania incydentów mających istotny wpływ na świadczenie usług (poważny incydent) powinna uwzględniać cyberhigienę, promować szkolenia w zakresie cyberbezpieczeństwa, wspierać rozwój umiejętności i kompetencji cyfrowych. Na polskim ustawodawcy ciąży istotny obowiązek dotyczący implementowania dyrektywy NIS 2 w sposób odpowiadający aktualnej, suwerennej polityce państwa w zakresie cyberbezpieczeństwa. Polski rząd przedmiotowe zagadnienie traktuje jako jeden z priorytetów rozwoju społeczno-gospodarczego, co także należy ocenić pozytywnie w kontekście wzmacniania bezpieczeństwa cyfrowego kraju. Biorąc pod uwagę powyższe, nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa jest nieunikniona.

Literatura

Błażewski M., *Zasada powszechności elektronicznej administracji*, „Folia Iuridica Universitatis Wratislaviensis" 2018, vol. 7(1).
Cytowski J., *Przestępcze i złośliwe wykorzystywanie sztucznej inteligencji*, [w:] *Internet. Hacking*, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2023.
Ejdys J., *Zaufanie do technologii w e-administracji*, Białystok 2018.
Lubiewski P., *Szczególna dynamika zmian współczesnych zagrożeń w sferze bezpieczeństwa publicznego na przykładzie cyberprzestrzeni*, „Zeszyty Naukowe SGSP" 2020, nr 76/4.
Monarcha-Matlak A., *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, „Lingwistyka Stosowana" 2017, issue 24.
Romaniuk P., *Tradycje i przyszłość administracji publicznej w zakresie rozwoju e-usług*, „Journal of Modern Science" 2020, t. 1/44.
Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu. Sprawy Karne" 2023, nr 53.
Skoczylas D., *Dostępność cyfrowa determinantą zmian w funkcjonowaniu administracji publicznej?*, „Studia Administracji i Bezpieczeństwa" 2022, nr 13, t. 13.
Szpor G., *Modele podnoszenia kompetencji cyfrowych*, [w:] *Internet. Hacking*, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2023.
Szpor G., *Problemy administracyjnoprawne związane z ekspansją Internetu*, [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W.R. Wiewiórowski, Warszawa 2012.
Wiszniewski P., *Cyberatak*, [w:] *Wielka Encyklopedia Prawa. Prawo Informatyczne*, red. B. Hołyst, R. Hauser, G. Szpor, L. Grochowski, t. 22, Warszawa 2021.

Akty prawne

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j. Dz.U. z 2024 r. poz. 1557.
Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, t.j. Dz.U. z 2024 r. poz. 1725.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz.U. z 2024 r. poz. 1077 ze zm.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 (tekst mający znaczenie dla EWG), Dz.Urz. UE L Nr 166, s.1.
Dyrektywa 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.Urz. UE L Nr 194, s. 1.
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego 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 L Nr 333, s. 80.