

Krzysztof Jurek

Uniwersytet Jagielloński
Szkoła Doktorska Nauk Społecznych

ORCID: ORCID: 0000-0003-4154-6416

e-mail: krzysztof.jurek@doctoral.uj.edu.pl

JEL Classification: H83, D73, L86,
M15, D83, M10

ZARZĄDZANIE W KONTEKŚCIE CYFRYZACJI ADMINISTRACJI PUBLICZNEJ: WYZWANIA I PERSPEKTYWY

Management in the context of the digitalization of public administration:
challenges and prospects

<https://doi.org/10.34739/maj.2026.05.01>

Streszczenie: Celem artykułu było przedstawienie podstaw prawnych oraz europejskich ram regulacyjnych dotyczących cyfryzacji administracji publicznej w Polsce, zwracając szczególną uwagę na konieczność pełnej zgodności z rozporządzeniami eIDAS, RODO oraz dyrektywą NIS2. Wskazuje trzy kluczowe wyzwania dla systemu administracyjnego: zapewnienie bezpieczeństwa danych, przeciwdziałanie narastającym cyberzagrożeniom oraz ograniczanie zjawiska wykluczenia cyfrowego. Artykuł podkreśla również potencjał wykorzystania technologii takich jak sztuczna inteligencja, blockchain czy narzędzia e-demokracji, jednocześnie akcentując potrzebę transparentności algorytmów oraz projektowania usług zgodnie z zasadami inkluzywności. W konkluzji przedstawiono rekomendacje obejmujące systematyczne szkolenia urzędników, certyfikację algorytmicznych modeli decyzyjnych, standaryzację zasad dostępności oraz utrzymanie alternatywnych kanałów obsługi obywateli. Ponadto autor zwraca uwagę na konieczność długofalowego monitorowania skutków wdrażanych rozwiązań cyfrowych oraz potrzebę zintegrowanego zarządzania projektami IT w administracji, co ma umożliwić spójne i zrównoważone rozwijanie infrastruktury cyfrowej państwa.

Słowa kluczowe: administracja publiczna, cyfryzacja, wyzwania w administracji publicznej, rozwój cyfryzacji

Abstract: This article presents the legal foundations and European regulatory framework for the digitization of public administration in Poland, paying particular attention to the need for full compliance with the eIDAS regulations, the GDPR, and the NIS2 Directive. It identifies three key challenges for the administrative system: ensuring data security, countering growing cyber threats, and reducing digital exclusion. The article also highlights the potential of leveraging technologies such as artificial intelligence, blockchain, and e-democracy tools, while emphasizing the need for algorithm transparency and service design in accordance with the principles of inclusiveness. The conclusion presents recommendations including systematic training of officials, certification of algorithmic decision-making models, standardization of accessibility principles, and maintaining alternative channels for serving citizens. Furthermore, the author emphasizes the need for long-term monitoring of the impact of implemented digital solutions and the need for integrated management of IT projects in administration, which will enable the coherent and sustainable development of the state's digital infrastructure.

Keywords: public administration, digitalization, challenges in public administration, prospects for digitalization

Wstęp

Cyfryzacja administracji publicznej stanowi jeden z fundamentalnych procesów transformacyjnych współczesnego państwa, które zobowiązane jest dostosowywać swoje ramy prawne, struktury organizacyjne oraz mechanizmy zarządzania do warunków szybko ewoluującego środowiska technologicznego. Implementacja nowoczesnych rozwiązań cyfrowych w sektorze publicznym ma na celu nie tylko zwiększenie efektywności funkcjonowania urzędów, lecz także poszerzenie dostępności usług publicznych oraz poprawę jakości interakcji państwo – obywatel (Androniceanu, Georgescu, Sabie, 2022, s. 13-14). Jednocześnie proces ten generuje szereg pytań dotyczących zgodności z obowiązującymi standardami prawnymi, ochrony praw jednostki oraz granic ingerencji technologii w sferę administracyjną.

Problematyka ta zajmuje dziś centralne miejsce w dyskursie naukowym prowadzonym w polskiej literaturze prawniczej i administracyjnej. Liczne opracowania podejmują próbę diagnozy dotychczasowych osiągnięć cyfrowej transformacji administracji publicznej w Polsce, analizując zarówno jej potencjał modernizacyjny, jak i zidentyfikowane w ostatnich latach wyzwania natury prawnej, organizacyjnej i społecznej.

Podstawy prawne cyfrowej transformacji administracji publicznej w Polsce wywodzą się bezpośrednio z konstytucyjnych gwarancji praw jednostki. Konstytucja Rzeczypospolitej Polskiej zapewnia obywatelom prawo do informacji o działalności organów władzy publicznej, a jednocześnie chroni prywatność i autonomię informacyjną jednostki (art. 51) (Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. 1997 Nr 78, poz. 483, art. 61, ze zm.). Pierwsze z tych uprawnień implikuje obowiązek transparentnego funkcjonowania instytucji państwowych oraz powszechnego udostępniania informacji publicznej, realizowany m.in. poprzez publikację danych w Biuletynie Informacji Publicznej oraz wdrażanie e-usług umożliwiających obywatelom kontrolę nad procesami administracyjnymi. Drugie prawo konstytucyjne ustanawia ograniczenia w zakresie gromadzenia danych osobowych, nakazując zbieranie jedynie tych informacji, które są niezbędne w demokratycznym państwie prawa, oraz zapewniając obywatelom prawo wglądu, korekty i usunięcia danych dotyczących ich osoby. W konsekwencji przepisy te wyznaczają ramy prawne dla cyfrowych systemów zarządzania informacją i usługami publicznymi, kształtując ich funkcjonalność, bezpieczeństwo oraz relacje administracji z obywatelami.

Na gruncie ustawowym kluczową rolę odgrywa ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005 r (Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2024 poz. 1557). Akt ten, wielokrotnie nowelizowany, określa zasady tworzenia i wykorzystywania systemów teleinformatycznych w administracji publicznej oraz wprowadza obowiązek stosowania form elektronicznych przy realizacji zadań publicznych, takich jak składanie wniosków, komunikacja z petentami czy wydawanie decyzji administracyjnych. Istotne zmiany w funkcjonowaniu administracji przyniosła również rozbudowa centralnych platform elektronicznych, takich jak ePUAP (Elektroniczna Platforma Usług Administracji Publicznej), umożliwiających załatwianie licznych spraw urzędowych online – od złożenia wniosku o dowód osobisty po uzyskanie odpisu aktu stanu cywilnego. Wdrożenie takich rozwiązań wymagało zintegrowanego podejścia do zarządzania systemami informatycznymi oraz ścisłej koordynacji między różnymi jednostkami administracyjnymi (Adnan, Ghazali, Othman, 2022). Jednocześnie rozwój platform cyfrowych stwarza nowe wyzwania związane z bezpieczeństwem danych, interoperacyjnością systemów oraz zapewnieniem powszechnego dostępu do usług administracyjnych dla wszystkich grup społecznych.

Proces cyfryzacji administracji publicznej w Polsce odbywa się w kontekście prawa Unii Europejskiej, co wymaga harmonizacji krajowych regulacji z unijnymi standardami. W obszarze usług elektronicznych szczególne znaczenie ma rozporządzenie eIDAS (Rozporządzenie UE nr 910/2014), które ujednoliciło w państwach członkowskich zasady dotyczące podpisu elektronicznego, pieczęci cyfrowej, znaczników czasu oraz identyfikacji elektronicznej. Wdrożenie tych regulacji w Polsce nastąpiło przede wszystkim poprzez ustawę o usługach zaufania oraz identyfikacji elektronicznej z 5 września 2016 r., ustanawiającą m.in. funkcjonowanie

krajowego węzła identyfikacji elektronicznej oraz status podpisu elektronicznego równoważnego podpisowi własnoręcznemu (Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. (eIDAS), Dz. U. UE L 257/73, 28.8.2014).

Kolejnym istotnym obszarem cyfryzacji administracji publicznej jest bezpieczeństwo infrastruktury teleinformatycznej. Unijna dyrektywa NIS2 z 2022 r., dotycząca bezpieczeństwa sieci i systemów informatycznych, obliguje państwa członkowskie do zaostreżenia wymogów ochrony tzw. infrastruktury krytycznej. W polskim kontekście wymusza to konieczność nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz powiązanych aktów wykonawczych w celu dostosowania krajowego porządku prawnego do standardów NIS2 (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. (dyrektywa NIS2)). Wcześniej wprowadzono już przepisy ustanawiające minimalne wymagania techniczne dla systemów teleinformatycznych w sektorze publicznym, w tym m.in. rozporządzenie w sprawie Krajowych Ram Interoperacyjności z 12 kwietnia 2012 r., które określa podstawowe standardy funkcjonowania systemów wykorzystywanych w administracji. W połączeniu ze strategicznymi dokumentami państwowymi, regulacje te wyznaczają ramy architektury rozwoju e-administracji, kształtując jednocześnie politykę zarządzania bezpieczeństwem cyfrowym oraz integrację systemów teleinformatycznych na poziomie krajowym. Dodatkowo, implementacja tych przepisów wymaga złożonego podejścia do monitorowania ryzyk cybernetycznych oraz wdrażania mechanizmów reagowania na incydenty, co staje się fundamentem zaufania obywateli do usług cyfrowych administracji.

Artykuł został opracowany w oparciu o systematyczny przegląd literatury przedmiotu, obejmujący zarówno krajowe, jak i zagraniczne publikacje naukowe z zakresu prawa administracyjnego oraz nauk o zarządzaniu publicznym (Jurek, 2025). W procesie badawczym dokonano selekcji źródeł według kryteriów aktualności, relewantności tematycznej oraz wartości merytorycznej, ze szczególnym uwzględnieniem opracowań dotyczących cyfryzacji administracji publicznej i regulacji prawnych w tym obszarze. Analizie poddano monografie, artykuły naukowe, akty normatywne oraz dokumenty strategiczne, co umożliwiło wieloaspektowe ujęcie omawianej problematyki. Zastosowana metoda pozwoliła na identyfikację dominujących kierunków badawczych, kluczowych wyzwań oraz luk interpretacyjnych w dotychczasowym dorobku naukowym.

Przegląd literatury

Pomimo licznych korzyści wynikających z informatyzacji administracji publicznej, proces cyfryzacji wiąże się z istotnymi wyzwaniami o charakterze prawnym i społecznym. Najistotniejsze z nich koncentrują się na zapewnieniu równowagi pomiędzy efektywnością funkcjonowania organów administracji a poszanowaniem praw obywateli, w szczególności prawa do prywatności oraz równego dostępu do usług publicznych (Miłek, Nowak, 2021). W literaturze przedmiotu wskazuje się przede wszystkim na dwa zasadnicze obszary problemowe: ochronę danych i bezpieczeństwo informacji oraz przeciwdziałanie wykluczeniu cyfrowemu, które mają kluczowe znaczenie dla kształtowania inkluzywnej i bezpiecznej e-administracji.

Administracja publiczna przetwarza obszerne zasoby danych osobowych obywateli, obejmujące zarówno informacje meldunkowe i podatkowe, jak i dane dotyczące stanu zdrowia czy sytuacji socjalnej. Zapewnienie adekwatnej ochrony tych danych stanowi fundament budowania zaufania społecznego wobec e-usług publicznych. Polskie ramy prawne, w tym art. 51 Konstytucji RP oraz przepisy RODO wraz z krajową ustawą o ochronie danych osobowych, ustanawiają rygorystyczne standardy w zakresie przetwarzania informacji osobowych. Każdy system teleinformatyczny w administracji powinien być projektowany zgodnie z zasadą *privacy by design*, uwzględniając zabezpieczenia danych oraz minimalizację ich gromadzenia już na etapie tworzenia systemu. Organy publiczne są zobowiązane m.in. do powoływania inspektorów ochrony danych, prowadzenia okresowej analizy ryzyka oraz zgłaszania incydentów naruszenia bezpieczeństwa (Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz. U. 2019 poz. 848).

Pomimo obowiązujących regulacji i procedur, w praktyce wciąż dochodzi do poważnych naruszeń, w tym wycieków i kradzieży danych z rejestrów państwowych. Przykładowo, w 2020 r. media donosiły o nieautoryzowanym dostępie do danych użytkowników platformy ePUAP, co istotnie podważyło zaufanie części obywateli do bezpieczeństwa cyfrowych usług administracyjnych (Kubanek, 2025). Zjawisko to wskazuje na potrzebę nie tylko rygorystycznego przestrzegania przepisów prawnych, lecz także systematycznego doskonalenia mechanizmów zarządzania bezpieczeństwem informacji w administracji publicznej oraz zwiększenia świadomości pracowników w zakresie ochrony danych osobowych.

Wraz z rosnącym stopniem cyfryzacji administracji publicznej zwiększa się również skala zagrożeń kierowanych wobec systemów teleinformatycznych instytucji państwowych. Z jednej strony obserwuje się wzrost liczby zaawansowanych ataków cybernetycznych, takich jak ransomware (Oz, Aris, Levi, Uluagac, 2022, s. 17), blokujący dostęp do baz danych, czy phishing (Safi, Singh, 2023, s. 598), ukierunkowany na wyłudzenie danych logowania urzędników. Z drugiej strony, wiele jednostek administracyjnych wciąż korzysta z przestarzałych systemów informatycznych, które nie spełniają współczesnych standardów bezpieczeństwa. Do problemów technicznych dochodzi czynnik ludzki – szacuje się, że istotna część incydentów wynika z błędów pracowników, np. nieostrożnego obchodzenia się z hasłami czy otwierania zainfekowanych załączników w wiadomościach e-mail.

W Polsce również odnotowano liczne ataki wymierzone w systemy rządowe i samorządowe, co jednoznacznie podkreśla konieczność stałego wzmacniania mechanizmów ochrony infrastruktury teleinformatycznej. Kluczowe znaczenie mają zarówno inwestycje w nowoczesne technologie zabezpieczeń, takie jak szyfrowanie danych, systemy wykrywania włamań czy regularne tworzenie kopii zapasowych, jak i kompleksowe szkolenia personelu w zakresie higieny cyfrowej i ochrony informacji. Podnoszenie świadomości pracowników administracji jest szczególnie istotne, gdyż nawet najbardziej zaawansowane procedury bezpieczeństwa okażą się nieskuteczne, jeśli nie zostaną odpowiednio wdrożone i przestrzegane w praktyce (Jurek, 2025, s. 128-129). W związku z tym zarządzanie bezpieczeństwem cyfrowym powinno obejmować równoległe aspekty techniczne, organizacyjne oraz edukacyjne, tworząc spójny system odporności administracji publicznej na zagrożenia cybernetyczne.

W kontekście ochrony danych osobowych kluczowe znaczenie ma zapewnienie pełnej transparentności działań administracji publicznej. Badania empiryczne wskazują, że obywatele chętniej korzystają z e-usług, gdy mają pewność, że ich dane są przetwarzane w sposób przejrzysty i zgodny z obowiązującymi regulacjami prawnymi. W związku z tym administracja powinna jednoznacznie informować petentów o rodzaju gromadzonych danych, celach ich przetwarzania oraz stosowanych środkach bezpieczeństwa. Istotnym elementem budowania zaufania są również rozwiązania techniczne wspierające ochronę prywatności, takie jak anonimizacja danych w procesie udostępniania zbiorczych informacji statystycznych czy podczas testowania nowych narzędzi cyfrowych. Zapewnienie bezpieczeństwa informacji oraz poszanowania prywatności obywateli stanowi warunek sine qua non efektywności i akceptacji e-administracji. Realizacja tego celu wymaga nie tylko rygorystycznego przestrzegania przepisów prawa, lecz także systematycznego doskonalenia środków technicznych i organizacyjnych. Niezbędne jest wprowadzenie mechanizmów ciągłego monitorowania zagrożeń, regularnej aktualizacji zabezpieczeń oraz promowanie kultury organizacyjnej, która stawia ochronę danych w centrum zarządzania administracją cyfrową. Tego rodzaju działania powinny być integralną częścią rozwoju usług cyfrowych, tak aby innowacyjność i funkcjonalność systemów szły w parze z bezpieczeństwem i zaufaniem społecznym, jak również w modelowy sposób wspierały partycypację lokalną (Jurek, 2023, s. 52).

Kolejnym istotnym wyzwaniem towarzyszącym procesowi cyfryzacji administracji publicznej jest zagwarantowanie, że rozwój usług cyfrowych będzie inkluzywny i nie doprowadzi do pogłębiania istniejących nierówności społecznych. Problem wykluczenia cyfrowego wciąż dotyka znaczną część społeczeństwa, zwłaszcza osoby starsze, mieszkańców obszarów peryferyjnych oraz grupy o niższym statusie społeczno-

ekonomicznym. Z danych Eurostatu wynika, że około 17% mieszkańców Polski w 2021 r. nie korzystało w ogóle z Internetu, co oznacza, iż dla istotnej części obywateli dostęp do e-usług pozostaje faktycznie wyłączony (Czarnecka, Kelm, Koczur, 2023, s. 96-97). Źródłem tego zjawiska należy upatrywać zarówno w niedostatkach infrastrukturalnych, takich jak brak dostępu do szerokopasmowych łącz internetowych w niektórych regionach kraju, jak i w niewystarczającym poziomie kompetencji cyfrowych, uniemożliwiającym samodzielne korzystanie z usług administracji online (Jurek, 2023, s. 93-94). W związku z tym działania legislacyjne muszą być uzupełnione programami inwestycyjnymi w infrastrukturę telekomunikacyjną oraz inicjatywami edukacyjnymi, obejmującymi szkolenia z zakresu podstaw obsługi komputera i Internetu. Bez odpowiedniego wsparcia w tych obszarach nawet najbardziej zaawansowane regulacje prawne dotyczące e-administracji pozostaną niewystarczające i nie osiągną zamierzonego efektu społecznego.

Istotnym zagadnieniem towarzyszącym procesowi cyfryzacji administracji publicznej jest także zapewnienie pełnej dostępności cyfrowej dla osób o szczególnych potrzebach, w tym dla osób z różnymi rodzajami niepełnosprawności. Publiczne portale internetowe oraz aplikacje administracyjne powinny być projektowane zgodnie z uznanymi standardami dostępności, takimi jak WCAG 2.1, umożliwiając korzystanie z nich użytkownikom niewidomym (z wykorzystaniem czytników ekranu), osobom niesłyszącym, a także osobom z ograniczeniami motorycznymi lub poznawczymi (Paul, 2023, s. 667). W praktyce jednak wiele systemów administracyjnych nadal nie spełnia przewidzianych prawem wymogów. Problemy te obejmują zarówno niedostosowane interfejsy użytkownika, brak napisów w materiałach audiowizualnych, jak i trudności w obsłudze kluczowych funkcji – takich jak składanie podpisu elektronicznego – przez osoby z różnorodnymi dysfunkcjami. Ustawa o dostępności cyfrowej z 2019 r. nałożyła na podmioty publiczne obowiązek osiągnięcia określonego poziomu dostępności swoich stron internetowych i aplikacji mobilnych, jednak stopień wdrożenia tych regulacji pozostaje zróżnicowany. Z tego względu konieczne jest nie tylko wzmocnienie nadzoru nad realizacją ustawowych obowiązków, lecz także zapewnienie odpowiedniego wsparcia – organizacyjnego, doradczego i finansowego – dla jednostek administracji publicznej w procesie dostosowywania istniejących systemów cyfrowych. Tylko kompleksowe działania w tym zakresie pozwolą zagwarantować, że cyfryzacja administracji będzie procesem inkluzywnym i rzeczywiście służącym wszystkim obywatelom.

Aby skutecznie przeciwdziałać zjawisku wykluczenia cyfrowego, administracja publiczna powinna realizować działania w dwóch komplementarnych obszarach. Po pierwsze, konieczne jest zapewnienie alternatywnych form dostępu do usług publicznych dla osób, które z różnych powodów nie są w stanie korzystać z kanałów elektronicznych. Obejmuje to utrzymanie tradycyjnych punktów obsługi interesantów, funkcjonowanie infolinii, tworzenie mobilnych placówek urzędowych, a także oferowanie wsparcia asystenckiego przy wypełnianiu formularzy online. Po drugie, administracja powinna aktywnie prowadzić działania edukacyjne i promocyjne w zakresie korzystania z e-usług. Znaczna część obywateli nie korzysta z narzędzi cyfrowych nie z powodu braku dostępu technologicznego, lecz z braku świadomości ich funkcjonowania lub z obawy przed korzystaniem z nowych rozwiązań. Doświadczenia międzynarodowe potwierdzają, że rozwój umiejętności cyfrowych wpływa bezpośrednio na zwiększenie partycypacji (Jurek, 2025, s. 17-18) obywateli w e-administracji i życiu publicznym (2022). Podobnie jak w obszarze ochrony danych, również w zakresie inkluzywności cyfrowej kluczowe znaczenie ma rzetelna diagnoza wyzwań i odpowiednio zaplanowana polityka długofalowa. Administracja powinna systematycznie monitorować stopień wykorzystania usług cyfrowych przez różne grupy społeczne, identyfikować bariery o charakterze technicznym, edukacyjnym czy językowym, a następnie wdrażać adekwatne środki naprawcze. Jedynie takie podejście pozwoli uniknąć sytuacji, w której cyfryzacja przynosi korzyści głównie obywatelom już uprzywilejowanym pod względem dostępu do usług publicznych, natomiast osoby znajdujące się w grupach marginalizowanych pozostają nadal wykluczone.

Wyniki

Rozwój zaawansowanych technologii informatycznych otwiera przed administracją publiczną całkowicie nowe perspektywy w zakresie świadczenia usług oraz optymalizacji procesów organizacyjnych. Narzędzia takie jak sztuczna inteligencja, analityka big data, przetwarzanie w chmurze czy technologie rozproszonego rejestru (blockchain) mogą zasadniczo przeobrazić mechanizmy pozyskiwania, przetwarzania i udostępniania informacji publicznej. Jednocześnie implementacja tych rozwiązań generuje złożone dylematy prawne i etyczne, odnoszące się chociażby do przypisania odpowiedzialności za decyzje podejmowane autonomicznie przez systemy algorytmiczne czy do zapewnienia adekwatnej ochrony prywatności jednostki w warunkach funkcjonowania zdecentralizowanych baz danych (Dudarski, 2024, 66-68). W literaturze przedmiotu akcentuje się, iż pełne i efektywne wykorzystanie nowoczesnych technologii w sferze publicznej wymaga nie tylko rewizji obowiązujących procedur administracyjnych, lecz także stopniowej transformacji klasycznych instytucji prawa administracyjnego, tak aby mogły one odpowiadać na wyzwania epoki cyfrowej oraz zapewniać równowagę między innowacyjnością a gwarancjami ochrony praw jednostki.

Sztuczna inteligencja (AI) odgrywa coraz bardziej znaczącą rolę w sektorze publicznym na świecie, obejmując zastosowania zarówno w zaawansowanej analizie danych masowych wykorzystywanych w procesach planistycznych, jak i w automatyzacji powtarzalnych zadań administracyjnych czy obsłudze komunikacji z obywatelami. W polskiej administracji publicznej prowadzone są obecnie pilotażowe wdrożenia systemów opartych na AI, w tym rozwiązań typu Robotic Process Automation, umożliwiających m.in. automatyczną weryfikację składanych dokumentów oraz generowanie wstępnych projektów decyzji administracyjnych (2022). Praktyka państw uznawanych za liderów cyfrowej transformacji – takich jak Estonia – wskazuje, że implementacja algorytmów może znacząco usprawnić realizację określonych kategorii usług publicznych. W estońskich e-urzędach systemy oparte na sztucznej inteligencji wspierają m.in. proces przyznawania świadczeń oraz rejestracji działalności gospodarczej, co skraca czas obsługi obywateli z kilku dni do zaledwie kilku minut.

Korzyści wynikające z implementacji narzędzi sztucznej inteligencji muszą być równoważone adekwatnym i precyzyjnym otoczeniem regulacyjnym, którego celem jest zarówno zapobieganie potencjalnym nadużyciom, jak i zagwarantowanie obywatelom pełnej ochrony ich praw. W aktualnym stanie prawnym brakuje szczegółowych, sektorowych regulacji normujących wykorzystanie AI w administracji publicznej (2025). Trwające prace legislacyjne nad unijnym Aktem o sztucznej inteligencji mają wprowadzić wielopoziomą klasyfikację systemów AI według stopnia ryzyka oraz nałożyć określone obowiązki na podmioty wdrażające te technologie. Już na obecnym etapie formułowane są jednak zasadnicze pytania dotyczące konsekwencji prawnych takich wdrożeń (Blicharz, Zacharko, 2024, s. 352). Jednym z kluczowych zagadnień jest kwestia odpowiedzialności za decyzje podejmowane z udziałem lub w pełni przez algorytmy. Jeśli system AI popełni błąd prowadzący do naruszenia praw jednostki – na przykład bezzasadnie odmówi przyznania świadczenia – powstaje problem wskazania podmiotu odpowiedzialnego. Tradycyjny model prawa administracyjnego opiera się na odpowiedzialności organu lub urzędnika, co nie przystaje do sytuacji, w której element decyzyjny zostaje częściowo lub całkowicie zautomatyzowany. W konsekwencji pojawia się potrzeba wypracowania nowych mechanizmów nadzoru, kontroli i przypisywania winy, uwzględniających zarówno rolę organu stosującego system, jak i producentów oprogramowania.

Kolejny istotny problem dotyczy przejrzystości algorytmów. Znaczna część współczesnych modeli, zwłaszcza opartych na głębokich sieciach neuronowych, funkcjonuje w sposób zbliżony do „czarnej skrzynki”, co oznacza, że nawet ich twórcy nie są w stanie jednoznacznie wyjaśnić logiki podejmowanych rozstrzygnięć. Taki stan rzeczy jest trudny do pogodzenia z zasadą zaufania obywateli do państwa oraz z obowiązkiem sporządzania zrozumiałego uzasadnienia decyzji administracyjnych. Jeżeli sztuczna inteligencja wspiera lub zastępuje urzędnika w procesie decyzyjnym, obywatel powinien posiadać realne prawo do poznania podstaw

merytorycznych i logicznych rozstrzygnięcia. W literaturze zwraca się ponadto uwagę na ryzyko generowania przez niekontrolowane algorytmy decyzji stroniczych, nieobiektywnych bądź wręcz dyskryminujących (2024). Z tego względu konieczne jest tworzenie mechanizmów oceny wpływu systemów AI na prawa podstawowe, wdrażanie audytów algorytmicznych oraz stosowanie zasad etycznego projektowania, tak aby innowacyjność nie odbywała się kosztem standardów demokratycznego państwa prawa.

Technologia blockchain stanowi kolejne narzędzie, które w ostatnich latach zyskuje szczególne zainteresowanie w kontekście modernizacji struktur administracji publicznej. Jako rozproszony rejestr kryptograficzny, gwarantujący integralność i weryfikowalność zapisów, blockchain odróżnia się od tradycyjnych, scentralizowanych baz danych przede wszystkim brakiem jednego nadrzędnego administratora (2023). Informacje są przechowywane równolegle w węzłach sieci, a ich modyfikacja wymaga osiągnięcia konsensusu przez większość uczestników. Taki model zapewnia wyjątkowo wysoki poziom odporności na manipulacje, co czyni go szczególnie atrakcyjnym z perspektywy procedur administracyjnych wymagających stabilności, transparentności i pełnej audytowalności. Jednym z najczęściej przywoływanych obszarów potencjalnego wykorzystania blockchainu jest prowadzenie rejestrów publicznych, takich jak księgi wieczyste, ewidencje gruntów czy rejestr pojazdów. Zapis każdej czynności – przykładowo transakcji zbycia nieruchomości – byłby chronologicznie utrwalany w łańcuchu bloków, a jego modyfikacja pozostawiałaby nieusuwalny ślad, eliminując ryzyko fałszerstw i wzmacniając pewność obrotu prawnego. Inspirującym precedensem jest projekt pilotażowy zrealizowany w Gruzji, gdzie blockchain wykorzystano do rejestracji praw własności. Z obserwacji wynika, że wdrożenie to przyczyniło się zarówno do skrócenia czasu finalizacji transakcji, jak i do zwiększenia zaufania uczestników rynku.

Pomimo znaczącego potencjału technologicznego, wdrożenie blockchainu w sektorze publicznym napotyka na szereg istotnych ograniczeń prawnych, technicznych i organizacyjnych. Jednym z najpoważniejszych wyzwań jest zapewnienie zgodności tej technologii z regulacjami dotyczącymi ochrony danych osobowych. Kluczowa cecha blockchainu – jego niezmiennosc – pozostaje w pozornym konflikcie z prawem do sprostowania i usunięcia danych, gwarantowanym przez RODO. Jeśli dane identyfikujące obywatela zostaną raz zapisane w łańcuchu bloków, ich późniejsze usunięcie jest w praktyce bardzo trudne: każda ingerencja w zapis naruszałaby integralność całej struktury. Z tego powodu w literaturze i praktyce proponuje się różne rozwiązania kompensacyjne, m.in. przechowywanie danych w postaci zaszyfrowanej (gdzie usunięcie polega na zniszczeniu klucza deszyfrującego, a więc uniemożliwia odczyt informacji) lub umieszczanie w blockchainie jedynie kryptograficznych skrótów (hashy), przy jednoczesnym przechowywaniu właściwych danych w zewnętrznych, tradycyjnych bazach. Niezależnie jednak od wybranej metody, nieodzowne jest stworzenie jasnych podstaw prawnych, które pozwolą pogodzić specyfikę blockchainu z reżimem ochrony prywatności (Moura, Brauner, Janissek-Muniz, 2020, s. 264). Dodatkowym wyzwaniem jest brak ujednoliconych standardów interoperacyjności oraz kwestie skalowalności systemów blockchain. Obecnie funkcjonuje wiele konkurencyjnych rozwiązań – zarówno publicznych, jak i prywatnych – które nie są z natury ze sobą kompatybilne. Masowe wdrożenie tej technologii w administracji wymagałoby przyjęcia wspólnych norm technicznych, tak aby systemy poszczególnych urzędów mogły współdziałać i wymieniać informacje. Istotnym ograniczeniem jest również wydajność: klasyczne łańcuchy bloków, takie jak Bitcoin, obsługują zaledwie kilka transakcji na sekundę, co jest niewystarczające w kontekście usług publicznych generujących ogromne wolumeny operacji. W rezultacie konieczne jest rozważenie bardziej zaawansowanych modeli blockchainu, np. rozwiązań opartych na mechanizmach konsensusu o wyższej przepustowości lub architekturach hybrydowych.

Wnioski i rekomendacje

Mimo licznych korzyści płynących z rozwoju e-demokracji, jej praktyczna implementacja napotyka szereg istotnych ograniczeń o charakterze społecznym i strukturalnym. Najpoważniejszą barierą pozostaje

wspomniane wcześniej wykluczenie cyfrowe: jeśli znacząca część obywateli nie posiada odpowiedniej infrastruktury, kompetencji bądź pewności w korzystaniu z technologii informacyjnych, wówczas wyniki konsultacji czy głosowań elektronicznych mogą odzwierciedlać jedynie poglądy grup bardziej uprzywilejowanych technologicznie. Badania empiryczne konsekwentnie wskazują, że w procesach partycypacji cyfrowej dominują osoby młodsze, lepiej wykształcone i częściej zamieszkujące duże ośrodki miejskie, podczas gdy seniorzy, osoby o niższym statusie materialnym czy mieszkańcy regionów peryferyjnych wykazują znacznie mniejszą aktywność. Drugim kluczowym wyzwaniem jest niski poziom zaangażowania obywatelskiego w ogóle (Rahnama, 2020, 146). Nawet w sytuacji, gdy narzędzia e-partycypacji są dostępne, użyteczne i formalnie otwarte dla wszystkich, wiele osób nie przejawia zainteresowania udziałem w debacie publicznej. Przyczyn tego stanu rzeczy jest wiele: brak czasu, przeciążenie informacyjne, poczucie braku wpływu na decyzje władz, sceptycyzm wobec skuteczności konsultacji czy też niewystarczająca promocja istniejących instrumentów partycypacyjnych. Doświadczenia międzynarodowe pokazują, że samo udostępnienie technologii nie prowadzi automatycznie do wzrostu aktywności obywateli. E-demokracja wymaga trwałej kultury uczestnictwa, opartej na długofalowej edukacji obywatelskiej, wzmacnianiu zaufania do instytucji publicznych oraz konsekwentnym zachęcaniu do podejmowania współodpowiedzialności za decyzje publiczne (Bastos, Fernández-Caballero, Pereira, Rocha, 2022, s. 5).

Analizując perspektywy rozwoju cyfryzacji administracji publicznej, można wskazać na jej istotny potencjał w zakresie wzmocnienia procesów demokratycznych – pod warunkiem skutecznego przewyższenia istniejących ograniczeń technologicznych, edukacyjnych i społecznych. Szczególne znaczenie przypada edukacji obywatelskiej oraz kształceniu kompetencji cyfrowych już na etapie szkolnym, co pozwala wykształcić postawy aktywnego uczestnictwa i zdolność racjonalnego korzystania z narzędzi e-demokracji. Równocześnie niezbędne jest projektowanie i rozwój intuicyjnych, interaktywnych platform cyfrowych, które umożliwiają szeroką partycypację społeczną (Pakhnenko, Kuan, 2023, s. 115). Przykładem innowacyjnego wsparcia procesów konsultacyjnych mogą być inteligentne systemy wspomagania decyzji (chatboty), które w sposób przystępny objaśniają złożone zagadnienia legislacyjne, umożliwiając obywatelom świadome formułowanie opinii. Integralnym elementem cyfryzacji pozostaje zapewnienie bezpieczeństwa procesów demokratycznych w środowisku online; w tym kontekście blockchain może pełnić funkcję gwaranta integralności e-głosowań oraz autentyczności udostępnianych dokumentów.

Cyfrowa partycypacja wpisuje się w nowoczesny model zarządzania publicznego, określany w literaturze przedmiotu jako *governance 2.0*, który zakłada przejście od jednostronnej komunikacji „administracja – obywatel” do modelu wielokierunkowego, w którym mieszkańcy stają się współtwórcami decyzji publicznych. Empiryczne obserwacje wskazują, że wdrożenie narzędzi e-partycypacji koreluje ze wzrostem aktywności społecznej, zarówno pod względem liczby uczestników konsultacji, jak i ilości zgłaszanych inicjatyw, np. w ramach budżetów partycypacyjnych. Tendencja ta ma charakter pozytywny i powinna być systematycznie wzmacniana. W miarę jak kolejne pokolenia, wychowane w środowisku cyfrowym, włączają się w życie publiczne, oczekiwania dotyczące możliwości realizowania spraw urzędowych oraz wyrażania opinii drogą elektroniczną stają się standardem. Wyzwanie dla administracji publicznej polega na zapewnieniu inkluzywności procesu cyfryzacji, tak aby innowacyjne rozwiązania nie prowadziły do marginalizacji żadnej grupy społecznej, a partycypacja cyfrowa stała się faktycznym mechanizmem wzmacniającym demokratyczne praktyki.

Cyfryzacja administracji publicznej w Polsce stanowi proces wielowymiarowy i długookresowy, wymagający skoordynowanych działań infrastrukturalnych, prawnych oraz społecznych. Kluczowe jest nie tylko unowocześnianie systemów teleinformatycznych i rozwijanie architektury cyfrowej państwa, lecz także stałe dostosowywanie regulacji prawnych do dynamiki środowiska technologicznego oraz wzmacnianie

społecznego zaufania do wdrażanych rozwiązań. Przeprowadzona analiza pozwala sformułować kilka zasadniczych konkluzji.

Fundamentem wszelkich działań cyfryzacyjnych muszą pozostać standardy konstytucyjne, w szczególności prawo do informacji publicznej oraz prawo do prywatności i ochrony danych osobowych. Każde wdrażane narzędzie e-administracji powinno być systematycznie weryfikowane pod kątem zgodności z Konstytucją RP i Kodeksem postępowania administracyjnego oraz z ustawodawstwem sektorowym, w tym ustawą o dostępie do informacji publicznej, ustawą o ochronie danych osobowych i ustawą o informatyzacji działalności podmiotów publicznych. Kluczowym wyzwaniem pozostaje utrzymanie właściwej równowagi między efektywnością usług a ich inkluzywnością. Rozwiązania cyfrowe muszą być projektowane w sposób zapewniający realną dostępność dla wszystkich grup społecznych, niezależnie od ich kompetencji cyfrowych, sytuacji ekonomicznej czy sprawności użytkownika, przy równoczesnym zagwarantowaniu wysokiej jakości, skróconego czasu realizacji oraz wygody obsługi.

Implementacja innowacyjnych technologii – takich jak automatyzacja procesów decyzyjnych, systemy oparte na sztucznej inteligencji czy zdecentralizowane struktury przechowywania danych – wymaga szczególnej ostrożności i zgodności z zasadami państwa prawa. Automatyzacja nie może prowadzić do ograniczenia prawa jednostki do sprawiedliwego postępowania, kontroli decyzji administracyjnych ani przejrzystości działania organów publicznych. Podobnie decentralizacja czy intensyfikacja przetwarzania danych muszą pozostawać w ścisłym związku z rygorystycznymi standardami ochrony prywatności. W konsekwencji cyfryzacja administracji powinna być postrzegana nie jako cel sam w sobie, lecz jako narzędzie modernizacji państwa, którego efektywność zależy od jednoczesnego zachowania ładu prawnego, zapewnienia dostępności usług oraz utrzymania wysokich standardów ochrony praw obywatelskich.

Bibliografia

- Adnan, M., Ghazali, M., & Othman, N. Z. S. (2022). E-participation within the context of e-government initiatives: A comprehensive systematic review. *Telematics and Informatics Reports* (8), 100015. <https://doi.org/10.1016/j.teler.2022.100015>.
- Androniceanu, A., Georgescu, I., & Sabie, O. M. (2022). The impact of digitalization on public administration, economic development, and well-being in the EU countries. *Central European Public Administration Review* (20), 9.
- Bastos, D., Fernández-Caballero, A., Pereira, A., & Rocha, N. P. (2022). Smart city applications to promote citizen participation in city management and governance: A systematic review. *Informatics* 9(4), 89. <https://doi.org/10.3390/informatics9040089> (MDPI).
- Blicharz, J., & Zacharko, L. (2024). Wdrażanie technologii sztucznej inteligencji w administracji publicznej – kilka refleksji. W: P. Lisowski (Red.), *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka* (ss. 349-355).
- Czarnecka, M., Kelm, H., & Koczur, W. (2023). Wykluczenie cyfrowe seniorów w zakresie korzystania z usług społecznych w Polsce w dobie demograficznego starzenia się ludności. *Optimum. Economic Studies* 1(111), 89-106.
- Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. *PeerJ Computer Science* (9), e1705. <https://doi.org/10.7717/peerj-cs.1705> (PeerJ).
- Dudarski, Ł. (2024). Cyfryzacja administracji publicznej w Polsce: Wyzwania i perspektywy. *Zeszyty Naukowe Collegium Witelona* 53(4), 57-70.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. (dyrektywa NIS2).
- Jurek, K. (2023). Zarządzanie kapitałem ludzkim w środowisku o wysokich kompetencjach – administracja publiczna. *Studia Administracji i Bezpieczeństwa* 14, 89-100. <https://doi.org/10.5604/01.3001.0053.7822>.
- Jurek, K. (2023). Dialog i partycypacja obywatelska na poziomie lokalnym na przykładzie miasta Krakowa. *Zeszyty Naukowe Collegium Witelona* 4(49), 49-59. <https://doi.org/10.5604/01.3001.0054.5169>.
- Jurek, K. (2025). The role of talent management in knowledge-based organizations. *Olsztyn Economic Journal* 20(2), 125-135. <https://doi.org/10.31648/oej.11596>.

- Jurek, K. (2025). Participatory budget implementation models in Poland as a contribution to organizational listening to the needs of residents: Diversity of practices and legislative consequences. *Management and Administration Journal* 65(4). <https://doi.org/10.34739/maj.2025.04.02>.
- Jurek, K. (2025). Basic literature review for young scientists. *SJ – Economics Scientific Journal* 59(4), 90-100. <https://doi.org/10.58246/sj-economics.v59i4.707>.
- Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. 1997 Nr 78, poz. 483, art. 61, ze zm.
- Kubanek, M. (2025). Elektroniczna platforma usług administracji publicznej (ePUAP) jako nowoczesna technologia administracji publicznej. *Dyskurs Prawniczy i Administracyjny* 1.
- Milek, D., & Nowak, P. (2021). Rozwój usług elektronicznej administracji publicznej w Polsce na tle Unii Europejskiej. *Nierówności Społeczne a Wzrost Gospodarczy* 65, 47-73.
- Moura, L. M. F. D., Brauner, D. F., & Janissek-Muniz, R. (2020). Blockchain and a technological perspective for public administration: A systematic review. *Revista de Administração Contemporânea* 24, 259-274.
- Mubarak, F., & Suomi, R. (2022). Elderly forgotten? Digital exclusion in the information age and the rising grey digital divide. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing* 59. <https://doi.org/10.1177/00469580221096272>.
- Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys* 54(11s), 1-37. <https://doi.org/10.1145/3514229>.
- Pakhnenko, O., & Kuan, Z. (2023). Ethics of digital innovation in public administration. *Business Ethics and Leadership* 7(1), 113-121.
- Passi, S., & Vorvoreanu, M. (2022). Overreliance on AI: Literature review. *Microsoft Research*, 339-340. Retrieved from <https://www.microsoft.com/en-us/research/wp-content/uploads/2022/06/Aether-Overreliance-on-AI-Review-Final-6.21.22.pdf>.
- Paul, S. (2022). Accessibility analysis using WCAG 2.1: Evidence from Indian e-government websites. *Universal Access in the Information Society* 22(2), 663-669. <https://doi.org/10.1007/s10209-021-00861-9> (OUCI).
- Rahnema, M. (2020). Participation. In *The applied theatre reader* (pp. 143-149). Routledge.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. (eIDAS), Dz.U. UE L 257/73, 28.8.2014.
- Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University-Computer and Information Sciences* 35(2), 590-611. <https://doi.org/10.1016/j.jksuci.2023.01.004>.
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2024 poz. 1557.
- Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U. 2019 poz. 848.