ACTA IURIDICA RESOVIENSIA Nr 2(53)/2026

ISSN 2720-0574 eISSN 2720-5797 DOI: 10.15584/actaires.2026.2.8

Dominika Skoczylas

Uniwersytet Szczeciński
ORCID: 0000-0003-1231-8078

PRAWO DO CYBERBEZPIECZEŃSTWA W KONTEKŚCIE PRAWA DO DOBREJ ADMINISTRACJI (E-ADMINISTRACJI)

Modernizacja administracji publicznej – determinanty funkcjonowania e-administracji

Transformacja cyfrowa ukształtowała nowy sposób (model) administrowania sprawami publicznymi znany pod pojęciem *e-administracja*. Informatyzacja administracji publicznej stała się warunkiem *sine qua non* załatwiania spraw publicznych. Można się pokusić o stwierdzenie, że nowoczesne technologie informacyjno-komunikacyjne ukształtowały trend e-administracji na miarę XXI w. Elektroniczny sposób zarządzania jest ściśle związany z innowacyjnością usług w sektorze publicznym. W odniesieniu do innowacji w administracji publicznej należy się zgodzić z A. Puczko, która wskazuje, że oprócz zmian technologicznych konieczne są również te o charakterze organizacyjnym „w samej administracji, tj. w sferze ustrojowej oraz w sferze jej działań wewnętrznych, jak i na zewnątrz”[1]. Niewątpliwie innowacyjność wymaga synergii wielu komponentów, co w szerszej perspektywie zapewnia dostępność, transparentność i wysoką jakość świadczonych e-usług. Nie można jednak zapomnieć o tym, że filary e-administrowania, podobnie jak w przypadku administracji w ujęciu klasycznym, stanowią zasady obiektywizmu, proporcjonalności i praworządności.

W nawiązaniu do powyższego należałoby zadać pytanie, czy informatyzacja administracji osiągnęła już taki poziom rozwoju, który satysfakcjonuje zarówno jej wewnętrzne struktury (urzędy), jak i podmioty korzystające z usług e-administracji (petentów). Wydaje się, że odpowiedź na to pytanie nie jest jednoznaczna z uwagi

[1] A. Puczko, *Model otwartej innowacji w administracji publicznej* [w:] *Prawo administracyjne jako miejsce spotkań. Księga jubileuszowa dedykowana Profesorowi Jerzemu Supernatowi*, red. B. Kowalczyk, K. Kulińska-Jachowska, Ł. Prus, M. Tabernacka, I. Sierpowska, E. Skorczyńska, Wrocław 2024, s. 607.

na to, że ocena funkcjonowania e-administracji opiera się na subiektywnym odczuciu podmiotu co do jej efektywnego (bądź nieefektywnego) i skutecznego (bądź nieskutecznego) działania. Za kluczowe należy uznać to, że rozwój usług elektronicznych zakłada nie tylko usprawnienie realizacji usług publicznych dla obywateli (głównie w ramach tzw. administracji świadczącej, ale też pozwala czy służy „optymalizacji różnego rodzaju procesów zachodzących wewnątrz aparatu administracyjnego”[2]. Modernizacja administracji publicznej uwarunkowana jest nie tylko zmianami technologicznymi, ale również natury prawnej, organizacyjnej, społeczno-gospodarczej czy wreszcie finansowej. Skądinąd interesujący pogląd wyraża K. Wasilewski, który działalność administracji publicznej utożsamia ze „stabilnością operacyjną” (ciągłość świadczenia usług publicznych) oraz „elastycznością adaptacyjną” (dostosowanie technologiczne)[3]. Oczywiście informatyzacja administracji publicznej jest procesem długofalowym i wieloaspektowym, co jest szczególnie widoczne w kontekście wyzwań czy barier związanych z jej wdrożeniem.

Technologie informacyjno-komunikacyjne zapewniają nie tylko szybszą i tańszą obsługę spraw administracyjnych, ale również pozwalają na wdrożenie zasad e-partycypacji czy dostępności cyfrowej dla osób ze szczególnymi potrzebami. O ile pierwsze z nich stanowią podstawowe zalety elektronizacji usług publicznych, o tyle kwestia e-partycypacji i dostępności cyfrowej wynika z nowoczesnego modelu zarządzania, administracji efektywnej, włączającej, zapewniającej równy dostęp do usług, sprzyjającej integracji, promującej obywatelski wzorzec postępowania w zakresie współdecydowania o sprawach publicznych. Niewątpliwie e-partycypacja jest jednym z fundamentalnych wyznaczników e-demokracji, co znajduje swój wyraz przede wszystkim w aktywnym „zaangażowaniu obywateli w proces podejmowania i realizowania decyzji politycznych za pośrednictwem narzędzi elektronicznych”[4]. Nie dziwi zatem zauważalny wzrost korzystania z prawa dostępu do e-informacji publicznej (np. z Biuletynu Informacji Publicznej[5]) czy zainteresowanie ponownym wykorzystywaniem informacji sektora publicznego[6].

---

[2] S. Dudzik, *Podstawy prawne działania e-administracji a ochrona danych osobowych* [w:] *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej*, red. S. Dudzik, I. Kawka, R. Śliwa, Kraków 2022, s. 15.

[3] K. Wasilewski, *E-administracja w Polsce: determinanty rozwoju i bariery wdrożeniowe*, „Przegląd Prawno-Ekonomiczny” 2025, nr 2, s. 96.

[4] N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, *Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*, Poznań 2020, s. 24.

[5] Biuletyn Informacji Publicznej to urzędowy publikator teleinformatyczny, którego celem jest powszechne udostępnianie informacji publicznej w postaci ujednoliconego systemu stron w sieci teleinformatycznej. Zob. art. 8 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2022, poz. 902 ze zm.).

[6] Powszechnie dostępny system teleinformatyczny służący do udostępniania informacji sektora publicznego w celu ponownego wykorzystywania oraz danych prywatnych w celu wykorzystywania to portal danych. Zob. art. 2 pkt 13 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. 2023, poz. 1524).

Na znaczeniu zyskują również e-doręczenia, e-konsultacje i e-wnioski. Współcześnie rozważania na temat e-partycypacji obejmują też wymagania dostępności cyfrowej (m.in. stron internetowych i aplikacji mobilnych podmiotów publicznych) czy wymagania dotyczące treści, przeglądu i aktualizacji deklaracji dostępności stron internetowych i aplikacji mobilnych podmiotów publicznych oraz ich publikacji[7]. Dostępność cyfrowa stała się „swoistym medium służącym niwelowaniu społecznej izolacji"[8] jej beneficjentów, tj. osób ze szczególnymi potrzebami. Tak rozumiany z jednej strony rozwój inteligentny, z drugiej sprzyjający włączeniu społecznemu pozostaje w symbiozie z podstawowymi zasadami (wartościami) mającymi swe źródło w prawie do dobrej administracji.

Aspekty e-administrowania oparte na zasadach obiektywizmu, proporcjonalności i rzecz jasna praworządności pozwalają urzeczywistnić postulat prawa do dobrej administracji, choć w zmodernizowanej formie prawa do dobrej e-administracji. Z drugiej strony pogłębiona informatyzacja usług publicznych stanowi wyzwanie zarówno pod kątem prawnym, jak i technologicznym. Podstawowym problemem są cyberzagrożenia, które mogą wpłynąć negatywnie na funkcjonowanie infrastruktury krytycznej, świadczenie usług kluczowych i bezpieczeństwo użytkowników środowiska online. Tym samym refleksji wymaga problematyka informatyzacji usług publicznych w dobie cyberzagrożeń. Badając przedmiotowe zagadnienie, należy najpierw odwołać się do pierwotnych założeń prawa do dobrej administracji, następnie wskazać, jak powinno się traktować zagadnienie cyberbezpieczeństwa w kontekście tego prawa. Celem artykułu jest wskazanie, w jaki sposób rozwój nowych technologii oddziałuje na aktualną politykę administracji publicznej w kwestii zapewnienia cyberbezpieczeństwa. Z uwagi na to, że administracja publiczna na gruncie dyrektywy NIS2 została uznana za sektor świadczący usługi kluczowe, prawo do cyberbezpieczeństwa stanowi obecnie zasadniczą determinantę prawa do dobrej administracji (e-administracji), które podlega szczególnej ochronie prawnej. Przyjęte metody badawcze obejmują analizę podstawowych aktów prawnych (prawa unijnego i krajowego) oraz literatury przedmiotu.

Prawo do dobrej administracji

Z perspektywy obywatela najważniejszą cechą administracji publicznej jest dostępność usług i sprawna realizacja zadań publicznych. Administracja charakteryzuje się władztwem administracyjnym (imperium), które pozwala na rozstrzygnięcie

[7] Por. art. 1 ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2023, poz. 1440).

[8] A. Rogacka-Łukasik, *Wybrane środki służące zapewnieniu dostępności cyfrowej dla osób z niepełnosprawnościami* [w:] *Aksjologiczne i prawne aspekty niepełnosprawności*, red. A. Drabarz, Białystok 2020, s. 211.

sprawy w sposób jednostronny (władczy) przez organ. Obecnie na znaczeniu zyskuje służebna rola administracji, tzw. administracja świadcząca, której podstawowym celem jest zaspokajanie potrzeb (oczekiwań) obywateli[9], a która ukierunkowana jest na realizację zadań użyteczności publicznej w kluczowych sektorach, np. ochrony zdrowia, pomocy społecznej czy transportu publicznego. J. Korczak wskazuje wprost tzw. konstytucyjne podstawy funkcji usługodawczej administracji publicznej, do których oprócz naczelnej zasady praworządności[10] zalicza również m.in. zasady pomocniczości, godności człowieka, sprawiedliwości społecznej, współdziałania władz publicznych czy decentralizacji[11]. Nie ulega wątpliwości, że wyeksponowane powyżej zasady konstytucyjne stanowią kwintesencję dobrej administracji.

Dobra administracja to administracja umożliwiająca realizację dobra wspólnego, z którym immanentnie związane jest świadczenie usług w konkretnej sprawie, na rzecz danej społeczności czy człowieka. Można zatem powiedzieć, że osadzenie koncepcji prawa do dobrej administracji wyłącznie na prawie jest niepełne, gdyż nie odzwierciedla „społecznego wymiaru prawa"[12]. Takie spojrzenie na administrację publiczną pozwala na sformułowanie wniosku, że prawo do dobrej administracji, które opiera się na fundamentalnych zasadach prawa, takich jak m.in. praworządność, bezstronność czy szybkość postępowania, ma kluczowe znaczenie w kontekście swego rodzaju „dobrostanu petenta". Przedmiotowy dobrostan należy jednak rozumieć dwutorowo, bowiem z perspektywy urzędnika będzie oznaczał kompleksowe wyjaśnienie sprawy, zaś ze strony petenta – załatwienie jej w sposób dla niego jak najbardziej korzystny (oczekiwany). Warto też zwrócić uwagę na to, że prawo do dobrej administracji wzmacnia zaufanie obywateli zarówno do organów administracji publicznej, jak i stanowionego (i stosowanego) przez nich prawa[13]. Przekonanie do rzetelności, skuteczności, efektywności i wiarygodności działań administracji publicznej determinuje wzrost poczucia bezpieczeństwa, a to stanowi jeden z wyznaczników dobrej administracji[14]. Zasada zaufania uczestników postępowania do władzy

[9] J. Smarż, P. Świtał, *Przyjazna administracja elektroniczna* [w:] *Administracja publiczna wobec procesów zmian w XXI wieku. Księga jubileuszowa Profesora Jerzego Korczaka*, red. P. Lisowski, Wrocław 2024, s. 298–299.

[10] Art. 7 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483) stanowi, że organy władzy publicznej działają na podstawie i w granicach prawa.

[11] J. Korczak, *Funkcja usługodawcza administracji publicznej w świetle konstytucyjnych zasad ustrojowych*, „Przegląd Prawa Konstytucyjnego" 2023, nr 4(74), s. 114–117.

[12] S. Fundowicz, *Administracja publiczna w świetle nauczania św. Tomasza z Akwinu i jego odczytania przez personalizm*, „Studia Prawnoustrojowe" 2025, nr 68, s. 90.

[13] J. Węglińska, *Zasada ochrony zaufania obywateli do państwa i do stanowionego przez nie prawa jako dyrektywa poprawnej legislacji*, „Prawo w Działaniu. Sprawy cywilne" 2020, nr 42, s. 175–176.

[14] J. Smarż, *Zasada pogłębiania zaufania obywateli do administracji publicznej jako fundament postępowania administracyjnego*, „Prawo i Więź" 2025, nr 1(54), s. 508.

publicznej[15] jest jedną z podstawowych zasad ogólnych postępowania administracyjnego, której nieodzownie towarzyszą zasady: praworządności (art. 6 k.p.a.), prawdy obiektywnej (art. 7 k.p.a.), rozstrzygania wątpliwości interpretacyjnych (art. 7a k.p.a.), adekwatności, proporcjonalności (art. 7b k.p.a.), udzielania informacji (art. 9 k.p.a.), wysłuchania stron (art. 10 k.p.a.), wyjaśniania zasadności przesłanek (art. 11 k.p.a.), szybkości i prostoty postępowania (art. 12 k.p.a.), polubownego rozstrzygania kwestii spornych (art. 13 k.p.a.), pisemności (art. 14 k.p.a.), oceny działania urzędów (art. 14a k.p.a.), dwuinstancyjności (art. 15 k.p.a.), trwałości decyzji (art. 16 k.p.a.).

Należy zdecydowanie podkreślić, że częściami składowymi dobrej administracji są nie tylko zasady prawa, ale również skuteczność i efektywność działania przedstawicieli władzy, co przekłada się na odpowiedni styl zarządzania (administrowania). Ten z kolei determinowany jest potrzebami społeczno-gospodarczymi i postępem technologicznym. Skądinąd kluczowe wydaje się zachowanie równowagi pomiędzy wykonaniem prawa przez urzędników a realizacją interesu obywatela. Zgodzić należy się zatem z poglądem, że „działaniom administracji towarzyszy człowiek", a „dobra administracja to dobrze stosowane prawo przez dobrze przygotowanego do pracy urzędnika"[16]. Standardy dobrej administracji promuje i wyznacza Kodeks Dobrej Praktyki Administracyjnej[17]. Określono w nim zasady dobrego administrowania, które należy interpretować jako obowiązki administracji publicznej wobec obywateli. Można powiedzieć, że stanowi on transparentne wytyczne dla urzędników, co niewątpliwie wpływa na jakość świadczonych usług publicznych. Rozpatrując powyższe kwestie szerzej, warto wskazać, że zasady określone w Kodeksie mają wymiar *stricte* prawny, ale także aksjologiczny. Pierwszy z nich należy odczytywać przede wszystkim przez pryzmat takich zasad, jak m.in. zasada praworządności (art. 4 Kodeksu), niedyskryminowania (art. 5 Kodeksu), proporcjonalności (art. 6 Kodeksu), zakazu nadużywania uprawnień (art. 7 Kodeksu), bezstronności i niezależności (art. 8 Kodeksu), obiektywności (art. 9 Kodeksu), odpowiadania na pisma w języku obywatela (art. 13 Kodeksu), prawa wysłuchania i do złożenia oświadczeń (art. 16 Kodeksu), stosownego terminu podjęcia decyzji (art. 17 Kodeksu) i obowiązku uzasadniania

[15] Art. 8 § 1 ustawy dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. 2025, poz. 1691), dalej: k.p.a., stanowi, że organy administracji publicznej prowadzą postępowanie w sposób budzący zaufanie jego uczestników do władzy publicznej, kierując się zasadami proporcjonalności, bezstronności i równego traktowania.

[16] B. Kozicka, E. Pierzchała, *Dobre praktyki w działaniu administracji: spotkania prakseologii i idei w sferze wewnętrznej iw otoczeniu administracji* [w:] *Prawo administracyjne jako miejsce spotkań. Księga jubileuszowa dedykowana Profesorowi Jerzemu Supernatowi*, red. B. Kowalczyk, K. Kulińska-Jachowska, Ł. Prus, M. Tabernacka, I. Sierpowska, E. Skorczyńska, Wrocław 2024, s. 724.

[17] Europejski Kodeks Dobrej Praktyki Administracyjnej przyjęty przez Parlament Europejski dnia 6 września 2001 r., Decyzja w sprawie Kodeksu Dobrej Praktyki Administracyjnej z 29 września 2011 r. (Dz. Urz. UE C 285 z 29 września 2011 r., s. 3), dalej: Kodeks.

decyzji (art. 18 Kodeksu) czy prawa do złożenia skargi do Europejskiego Rzecznika Praw Obywatelskich (art. 26 Kodeksu). Z kolei wymiar aksjologiczny immanentnie związany jest z usposobieniem urzędnika, jego postawą, etyką wykonywania zawodu. W ślad za P. Skrzydlewskim należałoby wskazać, że „etos i sama etyka zawodowa nie istnieją w urzędach z racji arbitralnej decyzji jakiejś władzy, ale z racji przyczyny celowej, motywu", którym „jest dobro wspólne – cel polityki i cel działania całej administracji"[18]. W tym zakresie należy wspomnieć o zasadach uczciwości (art. 11 Kodeksu[19]) i uprzejmości (art. 12 Kodeksu[20]). Oczywiście wszystkie wskazane w Kodeksie zasady pozostają ze sobą w trwałej symbiozie i muszą być przestrzegane przez urzędników. Postępowanie w sposób zgodny z zasadami wyrażonymi w Kodeksie przyczynia się do uwiarygodniana działań podejmowanych przez urzędników i wzmacnia zaufanie do administracji publicznej *sensu stricto*.

Prawo do cyberbezpieczeństwa jako prawo do dobrej administracji (e-administracji)

Mówiąc o prawie do dobrej administracji, nie można pominąć zmian, jakie na przestrzeni ostatnich lat miały miejsce w administracji publicznej. W tym aspekcie należy poruszyć wątek informatyzacji usług publicznych, który ukształtował nowy sposób funkcjonowania administracji publicznej, tj. e-administrację. Realizacja zadań publicznych przy użyciu środków komunikacji elektronicznej nie jest możliwa bez stosownych zmian natury prawnej, organizacyjnej i technologicznej. Co za tym idzie, niezbędna stała się modernizacja struktur administracji publicznej, a także wzmocnienie kompetencji cyfrowych urzędników. Powyższe działania są niezbędne z uwagi na zapewnienie jak najlepszej jakości usług publicznych uwzględniających potrzeby interesariuszy – członków społeczeństwa informacyjnego. Petent, który korzysta z dobrodziejstw transformacji cyfrowej, stawia konkretne wymagania wobec administracji publicznej, do których należą m.in.: całodobowa dostępność do różnorodnych usług publicznych, transparentność działań administracji publicznej, personalizacja i automatyzacja usług oraz bezpieczeństwo (cyberbezpieczeństwo) procedur

[18] P. Skrzydlewski, *Cnoty społeczne w administracji publicznej a etos urzędnika*, „Facta Simonidis" 2022, nr 15(1), s. 169.

[19] Zasada uczciwości oznacza, że urzędnik działa w sposób bezstronny, uczciwy i rozsądny.

[20] Art. 12 Kodeksu stanowi, że urzędnik jest usłużny, zachowuje się właściwie i uprzejmie i pozostaje dostępny w kontaktach z ogółem społeczeństwa. Ponadto stara się być w jak największym stopniu pomocny oraz odpowiadać na skierowane do niego pytania zgodnie z obowiązkami zawodowymi członka personelu. W przypadku braku właściwości powinien kierować obywatela do urzędnika właściwego, a gdy popełni błąd, który narusza prawa lub interesy jednostki, ma obowiązek złożyć stosowne przeprosiny.

administracyjnych[21]. Rzecz jasna, efektywna e-administracja uwzględnia postęp technologiczny. Tym samym oprócz tworzenia portali *stricte* informacyjnych wprowadza się elektroniczne systemy teleinformatyczne umożliwiające obsługę petenta i stałą komunikację z administracją oraz wdraża aplikacje mobilne, z których można korzystać za pomocą urządzeń mobilnych[22]. Przykładami powyższych rozwiązań są m.in. elektroniczna platforma usług administracji publicznej (ePUAP)[23], Biuletyn Informacji Publicznej czy aplikacja mObywatel 2.0[24]. Ze względu na coraz większe zastosowanie technologii informacyjno-komunikacyjnych w administracji publicznej oraz popularność e-usług wśród członków społeczeństwa informacyjnego należy wziąć pod uwagę pewne wyzwania w obszarze cyberbezpieczeństwa e-administracji.

Prawo do dobrej administracji trzeba też rozpatrywać pod kątem koncepcji *good goverance* (dobrego rządzenia). Jej części składowe stanowią takie zasady, jak praworządność, przejrzystość, rzetelność, terminowość, dostęp do informacji publicznej. Akcentowane jest także to, że proces decyzyjny powinien odbywać się zgodnie z zasadami sprawiedliwości i partycypacji społecznej, uwzględniać partnerstwo i dialog społeczny, a przede wszystkim interes społeczny – jako rezultat działań realizowanych przez administrację publiczną[25]. Nie ulega wątpliwości, że wskaźnikiem oceny skuteczności (sprawczości) i wydajności administracji jest rozwój społeczno-gospodarczy, co nie zmienia faktu, że standardy dobrego administrowania oparte są na czterech podstawowych filarach, tj. zasadzie praworządności, etyce urzędniczej, użyteczności usług administracji publicznej oraz ochronie praw człowieka. Ponadto można pokusić się o stwierdzenie, że prawo do dobrej administracji to prawo podmiotowe każdego człowieka[26]. Zważywszy na informatyzację urzędów i cyfryzację usług publicznych, wzrasta potrzeba prawa do dobrej administracji w znaczeniu prawa do bezpiecznego korzystania z e-usług. Trafne wydaje się zatem stwierdzenie, że prawo do cyberbezpieczeństwa stanowi kluczową determinantę prawa do dobrej administracji (e-administracji).

---

[21] B. Tubek, *E-administracja i jej wpływ na współczesne społeczeństwo informacyjne*, „Roczniki Administracji i Prawa" 2025, t. XXV, z. 2, s. 131.

[22] K. Miczek, *Transformacja administracji publicznej w kontekście koncepcji one-stop government*, „Rocznik Administracji Publicznej" 2025, nr 11(1), s. 148.

[23] Art. 3 pkt 13 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2025, poz. 1703 ze zm.) stanowi, że elektroniczna platforma usług administracji publicznej to system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci internet.

[24] Aplikacja mobilna dostępna na urządzenia mobilne, która umożliwia załatwienie spraw urzędowych online; za pomocą aplikacji można skontaktować się z administracją publiczną (np. e-Doręczenia, ePUAP) czy uzyskać dostęp do danych z rejestrów państwowych, np. bazy PESEL, Rejestru Dowodów Osobistych. *mObywatel*, https://www.gov.pl/web/mobywatel (30.07.2025).

[25] M. Princ, *Standardy dobrej administracji w prawie administracyjnym*, Poznań 2016, s. 76–78.

[26] D. Skoczylas, *Krajowy system cyberbezpieczeństwa*, Warszawa 2023, s. 290–291.

Obecnie zapewnienie cyberbezpieczeństwa należy uznać za kluczowe zadanie administracji publicznej. Dzieje się tak ze względu na ilość oraz rodzaj danych, które są przetwarzane w systemach teleinformatycznych wykorzystywanych przez administrację. Przesłanką szczególnie determinującą konieczność wdrożenia polityk cyberbezpieczeństwa są wszelkiego rodzaju okoliczności, które mogą zakłócić świadczenie e-usług bądź spowodować inne negatywne konsekwencje zarówno dla użytkowników, jak i infrastruktury teleinformatycznej[27]. Cyberzagrożenia mogą mieć różny zakres, skalę oddziaływania i skutki. Ataki *ransomware*, DDoS (*Distributed Denial of Service*), *malware* czy *phising* to tylko niektóre z możliwości, które stosują cyberprzestępcy w celu m.in. wyłudzenia poufnych informacji i danych osobowych, kradzieży tożsamości, środków pieniężnych bądź zainfekowania komputera złośliwym oprogramowaniem. Konsekwencje tch naruszeń można rozpatrywać indywidualnie (np. gdy zostanie naruszone prawo do prywatności jednostki) bądź w skali makro (np. zagrożenie stabilności infrastruktury krytycznej i przerwanie ciągłości świadczenia usług kluczowych)[28]. W obliczu potencjalnych cyberzagrożeń cyberbezpieczeństwo jawi się nie tylko jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[29], ale nade wszystko jako bezpieczeństwo użytkowników sieci.

Współcześnie prawo do dobrej e-administracji to również prawo do cyberbezpieczeństwa, na które składa się m.in. zapewnienie ochrony praw jednostki poprzez skuteczną ochronę danych osobowych i ochronę przed dezinformacją. W tym zakresie należy podkreślić dbałość o autentyczność, integralność i poufność danych przetwarzanych przed administrację. Administracja publiczna powinna niezwłocznie usuwać z cyberprzestrzeni nieprawdziwe i sfabrykowane informacje „przy jednoczesnej dbałości o transparentność działań i uszanowanie

[27] Art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz.UE.L 2019 nr 151, s. 15) stanowi, że cyberzagrożenie oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób.

[28] M. Fuksiewicz, *Rodzaje i cechy charakterystyczne cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa*, „Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu" 2023, t. 102, nr 3, s. 54–56.

[29] Zob. art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024, poz. 1077 ze zm.). Zgodnie z nowelizacją ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026, poz. 20 ze zm.) za cyberbezpieczeństwo uznaje się działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (zob. art. 2 pkt 4 znowelizowanej ustawy).

wartości demokratycznych”[30]. Kolejno prawo do dobrej e-administracji wyraża się także przez pryzmat zasady praworządności i bezstronności załatwiania spraw na odległość (online) oraz transparentności procedur (działań podejmowanych w ramach e-administracji). Wspólny mianownik stanowi dostępność e-usług, w tym wykorzystanie technologii *smart* i sztucznej inteligencji. Co zresztą warto odnotować, dyskusja na temat prawa do dobrej e-administracji i prawa do cyberbezpieczeństwa powinna zakładać pewnego rodzaju inwazyjność (szkodliwość) algorytmów. Mogą być one wykorzystywane nie tylko do wzmocnienia innowacyjności, optymalizacji i personalizacji usług, ale też zwiększać ryzyko cyberzagrożeń (np. destabilizować funkcjonowanie e-administracji czy wspierać działalność cyberprzestępców)[31]. Innymi słowy, utrzymanie zaufania do organów administracji publicznej oraz do e-usług świadczonych w ramach administracji wymaga zwrócenia uwagi na kontekst prawa do cyberbezpieczeństwa jako prawa do dobrej e-administracji.

Prawo do cyberbezpieczeństwa pozostaje w logicznym związku z obowiązkami administracji publicznej w zakresie budowy bezpiecznego środowiska online zarówno na płaszczyźnie prawnej, jak i technologicznej. Dlatego tak ważne jest zachowanie jednolitości i przejrzystości procedur w ramach informatyzacji usług publicznych, a w następstwie tego przeprowadzenie analizy i monitoringu stanu informatyzacji i cyberbezpieczeństwa e-usług. Prawo do cyberbezpieczeństwa polega również na zwiększeniu dostępności usług (w tym dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[32]) i różnorodności kanałów komunikacji wewnątrz i poza strukturami administracji przy jednoczesnym zapewnieniu bezpieczeństwa danych i infrastruktury krytycznej. Kolejną kwestią mającą istotne znaczenie w omawianym kontekście jest wzmacnianie umiejętności cyfrowych (cyberhigiena) pracowników administracji publicznej. Obywatel ma prawo wymagać od administracji, a *stricte* od urzędników, którzy korzystają z systemów teleinformatycznych, oprogramowań, aplikacji, portali i innych narzędzi cyfrowych (w celu realizacji zadań publicznych i komunikacji online z petentem), aby posiadali określone (jak najwyższe) kompetencje cyfrowe. Rację należy zatem przyznać A. Łukaszuk, która wskazuje, że na kompetencje cyfrowe kadry administracyjnej składa się „szeroki pakiet umiejętności”, do których należy zaliczyć zarówno „znajomość obsługi komputera i konkretnych programów”, jak i „umiejętność weryfikacji oraz selekcji danych, uczenia się, świadomości i zagrożeń świata

[30] D. Domalewska, *Dezinformacja jako zagrożenie dla demokracji i regulacje prawne w zakresie jej przeciwdziałania w Polsce i wybranych krajach europejskich*, „Politeja” 2024, nr 5(92), s. 377.

[31] D. Skoczylas, *Sztuczna inteligencja a dobrostan człowieka i ochrona praw podstawowych – rozważania na gruncie aktu w sprawie sztucznej inteligencji*, „Studia Prawnoustrojowe” 2025, nr 67, s. 355–358.

[32] Wymagania w zakresie dostępności cyfrowej określone są w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2023, poz. 1440).

cyfrowego”[33]. W istocie prawo do cyberbezpieczeństwa zyskało na znaczeniu w związku z treścią dyrektywy NIS2[34]. Na jej gruncie administracja publiczna została uznana za sektor świadczący usługi kluczowe, co implikuje nie tylko zmiany o charakterze technologicznym, ale głównie konieczność wdrożenia odpowiednich środków organizacyjnych i prawnych, a także wzmocnienie kompetencji cyfrowych pracowników sektora publicznego. Warunkiem *sine qua non* jest też opracowanie bądź udoskonalenie istniejących polityk cyberbezpieczeństwa.

Podsumowanie

Reasumując, obecny model funkcjonowania administracji publicznej ma charakter dualistyczny. Z jednej strony zadania użyteczności publicznej świadczone są w sposób tradycyjny (tj. stacjonarny), z drugiej zaś koncepcja nowoczesnego zarządzania sprawami publicznymi w ramach e-administracji opiera się na założeniach informatyzacji i cyfryzacji. Transformacja cyfrowa przyczyniła się do popularyzacji e-usług w sektorze publicznym. Niewątpliwie wpłynęły na to zalety e-administrowania, takie jak szybkość, automatyzacja czy personalizacja usług. Niestety, oprócz pozytywnych aspektów związanych z modernizacją usług w administracji publicznej należy zwrócić uwagę na potencjalne ryzyko, tj. cyberzagrożenia, których wystąpienie może oddziaływać na bezpieczeństwo użytkowników e-administracji i infrastruktury krytycznej oraz świadczenie usług online. Dlatego też nie dziwi, że jednym z kluczowych elementów przeciwdziałania cyberzagrożeniom będzie odwołanie do pierwotnych założeń prawa do dobrej administracji, które stanowią również kryteria prawa do dobrej e-administracji.

Należałoby przede wszystkim wskazać, że aspekty e-administrowania oparte na zasadach m.in. praworządności, obiektywizmu czy proporcjonalności pozwalają urzeczywistnić postulat prawa do dobrej e-administracji, jednak z uwagi na omówione w niniejszym artykule cyberzagrożenia warto zastanowić się nad istotą cyberbezpieczeństwa. Innymi słowy, prawo do cyberbezpieczeństwa stanowi obecnie jeden z elementów prawa do dobrej administracji (e-administracji), wartość podlegającą szczególnej ochronie prawnej. Ponadto prawo do cyberbezpieczeństwa jest kluczową determinantą prawa do dobrej administracji (e-administracji). Podkreślenia wymaga, że prawo do dobrej e-administracji i prawo do cyberbezpieczeństwa

[33] A. Łukaszuk, *Problematyka kompetencji cyfrowych kadr administracji publicznej jako istotnego czynnika procesu transformacji cyfrowej jednostek samorządu terytorialnego w Polsce*, „Studia Prawnoustrojowe” 2022, nr 58, s. 310.

[34] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 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 2022 nr 333, s. 80).

należy utożsamiać przez pryzmat innowacyjności, dostępności (w tym dostępności cyfrowej dla osób ze szczególnymi potrzebami) i bezpieczeństwa (ochrona danych osobowych, informacji niejawnych, ochrona przed dezinformacją). Ważne miejsce zajmują także takie zagadnienia, jak kompetencje cyfrowe kadry administracyjnej oraz algorytmizacja e-usług. W konkluzji zapewnienie cyberbezpieczeństwa przyczynia się nie tylko do realizacji prawa do dobrej e-administracji, ale również powoduje wzrost zaufania do środowiska online oraz urzędników, którzy realizują zadania z zakresu użyteczności publicznej w sposób elektroniczny.

Bibliografia

Domalewska D., *Dezinformacja jako zagrożenie dla demokracji i regulacje prawne w zakresie jej przeciwdziałania w Polsce i wybranych krajach europejskich*, „Politeja" 2024, 5(92).

Dudzik S., *Podstawy prawne działania e-administracji a ochrona danych osobowych* [w:] *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej*, red. S. Dudzik, I. Kawka, R. Śliwa, Kraków 2022.

Fuksiewicz M., *Rodzaje i cechy charakterystyczne cyberataków oraz zarys działań w obszarze cyberbezpieczeństwa*, „Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu" 2023, t. 102.

Fundowicz S., *Administracja publiczna w świetle nauczania św. Tomasza z Akwinu i jego odczytania przez personalizm*, „Studia Prawnoustrojowe" 2025, nr 68.

Korczak J., *Funkcja usługodawcza administracji publicznej w świetle konstytucyjnych zasad ustrojowych*, „Przegląd Prawa Konstytucyjnego" 2023, nr 4(74).

Kozicka B., Pierzchała E., *Dobre praktyki w działaniu administracji: spotkania prakseologii i idei w sferze wewnętrznej iw otoczeniu administracji* [w:] *Prawo administracyjne jako miejsce spotkań. Księga jubileuszowa dedykowana Profesorowi Jerzemu Supernatowi*, red. B. Kowalczyk, K. Kulińska-Jachowska, Ł. Prus, M. Tabernacka, I. Sierpowska, E. Skorczyńska, Wrocław 2024.

Lubik-Reczek N., Kapsa I., Musiał-Karg M., *Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania*, Poznań 2020.

Łukaszuk A., *Problematyka kompetencji cyfrowych kadr administracji publicznej jako istotnego czynnika procesu transformacji cyfrowej jednostek samorządu terytorialnego w Polsce*, „Studia Prawnoustrojowe" 2022, nr 58.

Miczek K., *Transformacja administracji publicznej w kontekście koncepcji one-stop government*, „Rocznik Administracji Publicznej" 2025, nr 11(1).

mObywatel, https://www.gov.pl/web/mobywatel (30.07.2025).

Princ M., *Standardy dobrej administracji w prawie administracyjnym*, Poznań 2016.

Puczko A., *Model otwartej innowacji w administracji publicznej* [w:] *Prawo administracyjne jako miejsce spotkań. Księga jubileuszowa dedykowana Profesorowi Jerzemu Supernatowi*, red. B. Kowalczyk, K. Kulińska-Jachowska, Ł. Prus, M. Tabernacka, I. Sierpowska, E. Skorczyńska, Wrocław 2024.

Rogacka-Łukasik A., *Wybrane środki służące zapewnieniu dostępności cyfrowej dla osób z niepełnosprawnościami* [w:] *Aksjologiczne i prawne aspekty niepełnosprawności*, red. A. Drabarz, Białystok 2020.

Skoczylas D., *Krajowy system cyberbezpieczeństwa*, Warszawa 2023.

Skoczylas D., *Sztuczna inteligencja a dobrostan człowieka i ochrona praw podstawowych – rozważania na gruncie aktu w sprawie sztucznej inteligencji*, „Studia Prawnoustrojowe" 2025, nr 67.

Skrzydlewski P., *Cnoty społeczne w administracji publicznej a etos urzędnika*, „Facta Simonidis" 2022, nr 15(1).
Smarż J., *Zasada pogłębiania zaufania obywateli do administracji publicznej jako fundament postępowania administracyjnego*, „Prawo i Więź" 2025, nr 1(54).
Smarż J., Świtał P., *Przyjazna administracja elektroniczna* [w:] *Administracja publiczna wobec procesów zmian w XXI wieku. Księga jubileuszowa Profesora Jerzego Korczaka*, red. P. Lisowski, Wrocław 2024.
Tubek B., *E-administracja i jej wpływ na współczesne społeczeństwo informacyjne*, „Roczniki Administracji i Prawa" 2025, t. XXV, z. 2.
Wasilewski K., *E-administracja w Polsce: determinanty rozwoju i bariery wdrożeniowe*, „Przegląd Prawno-Ekonomiczny" 2025, nr 2.
Węglińska J., *Zasada ochrony zaufania obywateli do państwa i do stanowionego przez nie prawa jako dyrektywa poprawnej legislacji*, „Prawo w Działaniu. Sprawy cywilne" 2020, nr 42.

Streszczenie

Celem artykułu jest wskazanie, w jaki sposób rozwój nowych technologii oddziałuje na aktualną politykę administracji publicznej w kwestii zapewnienia cyberbezpieczeństwa. Należy zaznaczyć, że administracja publiczna na gruncie dyrektywy NIS2 została uznana za sektor świadczący usługi kluczowe, co implikuje konieczność dokonania zmian w obrębie opracowania bądź udoskonalenia polityk cyberbezpieczeństwa, wdrożenia odpowiednich środków organizacyjnych i prawnych, wzmocnienia kompetencji cyfrowych pracowników czy zmian o charakterze technologicznym. W artykule przedstawiono pozytywne i negatywne aspekty dotyczące przeobrażenia modelu funkcjonowania administracji publicznej w związku z wprowadzeniem aktów prawnych o tematyce informatyzacji i cyberbezpieczeństwa. Opracowanie podkreśla, że prawo do cyberbezpieczeństwa stanowi obecnie kluczową determinantę prawa do dobrej administracji (e-administracji), wartość podlegającą szczególnej ochronie prawnej.

Słowa kluczowe: cyberbezpieczeństwo, e-administracja, prawo do cyberbezpieczeństwa, prawo do dobrej administracji

THE RIGHT TO "CYBERSECURITY" IN THE CONTEXT OF THE RIGHT TO GOOD ADMINISTRATION (E-GOVERNMENT)

Summary

The aim of this article is to show how the development of new technologies affects the current policies of public administrations to ensure cybersecurity. It should be noted that public administration has been recognized as a key service sector under the NIS2 directive, which implies the need for changes in the development or improvement of cybersecurity policies, the implementation of appropriate organisational and legal measures, the strengthening of digital competences of employees and technological changes. The article outlines the positive and negative aspects regarding the transformation of the public administration's operating model due to the introduction of legislation on computerization and cybersecurity. The article emphasizes that the right to cybersecurity is now a key determinant of the right to good administration (e-government), a value subject to special legal protection.

Keywords: cybersecurity, e-government, right to cybersecurity, right to good administration