

Dominika Skoczyła

AKSJOLOGICZNY WYMIAR E-ADMINISTRACJI I CYBERBEZPIECZEŃSTWA W KONTEKŚCIE POTRZEB JEDNOSTKI I WSPÓLNOTY

1. Wprowadzenie

Współcześnie determinanty rozwoju państwa są związane z efektywnym i skutecznym wykorzystaniem nowoczesnych technologii informacyjno-komunikacyjnych (ICT) w sferze publicznej. Szczególną rolę w tym zakresie odgrywa administracja publiczna, a ściślej prawo administracyjne. W tym miejscu, w ślad za I. Niżnik-Dobosz, należy potwierdzić, że to właśnie „rozwój cywilizacyjny stał się determinantą powstania prawa administracyjnego, a także kształtowania się ustroju, celów i zadań publicznych”¹.

W nurcie tych rozważań na uwagę zasługują czynniki, które mają obecnie największy wpływ na aksjologiczny wymiar prawa administracyjnego. Istotne znaczenie mają potrzeby społeczeństwa informacyjnego, dla

¹ I. Niżnik-Dobosz, *Prawo administracyjne jako czynnik gwarantujący rozwój cywilizacyjny* [w:] *Fenomen prawa administracyjnego. Księga jubileuszowa Profesora Jana Zimmermanna*, red. W. Jakimowicz, M. Krawczyk, I. Niżnik-Dobosz, Warszawa 2019, s. 655.

którego szczególną wartość stanowi stały dostęp do informacji (wiedzy). Systemy informacyjne, w tym globalne sieci informatyczne są traktowane jako podstawowe źródło wymiany informacji i komunikacji zarówno międzyludzkiej, jak i na poziomie instytucjonalnym². Potrzeby społeczeństwa informacyjnego przyczyniły się do zmian w zakresie funkcjonowania administracji (wprowadzono model elektronicznej administracji) oraz ustalenia standardów bezpieczeństwa e-usług i użytkowników sieci (cyberbezpieczeństwo). Nowe wzorce i zasady działania pozostają w zgodzie z zasadami dobrej administracji, powszechnie akceptowanymi przez społeczeństwo. W tym właśnie przejawia się służebny charakter działania administracji. Elektroniczna administracja umożliwia bowiem zdecydowanie szybsze i łatwiejsze załatwianie spraw administracyjnych, a co za tym idzie zaspokajanie zbiorowych i indywidualnych potrzeb obywateli³. Obok licznych korzyści e-administracji, należy także wskazać problemy wynikające z korzystania z cyberprzestrzeni. Współcześnie wartości aksjologiczne prawa administracyjnego związane są z e-administracją oraz cyberbezpieczeństwem. Co więcej, całemu społeczeństwu i poszczególnym obywatelom należy zapewnić zarówno najwyższej jakości usługi, jak i określić jednolite standardy bezpieczeństwa sieciowego, czemu służyć ma korespondujące z wartościami cyfrowymi prawo administracyjne.

W dalszych rozważaniach warto się zatem przyjrzeć temu, jak współcześnie kształtują się wartości prawa administracyjnego w odniesieniu do aksjologicznego wymiaru e-administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty. W pierwszej części pracy zostaną przedstawione zagadnienia odnoszące się do e-administracji oraz cyberbezpieczeństwa. Druga część stanowi uzasadnienie aksjologicznego wymiaru wyżej wymienionych, ze względu na aktualne potrzeby jednostki i wspólnoty.

² P. Sienkiewicz, *Ocena poziomu rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica” 2010/25, s. 58–59.

³ A. Monarcha-Matlak, *Wzorce i zasady obecnej i przyszłej administracji publicznej* [w:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. B. Jaworska-Dębska, P. Kledzik, J. Sługocki, Warszawa 2020, s. 908–914.

2. E-administracja i cyberbezpieczeństwo jako obiektywne standardy rozwoju społeczno-gospodarczego

Dążenia dotyczące poprawy organizacji administracji publicznej w ramach świadczenia usług o szczególnym znaczeniu społecznym mają ogromne znaczenie w kontekście realizacji potrzeb jednostki i wspólnoty. Przy czym skuteczność i prawidłowość działań administracji ocenia się przede wszystkim według konstytucyjnej zasady legalizmu⁴. Administracja świadcząca, użyteczna społecznie, odgrywa niezwykle ważną rolę w zakresie zaspokajania potrzeb ogółu. Ponadto jest „głównym organizatorem usług publicznych, zobowiązanym do tworzenia odpowiedniej bazy materialnej i świadczenia tych usług”⁵.

W XXI w. interaktywność relacji pomiędzy administracją a obywatelami wymaga uwzględnienia narzędzi informatycznych w procesach organizacyjnych, decyzyjnych, społeczno-kulturowych i gospodarczych. Warto jednocześnie zwrócić uwagę na to, że w odniesieniu do zwiększenia wpływu ICT na zarządzanie publiczne na pierwszy plan wysuwa się, wspomniana już w rozdziale, służebna rola administracji wobec jednostki i wspólnoty. Obecnie zaspokajanie indywidualnych i zbiorowych potrzeb obywateli nie jest bowiem możliwe bez rozwoju elektronicznej administracji. E-administracja zapewnia nie tylko wyższą jakość usług publicznych, zwiększając przy tym efektywność wykonywania zadań publicznych, lecz także zwiększa partycypację publiczną obywateli w sferze publicznej⁶.

Jak można zauważyć, zagadnienia związane z informatyzacją, cyfryzacją, sztuczną inteligencją (SI) oraz cyberbezpieczeństwem wpływają na czynności i przedsięwzięcia podejmowane przez administrację

⁴ Art. 7 Konstytucji RP stanowi, że organy władzy publicznej działają na podstawie i w granicach prawa.

⁵ M. Stahl, *Pojęcie administracji, jej cechy i funkcje* [w:] *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. M. Stahl, Warszawa 2013, s. 24.

⁶ K. Jastrzębska, *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, Warszawa 2018, s. 47–48.

publiczną. Ich celem jest realizacja interesu publicznego. Niemniej jednak źródeł powszechnie przyjmowanych regulacji należy szukać w aksjologii, tj. wartościach, które są cenne i pożądane w społeczeństwie. Obecnie za takie uchodzą wartości cyfrowe. Warto zastanowić się nad tym, dlaczego to właśnie technologie informacyjno-komunikacyjne (ICT) i potrzeby społeczeństwa informacyjnego stały się kryteriami oceny efektywności prawa administracyjnego. Ponadto warto wskazać korzyści e-administracji oraz ustosunkować się do kwestii cyberbezpieczeństwa. Odpowiadając na pierwsze z zadanych pytań, potrzeby społeczeństwa informacyjnego wpłynęły na rozszerzenie katalogu zadań administracji w ramach informatyzacji. To oczekiwania społeczeństwa informacyjnego zwiększyły popyt na dostęp i przetwarzanie informacji oraz usług. Usługi społeczeństwa informacyjnego zmodernizowały rolę administracji publicznej, określając ją za pomocą charakterystycznej funkcji – świadczącej e-usługi, a jednocześnie regulującej, porządkującej i gwarantującej prawne reguły funkcjonowania w cyberprzestrzeni. Współcześnie ogromne wyzwanie dla społeczeństwa informacyjnego stanowi „zachowanie dostępności i integralności sieci i infrastruktury informacyjnej oraz zachowanie poufności zawartych w nich informacji”⁷. Reasumując, obok zalet związanych z funkcjonowaniem elektronicznej administracji, kluczowy wymiar prawny i aksjologiczny posiadają kwestie cyberbezpieczeństwa.

Wdrożenie nowych, innowacyjnych technologii stanowi impuls rozwoju państwa i społeczeństwa. Efektywność prawa administracyjnego współcześnie oceniana jest zatem pod kątem możliwości zastosowania narzędzi i systemów informatycznych w sferze publicznej. Korzyści w obszarze wykorzystania nowych technologii obejmują m.in. świadczenie wysokiej jakości usług o spersonalizowanym charakterze oraz automatyzm e-usług, liczne ułatwienia w przekazywaniu informacji czy redukcję kosztów funkcjonowania administracji. Ponadto różnorodność narzędzi i kanałów informacyjnych sprawia, że działalność e-administracji i oferowane przez nią e-usługi są istotnym elementem

⁷ G. Szpor, *Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa* [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 3.

cyfryzacji życia publicznego, w szczególności sektora gospodarczego oraz pozwalają na zaspokojenie potrzeb społeczeństwa informacyjnego⁸. Współcześnie administracja publiczna posiada swoisty elektroniczny wymiar (sposób) rozstrzygania spraw administracyjnych. Komunikacja obywatela z organem administracji publicznej w formie on-line jest ważnym aspektem w kontekście czynników determinujących aksjologię prawa administracyjnego. Wyzwanie dla administracji stanowi stworzenie warunków koniecznych dla rozwoju gospodarczego w przestrzeni wirtualnej. Rację ma A. Haręża, w ocenie którego „elektroniczna administracja publiczna ma na celu stworzenie cyfrowego pomostu między władzą a obywatelami”⁹. Świadomość istniejących potrzeb informacyjnych i informatycznych nakłada na organy administracji publicznej obowiązek podjęcia działań zmierzających do realizacji zadań publicznych w kompleksowy i skuteczny sposób. Z tych względów aksjologiczny wymiar wartości cyfrowych odnosi się także do cyberbezpieczeństwa.

Bezpieczeństwo publiczne zajmuje szczególne miejsce w hierarchii podstawowych wartości, zarówno z perspektywy funkcjonowania administracji publicznej, jak i samych obywateli. Jest ważnym składnikiem ładu publicznego¹⁰. Dziś problem zagrożeń bezpieczeństwa publicznego należy również rozpatrywać pod kątem cyberbezpieczeństwa. Wartości aksjologiczne w tym przypadku przyjmują szczególną postać. Cyberbezpieczeństwo oznacza bowiem odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy¹¹, dotyczy ochrony nie tylko sieci i systemów, lecz także użytkowników przed różnego typu cyberzagrożeniami¹². Cyberbezpie-

⁸ P. Romaniuk, *Tradycje i przyszłość administracji publicznej w zakresie rozwoju e-usług*, „Journal of Modern Science” 2020/1(44), s. 270–271.

⁹ A. Haręża, *The Role of Administrative Law in Times of Technological* [w:] *Legal Innovation in Polish Law*, red. J. Gołaczyński, W. Kilian, T. Scheffler, Warszawa 2019, s. 111.

¹⁰ M. Zdyb, *Aksjologiczne podstawy bezpieczeństwa wewnętrznego w Rzeczypospolitej Polskiej* [w:] *Publicznoprawne podstawy bezpieczeństwa wewnętrznego*, red. M. Zdyb, Warszawa 2014, s. 27–30.

¹¹ Art. 2 pkt 4 u.k.s.c.

¹² Art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz

czeństwo stanowi wartość nadrzędną, jest pożądanym elementem bezpieczeństwa powszechnego i indywidualnego, podmiotowym prawem człowieka i obywatela. Wymaga wyeksponowania stwierdzenie, że aksjologia prawa administracyjnego w XXI w. związana jest z wartościami cyfrowymi. Warto jednak zastanowić się nad tym, jakie wartości i jakie antywartości niesie ze sobą korzystanie z cyberprzestrzeni.

3. Aksjologiczny wymiar cyberbezpieczeństwa i e-administracji w kontekście potrzeb jednostki i wspólnoty. Wartości a antywartości świata cyfrowego

Cyberprzestrzeń jest miejscem wymiany informacji i komunikacji międzyludzkiej. Pod znakiem zapytania staje natomiast kwestia, na ile jest to miejsce niezawodne i bezpieczne. Niemniej jednak, w ramach analizy mierników rozwoju społeczno-gospodarczego, współcześnie wymienia się przede wszystkim cyfryzację i usieciowienie społeczeństwa (potrzeby społeczeństwa informacyjnego), innowacyjność i postęp technologiczny, a także dostępność administracji publicznej (e-administracji). Idąc dalej, kryteria przyjaznego świata cyfrowego wymagają od e-administracji ustanowienia mechanizmów i procedur o elastycznym i otwartym charakterze. Jednocześnie w wymiarze aksjologicznym, obok wprowadzenia transparentnych i skutecznych regulacji prawnych, znaczenie ma również praktyczna realizacja zadań publicznych i świadczenie e-usług. Zaspokajanie zbiorowych i indywidualnych potrzeb w tym zakresie wymaga interoperacyjności i innowacyjności e-usług w wymiarze technologicznym (sprzęt, oprogramowanie, system), ale również zmian organizacyjnych (zarówno samych struktur, jak i pracy urzędników)¹³.

certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15).

¹³ D. Fleszer, *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa” 2014/14/1, s. 126–127.

To właśnie aksjologia w obszarze nowych technologii ma ogromny wpływ na kształt obowiązujących regulacji prawnych.

Cyberprzestrzeń kształtuje świat nowych wartości. Z jednej strony ułatwia dostęp do informacji i usług, z drugiej jest miejscem nieprzewidywalnych zagrożeń, zarówno dla samego użytkownika, jak i infrastruktury informatycznej¹⁴. Nie można pominąć jednak faktu, że na przestrzeni lat wartości cyfrowe uległy przeobrażeniu. Obecnie słusznie podkreśla się już nie tylko wzajemną e-interakcję, lecz także rolę sztucznej inteligencji w działaniach administracji publicznej. Aksjologiczny wymiar SI uwidacznia się tutaj przede wszystkim w udostępnianiu i wykorzystaniu danych w sektorach publicznych, np. transporcie, medycynie czy przemyśle. Dodatkowo SI może być również pomocna w celu określenia reguł cyberbezpieczeństwa sieci i systemów informatycznych oraz przetwarzania danych¹⁵. Można zauważyć, że SI jest rozwiązaniem coraz chętniej wykorzystywanym w różnych dziedzinach życia, zarówno sfery prawa publicznego, jak i prywatnego. Algorytmy stanowią nieodzowne wsparcie realizowanych zadań, przy czym powodują też obawę co do całkowitego zastąpienia człowieka robotem (maszyną)¹⁶.

Aksjologiczny wymiar nowych technologii w kontekście potrzeb jednostki i wspólnoty odpowiada aktualnym potrzebom cywilizacyjnym, do których należy zaliczyć: informatyzację w zakresie zarządzania sprawami publicznymi, zrównoważony rozwój w ramach wykorzystywania ICT, cyberbezpieczeństwo danych osobowych, e-usług, sieci i systemów informatycznych. Odzwierciedleniem tych założeń jest rozwój społeczeństwa informacyjnego, przy czym rozwój ten ma być zrównoważony. Takim można nazwać ten, który uwzględni różnorodność i równowagę czynników ekonomicznych, technologicznych społeczno-kulturowych i politycznych oraz zrównoważony rozwój infrastruktury, kompetencji, jak również samego użytkownika ICT. Nie należy także zapominać

¹⁴ R.A. Podgórski, *Aksjologiczny wymiar Internetu (na podstawie badań ankietowych)*, „Media i Społeczeństwo” 2015/5, s. 22–23.

¹⁵ Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019–2027, <https://www.gov.pl/attachment/0aa51cd5-b934-4bcb-8660-bfecb20ea2a9> (dostęp: 1.09.2022 r.).

¹⁶ I. Oleksiuk, *Założenia aksjologiczne autorskoprawnej ochrony twórczości w świetle rozwoju sztucznej inteligencji*, „Acta Iuris Stetinensis” 2017/18, s. 249–250.

o tym, że aksjologia w zakresie nowych technologii determinuje zmiany prawne. Może zatem mieć wpływ na rozwój społeczno-gospodarczy, a w perspektywie długoterminowej na dobrobyt obecnych i przyszłych pokoleń¹⁷.

Przedstawiając uwagi w przedmiocie nowych technologii, warto podkreślić, że wartości cyfrowe mają charakter niematerialny. M. Błażewski zwraca szczególną uwagę na bezpieczeństwo e-administracji, zasady zarządzania i użytkowania systemów oraz środków komunikacji elektronicznej. W ślad za nim można stwierdzić, że aksjologiczny wymiar e-administracji warunkuje wprowadzenie zróżnicowanych regulacji prawnych, pozwalających na „zachowanie wysokiej jakości wymagań i warunków technicznych oraz organizacyjnych gwarantujących w sposób optymalny bezpieczeństwo w e-administracji”¹⁸.

W świecie eksponowanych wartości cyfrowych występują także antywartości. Zagrożone jest zarówno cyberbezpieczeństwo osób prywatnych i grup interesów (tu szczególnie znaczenie mają: ochrona danych osobowych i tajemnicy przedsiębiorstwa, bezpieczeństwo środków finansowych, transakcji biznesowych, zapewnienie ciągłości świadczenia usług), jak i państwa (ochrona infrastruktury krytycznej, usług kluczowych i usług cyfrowych, walka z cyberprzestępczością i cyberterroryzmem)¹⁹. Szczególnie niebezpieczne są incydenty, czyli zdarzenia, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo (art. 2 pkt 5 u.k.s.c.)²⁰. Mogą one zakłócić m.in. ciągłość świadczenia usługi kluczowej i usługi cyfrowej, skutkować znaczną szkodą dla bezpieczeństwa

¹⁷ E. Ziembka, *Ku zrównoważonemu społeczeństwu informacyjnemu*, „Roczniki Kolegium Analiz Ekonomicznych” 2013/29, s. 418.

¹⁸ M. Błażewski, *Zasada zapewnienia bezpieczeństwa w e-administracji*, „Folia Iuridica Universitatis Wratislaviensis” 2017/1(6), s. 115.

¹⁹ T. Hoffmann, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018, s. 19–20.

²⁰ Ustawa o krajowym systemie cyberbezpieczeństwa w art. 2 wymienia różne rodzaje incydentów: incydent krytyczny (art. 2 pkt 6), incydent poważny (art. 2 pkt 7), incydent istotny (art. 2 pkt 8) czy incydent w podmiocie publicznym (art. 2 pkt 9). Wskazuje również warunki tzw. obsługi incydentu, do których należą czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu (art. 2 pkt 10).

lub porządku publicznego, interesów gospodarczych czy praw i wolności obywatelskich. Ponadto zagrożenie stanowią ataki cyberprzestępców czy, w skrajnych przypadkach, cyberterrorystów. Dochodzi m.in. do kradzieży tożsamości i danych osobowych, ujawniania informacji niejawnych, nielegalnych transakcji płatniczych, nadużyć związanych z łamaniem zabezpieczeń systemów komputerowych, sabotażu i szpiegostwa komputerowego, nękania, hackingu, cyberataków na infrastrukturę krytyczną czy usługi kluczowe²¹.

Jednym z podstawowych kryteriów działań podejmowanych w cyberprzestrzeni jest polityka cyberbezpieczeństwa. Organy administracji publicznej świadome istniejących zagrożeń bezpieczeństwa indywidualnego i zbiorowego w cyberprzestrzeni mają obowiązek podejmować działania prewencyjne bądź następcze, aby uchronić bądź zminimalizować negatywne skutki cyberzagrożeń. Wyzwanie stanowi zarówno określenie zasad i polityki cyberbezpieczeństwa, jak i organizacja struktur oraz pozyskanie specjalistycznych kadr eksperckich zdolnych do natychmiastowej obsługi incydentów²². Wielopoziomowa regulacja cyberbezpieczeństwa, w tym brak jednolitości w zakresie definicji i niewyodrębnienie cyberbezpieczeństwa w klasyfikacjach działalności, powoduje nie tylko trudności interpretacyjne, lecz przede wszystkim także te związane z ustaleniem spójnych kryteriów polityki cyberbezpieczeństwa. G. Szpor słusznie zaznacza, że warunkiem koniecznym optymalnych działań w ramach cyberbezpieczeństwa jest jednoznaczne i spójne określenie terminu „cyberbezpieczeństwo” oraz wyodrębnienie w Polskiej Klasyfikacji Działalności Gospodarczej – cyberbezpieczeństwa (szansa dla rozwoju usług związanych z sektorem cybernetycznym)²³. Wartości aksjologiczne w odniesieniu do e-administracji oraz cyberbezpieczeństwa łączy polityka bezpieczeństwa cybernetycznego. Mając na uwadze regulacje powszechnie obowiązującego prawa (m.in. ustawę

²¹ M. Sitek, *The legal framework for the security of the individual in cyberspace*, „Journal of Modern Science” 2018/2(37), s. 181–183.

²² T. Zdzikot, *Państwo i administracja publiczna na straży cyberbezpieczeństwa* [w:] *Stulecie polskiej administracji. Doświadczenia i perspektywy*, red. W. Federczyk, Warszawa 2018, s. 254–255.

²³ G. Szpor, *Nowelizacja siatki pojęciowej cyberbezpieczeństwa*, MoP 2020/22, s. 1189–1193.

o krajowym systemie cyberbezpieczeństwa i Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024), należy podkreślić, że bezpieczeństwo świadczenia e-usług zależy od wprowadzenia szczególnych środków bezpieczeństwa. Owe środki mają na celu zwiększyć odporność sektora publicznego i prywatnego na cyberzagrożenia oraz utrzymać dostęp do zasobów informacyjnych i ciągłość świadczenia usług. Kluczowe znaczenie mają także inwestycje w obszarze nowych technologii i aspekty transformacji cyfrowej oraz budowa otwartej i bezpiecznej cyberprzestrzeni w skali globalnej. Stosunki społeczne i gospodarcze implikują standardy efektywnej i skutecznej e-administracji oraz bezpieczeństwa sieciowego. Z punktu widzenia potrzeb jednostki i wspólnoty aspekty aksjologiczny i prawny uzupełniają się wzajemnie.

4. Konkluzje

Postęp technologiczny przyczynia się do zmian prawa administracyjnego także na płaszczyźnie aksjologicznej. Nie ulega wątpliwości, że współcześnie ze względu na wzmożoną aktywność organów władzy publicznej i człowieka w przestrzeni wirtualnej aksjologiczny wymiar prawa administracyjnego należy rozpatrywać przez pryzmat e-administracji i cyberbezpieczeństwa. Przy czym wartości cyfrowe muszą być kompatybilne z potrzebami jednostki i wspólnoty (społeczeństwa informacyjnego). Potrzeby społeczeństwa informacyjnego i potrzeby technologiczne oczywiście wpływają na jakość świadczonych e-usług i zadań e-administracji. Jednocześnie na podstawie oceny aktualnych warunków faktycznych i prawnych dochodzi do zmian legislacyjnych.

Aksjologia w kontekście cyfryzacji zarówno w aspekcie potrzeb jednostki, jak i wspólnoty wyraża się poprzez: szybkość przepływu informacji, nieprzerwany dostęp do baz danych, automatyzację, stałe świadczenie usług kluczowych i usług cyfrowych oraz bezpieczeństwo cybernetyczne. Należy jednak pamiętać, że obok wartości świata cyfrowego występują również antywartości – incydenty i cyberzagrożenia. W tym kontekście kluczowe znaczenie ma stworzenie standardów cyberbezpieczeństwa.

Konkludując, aksjologiczny wymiar e-administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty wynika przede wszystkim z indywidualizacji oraz specjalizacji e-usług oraz dynamicznego rozwoju ICT i postępu technologicznego. Obowiązkiem administracji publicznej jest ochrona wartości cyfrowych, co jest szczególnie trudnym zadaniem w związku z coraz większą aktywnością człowieka w sieci oraz intensyfikacją cyberzagrożeń.

Bibliografia

- Błażewski M., *Zasada zapewnienia bezpieczeństwa w e-administracji*, „Folia Iuridica Universitatis Wratislaviensis” 2017/1(6)
- Fleszer D., *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa” 2014/14/1
- Haręża A., *The Role of Administrative Law in Times of Technological* [w:] *Legal Innovation in Polish Law*, red. J. Gołaczyński, W. Kilian, T. Scheffler, Warszawa 2019
- Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018
- Jastrzębska K., *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, Warszawa 2018
- Monarcha-Matlak A., *Wzorce i zasady obecnej i przyszłej administracji publicznej* [w:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. B. Jaworska-Dębska, P. Kledzik, J. Sługocki, Warszawa 2020
- Niżnik-Dobosz I., *Prawo administracyjne jako czynnik gwarantujący rozwój cywilizacyjny* [w:] *Fenomen prawa administracyjnego. Księga jubileuszowa Profesora Jana Zimmermanna*, red. W. Jakimowicz, M. Krawczyk, I. Niżnik-Dobosz, Warszawa 2019
- Oleksiuk I., *Założenia aksjologiczne autorskoprawnej ochrony twórczości w świetle rozwoju sztucznej inteligencji*, „Acta Iuris Stetinensis” 2017/18
- Podgórski R.A., *Aksjologiczny wymiar Internetu (na podstawie badań ankietowych)*, „Media i Społeczeństwo” 2015/5
- Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019–2027, <https://www.gov.pl/attachment/0aa51cd5-b934-4bcb-8660-bfecb20ea2a9> (dostęp: 1.09.2022 r.).
- Romaniuk P., *Tradycje i przyszłość administracji publicznej w zakresie rozwoju e-usług*, „Journal of Modern Science” 2020/1(44)
- Sienkiewicz P., *Ocena poziomu rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica” 2010/25

- Sitek M., *The legal framework for the security of the individual in cyberspace*, „Journal of Modern Science” 2018/2(37)
- Stahl M., *Pojęcie administracji, jej cechy i funkcje* [w:] *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. M. Stahl, Warszawa 2013
- Szpor G., *Europejska regulacja bezpieczeństwa sieci i systemów informacyjnych a suwerenność państwa* [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017
- Szpor G., *Nowelizacja siatki pojęciowej cyberbezpieczeństwa*, MoP 2020/22
- Zdyb M., *Aksjologiczne podstawy bezpieczeństwa wewnętrznego w Rzeczypospolitej Polskiej* [w:] *Publicznoprawne podstawy bezpieczeństwa wewnętrznego*, red. M. Zdyb, Warszawa 2014
- Zdzikot T., *Państwo i administracja publiczna na straży cyberbezpieczeństwa* [w:] *Stulecie polskiej administracji. Doświadczenia i perspektywy*, red. W. Federczyk, Warszawa 2018
- Ziemia E., *Ku zrównoważonemu społeczeństwu informacyjnemu*, „Roczniki Kolegium Analiz Ekonomicznych” 2013/29

Dominika Skoczylas [ORCID: 0000-0003-1231-8078] – doktor nauk prawnych, Uniwersytet Szczeciński, Wydział Prawa i Administracji.