

DOI: 10.5604/01.3001.0055.2334

**Łukasz Dudarski**

e-mail: lukaszdudarski7@wp.pl

ORCID: 0009-0008-5511-3578

## **Cyfryzacja administracji publicznej w Polsce: wyzwania i perspektywy**

### **STRESZCZENIE**

Artykuł syntetycznie omawia fundamenty prawne i europejskie ramy cyfryzacji polskiej administracji, zwracając uwagę na konieczność zgodności z eIDAS, RODO i NIS2. Wskazuje trzy główne wyzwania: bezpieczeństwo danych, cyberzagrożenia oraz wykluczenie cyfrowe. Autorzy akcentują potencjał AI, blockchainu i narzędzi e-demokracji, podkreślając zarazem potrzebę przejrzystości algorytmów i inkluzywnego projektowania usług. Konkluzją są rekomendacje: szkolenia urzędników, certyfikacja algorytmów, jednolite standardy dostępności i utrzymanie alternatywnych kanałów obsługi obywateli.

**Słowa kluczowe:** cyfryzacja administracji publicznej,; e-government, ochrona danych osobowych, cyberbezpieczeństwo, wykluczenie cyfrowe, dostępność cyfrowa, sztuczna inteligencja, blockchain, e-partycypacja obywatelska, prawo administracyjne.

### **Wprowadzenie**

Cyfryzacja administracji publicznej jest jednym z kluczowych procesów transformacyjnych współczesnego państwa, które musi dostosować swoje struktury prawne i organizacyjne do dynamicznie zmieniającego się środowiska technologicznego. Wprowadzenie nowoczesnych technologii do administracji publicznej ma na celu zwiększenie efektywności działania urzędów oraz dostępności usług dla obywateli. Jednocześnie przemiany te rodzą pytania o zgodność z zasadami prawnymi i ochronę praw obywatelskich. Zagadnienie to znajduje się w centrum uwagi polskiej literatury prawniczej i administracyjnej ostatnich lat – liczne opracowania analizują osiągnięcia i wyzwania cyfrowej transformacji administracji w Polsce<sup>1</sup>.

Niniejszy artykuł przedstawia przekrojową analizę prawnych, technologicznych i organizacyjnych aspektów wdrażania e-administracji w Polsce, uwzględniając podstawy

---

<sup>1</sup> Por. np. M. Kozak, *Cyfryzacja administracji publicznej w Polsce – wyzwania i perspektywy rozwoju*, Wydawnictwo Uniwersytetu Warszawskiego, 2020; M. Nowak, *Cyfryzacja administracji publicznej w Polsce*, Warszawa 2021, M. Kwiecień, *Cyfryzacja usług publicznych w Polsce – stan i wyzwania*, Wydawnictwo Naukowe UAM, 2021.

prawne tego procesu, główne napotymane problemy (takie jak ochrona danych osobowych czy wykluczenie cyfrowe) oraz rosnącą rolę nowych technologii (sztucznej inteligencji, blockchain) w sektorze publicznym. Szczególna uwaga została poświęcona konstytucyjnym ramom cyfryzacji – prawu do informacji publicznej, ochronie prywatności – oraz wynikającym z nich wymogom prawnym. Artykuł kończy się podsumowaniem najważniejszych wniosków oraz rekomendacjami usprawniającymi proces dalszej cyfryzacji administracji.

## **1. Ramy prawne cyfryzacji administracji publicznej**

### **1.1. Konstytucyjne i ustawowe podstawy cyfryzacji**

Podstawy prawne transformacji cyfrowej administracji w Polsce zostały określone już na poziomie konstytucyjnym. Konstytucja RP gwarantuje obywatelom prawo do uzyskiwania informacji o działalności organów władzy publicznej (art. 61) oraz chroni prywatność i autonomię informacyjną jednostki (art. 51).<sup>2</sup> Pierwsze z tych praw przekłada się na obowiązek transparentności działania organów władzy i zapewnienia powszechnego dostępu do informacji publicznej (realizowanego m.in. poprzez publikację informacji w Biuletynie Informacji Publicznej oraz udostępnianie e-usług umożliwiających wgląd w działania administracji). Drugie z praw konstytucyjnych nakłada na władze publiczne wymóg, by nie pozyskiwały i nie gromadziły informacji o obywatelach ponad to, co niezbędne w demokratycznym państwie prawnym, a także by każdy miał wgląd w dotyczące go urzędowe zbiory danych i możliwość ich poprawiania lub usunięcia. Te zasady wyznaczają fundamentalne ramy, w których musi mieścić się cyfryzacja administracji.

Na gruncie ustawowym kluczową rolę odgrywa ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005 r.<sup>3</sup> Akt ten (wielokrotnie nowelizowany) określa zasady tworzenia i wykorzystywania systemów teleinformatycznych w administracji publicznej oraz wprowadza obowiązek używania form elektronicznych przy realizacji zadań publicznych – takich jak składanie wniosków, komunikacja z petentami czy wydawanie decyzji administracyjnych. Istotne zmiany w procedurach administracyjnych przyniosła nowelizacja Kodeksu postępowania administracyjnego umożliwiająca prowadzenie postępowań w formie elektronicznej. Zgodnie z art. 63 § 1 KPA strona postępowania może wnieść podanie (wniosek, odwołanie itp.) w postaci elektronicznej opatrzonej podpisem zaufanym lub kwalifikowanym, co znacząco ułatwia obywatelom dostęp do postępowań i usług administracyjnych. Ponadto na mocy przepisów szczególnych powstały centralne platformy elektroniczne, takie jak ePUAP (Elektroniczna Platforma Usług Administracji Publicznej), umożliwiające załatwianie wielu spraw urzędowych online – od złożenia wniosku o dowód osobisty po uzyskanie odpisu aktu stanu cywilnego.

---

<sup>2</sup> Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. 1997 Nr 78, poz. 483 ze zm., art. 61.

<sup>3</sup> Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2024 poz. 1557.

## 1.2. Integracja z regulacjami unijnymi

Proces cyfryzacji administracji publicznej przebiega w ramach wyznaczonych przez prawo Unii Europejskiej, co wymaga harmonizacji przepisów krajowych z unijnymi. W obszarze usług elektronicznych kluczowe znaczenie ma rozporządzenie eIDAS – Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania – które ujednoliciło w państwach członkowskich zasady dotyczące podpisu elektronicznego, pieczęci cyfrowej, znaczników czasu czy identyfikacji elektronicznej<sup>4</sup>. W Polsce przepisy tego rozporządzenia zostały wdrożone przede wszystkim poprzez ustawę o usługach zaufania oraz identyfikacji elektronicznej z 5 września 2016 r.<sup>5</sup>, która określa m.in. funkcjonowanie krajowego węzła identyfikacji elektronicznej oraz status podpisu elektronicznego równoważnego podpisowi własnoręcznemu. Równie istotne było dostosowanie przepisów krajowych do ogólnego rozporządzenia o ochronie danych osobowych (RODO) – Rozporządzenia (UE) 2016/679, obowiązującego bezpośrednio od 2018 r.<sup>6</sup> W celu zapewnienia spójności polskiego porządku prawnego z RODO uchwalono ustawę z 10 maja 2018 r. o ochronie danych osobowych<sup>7</sup>, która określa krajowe mechanizmy egzekwowania zasad przetwarzania danych oraz powoływania organów nadzorczych. RODO wprowadziło do administracji publicznej surowe wymogi dotyczące ochrony danych – takie jak zasada minimalizacji zbieranych danych, ograniczenie celu przetwarzania czy prawo do ich usunięcia („prawo do bycia zapomnianym”) – co wymusiło istotne zmiany organizacyjne i techniczne w urzędach. Niespełnienie tych wymagań grozi nie tylko sankcjami finansowymi, ale i utratą zaufania obywateli do e-administracji.

Kolejnym ważnym obszarem jest bezpieczeństwo infrastruktury teleinformatycznej administracji. Unijna dyrektywa NIS2 z 2022 r., dotycząca bezpieczeństwa sieci i systemów informatycznych, zobowiązuje państwa członkowskie do zaostrzenia wymogów ochrony tzw. infrastruktury krytycznej<sup>8</sup>. W Polsce oznacza to konieczność nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz innych aktów wykonawczych, aby sprostać standardom NIS2. Już wcześniej obowiązywały przepisy ustanawiające minimalne wymagania techniczne – np. rozporządzenie w sprawie Krajowych Ram Interoperacyjności z 12 kwietnia 2012 r., które określa minimalne standardy dla systemów teleinformatycznych używanych w sektorze publicznym<sup>9</sup>. Takie akty prawne, wraz ze strategicznymi dokumentami państwowymi, wyznaczają architekturę rozwoju e-administracji. Warto również wspomnieć o dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/2102, która zobowiązała instytucje publiczne do zapewnienia dostępności swoich stron internetowych i aplikacji mobilnych

---

<sup>4</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. (eIDAS), Dz. U. UE L 257/73, 28.8.2014.

<sup>5</sup> Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz. U. 2016 poz. 1579.

<sup>6</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. (RODO), Dz. U. UE L 119/1, 4.5.2016.

<sup>7</sup> Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018 poz. 1000; t.j. Dz. U. 2019 poz. 1781.

<sup>8</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. (dyrektywa NIS2) (Dz. U. UE L 333/80, 27.12.2022).

<sup>9</sup> Rozporządzenie Ministra Cyfryzacji z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, Dz. U. 2017 poz. 2247.

dla osób niepełnosprawnych – w Polsce wdrożonej poprzez ustawę z 4 kwietnia 2019 r. o dostępności cyfrowej<sup>10</sup>.

## 2. Wyzwania cyfrowej administracji publicznej

Mimo wielu korzyści, jakie niesie za sobą informatyzacja urzędów, proces cyfryzacji administracji publicznej wiąże się z szeregiem wyzwań natury prawnej i społecznej. Najważniejsze z nich dotyczą zapewnienia równowagi między efektywnością działania administracji a poszanowaniem praw obywateli, w szczególności prawa do prywatności oraz równego dostępu do usług publicznych. Poniżej omówiono dwa kluczowe obszary problemowe: ochronę danych i bezpieczeństwo informacji oraz kwestię wykluczenia cyfrowego.

### 2.1. Ochrona danych osobowych i bezpieczeństwo informacji

Administracja publiczna gromadzi i przetwarza ogromne zasoby danych osobowych obywateli – od danych meldunkowych i podatkowych po informacje o stanie zdrowia czy sytuacji socjalnej. Zapewnienie należytej ochrony tych danych stanowi fundament zaufania obywateli do e-usług. Polskie regulacje prawne, w tym wspomniany art. 51 Konstytucji RP oraz przepisy RODO wraz z ustawą krajową o ochronie danych, ustanawiają rygorystyczne standardy przetwarzania informacji osobowych. Każdy system informatyczny w administracji powinien być projektowany zgodnie z zasadą „privacy by design”, tak aby już na etapie tworzenia uwzględniał zabezpieczenie danych i minimalizację ich zbierania. Organy publiczne są zobowiązane m.in. do wyznaczania inspektorów ochrony danych, okresowej analizy ryzyka i zgłaszania incydentów naruszenia bezpieczeństwa. Mimo to w praktyce wciąż dochodzi do poważnych naruszeń – w tym wycieków i kradzieży danych z rejestrów państwowych. Przykładowo, w 2020 r. media informowały o nieautoryzowanym dostępie do danych użytkowników platformy ePUAP, co podważyło zaufanie części obywateli do bezpieczeństwa usług online<sup>11</sup>.

Wraz z postępującą cyfryzacją rośnie także skala zagrożeń dla systemów administracyjnych. Z jednej strony coraz częstsze są zaawansowane ataki cybernetyczne (np. ransomware blokujący dostęp do baz danych czy phishing wyłudający dane logowania urzędników). Z drugiej strony, wiele urzędów nadal korzysta z przestarzałych systemów informatycznych, niespełniających współczesnych standardów zabezpieczeń. Braki techniczne potęguje czynnik ludzki – szacuje się, że znaczący odsetek incydentów bezpieczeństwa wynika z błędów pracowników, np. nieostrożnego obchodzenia się z hasłami czy otwierania zainfekowanych załączników e-mail<sup>12</sup>. Według raportów ENISA rok 2021 przyniósł rekordową liczbę incydentów cyberbezpieczeństwa w Europie, z czego wiele dotyczyło administracji publicznej<sup>13</sup>.

<sup>10</sup> Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz. U. 2019 poz. 848.

<sup>11</sup> Ibidem.

<sup>12</sup> Zob. P. Dunleavy, H. Margetts, S. Bastow, J. Tinkler, *Digital Era Governance: IT Corporations, the State and e-Government. Revised Edition*, Oxford University Press, Oxford 2006, s. 142–150.

<sup>13</sup> European Union Agency for Cybersecurity – ENISA. (2021), *Threat Landscape 2021*, [online: enisa.europa.eu].

W Polsce również odnotowano ataki na systemy rządowe i samorządowe, co uwiadamia potrzebę ciągłego wzmocnienia ochrony. Niezbędne są inwestycje w nowoczesne zabezpieczenia (szyfrowanie, systemy wykrywania włamań, kopie zapasowe) oraz – co równie ważne – szkolenia personelu z zakresu higieny cyfrowej i ochrony danych. Podnoszenie świadomości urzędników jest kluczowe, ponieważ nawet najlepsze procedury bezpieczeństwa zawiodą, jeśli nie będą przestrzegane w praktyce.

W kontekście ochrony danych osobowych niezwykle istotna jest transparentność działań administracji. Badania wskazują, że obywatele chętniej korzystają z e-usług, jeśli mają pewność, że ich dane są wykorzystywane w sposób przejrzysty i zgodny z prawem<sup>14</sup>. Administracja powinna więc jasno informować petentów, jakie dane są zbierane, w jakim celu oraz jakie środki bezpieczeństwa zostały wdrożone. Budowaniu zaufania służą także rozwiązania techniczne wspierające prywatność, np. anonimizacja danych obywateli przy udostępnianiu zbiorczych informacji statystycznych lub podczas testowania nowych rozwiązań. Podsumowując, zapewnienie bezpieczeństwa informacji i poszanowania prywatności obywateli jest warunkiem sine qua non sukcesu e-administracji. Wymaga to nie tylko przestrzegania litery prawa, ale i stałego doskonalenia środków technicznych oraz organizacyjnych. Konieczne jest wprowadzenie zasady ciągłego monitorowania zagrożeń i aktualizacji zabezpieczeń, a także kultury organizacyjnej kładącej nacisk na ochronę danych. Działania te muszą towarzyszyć rozwojowi usług cyfrowych, tak aby innowacyjność szła w parze z bezpieczeństwem.

## 2.2. Wykluczenie cyfrowe i dostępność usług

Kolejnym wyzwaniem w procesie cyfryzacji jest zapewnienie, że nowe rozwiązania są dostępne dla wszystkich obywateli, a transformacja nie pogłębia istniejących nierówności. Wykluczenie cyfrowe nadal dotyka istotnej części społeczeństwa – zwłaszcza osób starszych, mieszkańców obszarów wiejskich oraz osób o niższym statusie materialnym. Według danych Eurostatu ok. 17% Polaków w 2021 r. w ogóle nie korzystało z Internetu<sup>15</sup>, co oznacza, że dla znaczącej grupy obywateli usługi online są w praktyce niedostępne. Przyczyny takiego stanu rzeczy to zarówno braki infrastrukturalne (np. obszary pozbawione szybkiego łącza internetowego), jak i niedostateczny poziom kompetencji cyfrowych. Rządowe programy rozwoju sieci szerokopasmowych oraz szkolenia z obsługi komputera i Internetu są zatem niezbędnym uzupełnieniem działań legislacyjnych – bez infrastruktury i edukacji nawet najlepsze prawo o e-administracji pozostanie na papierze.

Istotny aspekt stanowi również dostępność cyfrowa dla osób ze szczególnymi potrzebami, w tym z niepełnosprawnościami. Publiczne serwisy internetowe i aplikacje powinny być projektowane zgodnie ze standardami dostępności (takimi jak WCAG 2.1), aby mogli z nich korzystać użytkownicy niewidomi (przy pomocy czytników ekranu), niesłyszący, mający ograniczenia motoryczne czy poznawcze. Niestety, wiele systemów administracyjnych wciąż nie spełnia tych wymogów – interfejsy są niedostosowane, brakuje napisów

<sup>14</sup> Por. F. Bannister, R. Connolly, *The effects of transparency on public sector performance*, GIQ 2014, nr 31(1), s. 108–110.

<sup>15</sup> Eurostat, *Digital economy and society statistics – households and individuals*, 2021, online: [ec.europa.eu/eurostat](https://ec.europa.eu/eurostat).

do materiałów wideo, a niektóre funkcje (np. podpis elektroniczny) bywają trudne do użycia dla osób z dysfunkcjami. Ustawa o dostępności cyfrowej z 2019 r. nałożyła na podmioty publiczne obowiązek zapewnienia określonego poziomu dostępności swoich stron i aplikacji, lecz praktyka wdrażania tych przepisów jest nierówna. Konieczny jest dalszy nadzór nad realizacją wymogów dostępności oraz wsparcie (finansowe i doradcze) dla jednostek administracji w dostosowaniu istniejących serwisów.

Aby przeciwdziałać wykluczeniu cyfrowemu, administracja publiczna musi prowadzić działania dwutorowo. Po pierwsze – zapewnić alternatywne formy dostępu do usług dla osób, które nie mogą lub nie potrafią skorzystać z kanałów elektronicznych. Oznacza to utrzymanie tradycyjnych punktów obsługi, infolinii, mobilnych placówek urzędowych czy też oferowanie pomocy asystenckiej przy wypełnianiu formularzy online. Po drugie – aktywnie promować i edukować w zakresie e-usług. Wielu obywateli nie korzysta z dostępnych rozwiązań cyfrowych z braku świadomości ich istnienia lub z obawy przed nową technologią. Kampanie informacyjne, szkolenia (np. organizowane w bibliotekach lub urzędach gmin) i inicjatywy typu „Latarnik Polski Cyfrowej” mogą stopniowo podnosić poziom kompetencji cyfrowych społeczeństwa. Doświadczenia innych krajów pokazują, że wzrost umiejętności korzystania z Internetu przekłada się na większą partycypację obywateli w e-administracji i życiu publicznym.

Podobnie jak w przypadku ochrony danych, tak i w sferze inkluzywności cyfrowej bardzo ważna jest trafna diagnoza problemów oraz długofalowa strategia. Administracja powinna monitorować poziom korzystania z usług cyfrowych przez różne grupy społeczne i identyfikować bariery (techniczne, edukacyjne, językowe itp.), a następnie podejmować środki zaradcze. Tylko w ten sposób uda się uniknąć sytuacji, w której cyfryzacja przynosi korzyści głównie tym obywatelom, którzy już wcześniej mieli łatwy dostęp do urzędów, podczas gdy grupy zmarginalizowane pozostaną na uboczu.

### 3. Nowe technologie w administracji publicznej

Rozwój innowacyjnych technologii informatycznych stwarza administracji publicznej zupełnie nowe możliwości świadczenia usług i usprawnienia swojej pracy. Sztuczna inteligencja, technologie big data, cloud computing czy blockchain mogą zrewolucjonizować sposób gromadzenia, przetwarzania i udostępniania informacji publicznej. Jednocześnie zastosowanie tych narzędzi rodzi wyzwania natury prawnej i etycznej – związane choćby z odpowiedzialnością za decyzje podejmowane przez algorytmy czy ochroną prywatności obywateli w dobie sieci blokowych. W literaturze podkreśla się, że skuteczne wykorzystanie nowych technologii w administracji wymaga nie tylko zmiany procedur, ale i ewolucji tradycyjnych instytucji prawa administracyjnego<sup>16</sup>.

---

<sup>16</sup> A. Kaczyńska, S. Kańduła, J. Przybylska, *Transformacja cyfrowa z punktu widzenia samorządu terytorialnego – wybrane zagadnienia*, „Nierówności Społeczne a Wzrost Gospodarczy” 2021, nr 65, DOI: <https://doi.org/10.15584/nsawg.2021.1.2>, s. 45–52.

### 3.1. Sztuczna inteligencja w administracji

Sztuczna inteligencja (AI) znajduje coraz szersze zastosowanie w sektorze publicznym na świecie – począwszy od analizy big data dla celów planistycznych, poprzez automatyzację rutynowych czynności urzędowych, aż po interakcję z obywatelami. W administracji polskiej trwają pilotażowe wdrożenia narzędzi AI, np. systemów klasy Robotic Process Automation do automatycznej weryfikacji składanych dokumentów czy generowania projektów decyzji administracyjnych. Doświadczenia pionierów cyfryzacji (jak Estonia) pokazują, że algorytmy mogą istotnie przyspieszyć realizację niektórych usług – estońskie e-urzędy korzystają z AI przy przyznawaniu świadczeń czy rejestracji działalności gospodarczej, co skraca czas obsługi obywatela z dni do minut<sup>17</sup>. Również komunikacja między urzędem a petentem może zostać usprawniona dzięki AI – coraz popularniejsze stają się wirtualni asystenci i chatboty, które potrafią udzielać odpowiedzi na najczęściej zadawane pytania, pomagać w nawigacji po serwisach administracji czy nawet przeprowadzać obywatela krok po kroku przez elektroniczny wniosek (przykładem może być portal gov.uk, gdzie chatboty wspomagają użytkowników w znalezieniu właściwych usług i procedur).

Korzyści z wykorzystania AI muszą jednak zostać zrównoważone odpowiednim otoczeniem prawnym, które zapobiegnie nadużyciom i zagwarantuje obywatelom ochronę ich praw. Obecnie brak jest szczegółowych regulacji ustawowych dotyczących zastosowania AI w administracji – trwają prace nad unijnym Aktem o sztucznej inteligencji, który wprowadzi klasyfikację systemów AI pod kątem ryzyka i obowiązki dla podmiotów je stosujących. Już teraz pojawiają się jednak istotne pytania. Jedno z najważniejszych dotyczy odpowiedzialności za decyzje podejmowane przez algorytmy: jeżeli system AI popełni błąd skutkujący naruszeniem praw obywatela (np. niesłuszne odmówienie świadczenia), to kto ma ponieść odpowiedzialność – organ wdrażający rozwiązanie, producent oprogramowania, a może sam algorytm? Tradycyjne prawo administracyjne opiera się na odpowiedzialności urzędnika lub urzędu, więc wprowadzenie zautomatyzowanych decyzji wymusza wypracowanie nowych mechanizmów nadzoru i przypisywania winy. Kolejnym problemem jest przejrzystość algorytmów. Wiele modeli AI (zwłaszcza opartych na sieciach neuronowych) działa jak „czarna skrzynka” – trudno zrozumieć logikę ich rozstrzygnięć nawet twórcom systemu. Taka sytuacja jest nie do pogodzenia z zasadą zaufania obywatela do państwa i z wymogiem uzasadniania decyzji administracyjnych. Jeśli AI wspiera lub zastępuje urzędnika, obywatel powinien mieć prawo wiedzieć, na jakiej podstawie podjęto rozstrzygnięcie. W literaturze wskazuje się ryzyko, że niekontrolowane algorytmy mogą prowadzić do decyzji nieobiektywnych lub dyskryminujących. Wymaga to wprowadzenia zasady algorytmicznej transparentności, czyli możliwości audytu zastosowanych modeli AI oraz ich wyników przez niezależne podmioty (np. sądy administracyjne lub organy ochrony danych).

Pomimo tych wyzwań potencjał sztucznej inteligencji w administracji jest ogromny. Odpowiednio zaprogramowane algorytmy mogą usprawnić analizy predykcyjne – np. prognozować zapotrzebowanie na usługi społeczne czy identyfikować obszary wymagające interwencji państwa. AI może także przyczynić się do lepszego wykrywania nadużyć (np. analizując wzorce w danych w celu wytypowania podejrzanych transakcji lub wyłudzeń

---

<sup>17</sup> M. Janssen, G. Kuk, C. Baltaci, *Digital government: Beyond modernization*, GIQ 2020, 37(3), art. 101477.

świadczeń). Warunkiem jest jednak zachowanie nad tymi narzędziami pełnej kontroli i zgodności z prawem. Polskie organy władzy powinny już teraz przygotowywać się do szerszej implementacji AI – zarówno poprzez udział w tworzeniu europejskich ram regulacyjnych, jak i budowanie krajowych kompetencji (specjalistyczne zespoły ds. AI w administracji, wytyczne etyczne, pilotaże z niezależną oceną skutków). W publikacjach podkreśla się, że administracja cyfrowa wymaga nowego podejścia, ale nie może odbywać się kosztem zasad państwa prawa.

### 3.2. Blockchain i decentralizacja danych

Drugą technologią, która budzi duże zainteresowanie w kontekście administracji publicznej, jest blockchain – rozproszony rejestr oparty na kryptografii, zapewniający niezmienną i weryfikowalność zapisów. W przeciwieństwie do tradycyjnych scentralizowanych baz danych blockchain nie ma jednego administratora – dane są przechowywane w sieci użytkowników, a każda zmiana wymaga konsensusu większości z nich. Takie rozwiązanie oferuje unikalne walory w zakresie transparentności i bezpieczeństwa procedur administracyjnych. Jednym z potencjalnych zastosowań jest prowadzenie rejestrów publicznych (np. ksiąg wieczystych, rejestrów gruntów, rejestru pojazdów) na blockchainie. Każdy wpis (np. transakcja sprzedaży nieruchomości) zapisany w łańcuchu bloków byłby trwale utrwalony i niemożliwy do zmiany lub usunięcia bez pozostawienia śladu, co zapobiega fałszerstwom i sprzyja budowaniu zaufania do rejestru. Przykładem takiego rozwiązania jest pilotażowy projekt przeprowadzony w Gruzji, gdzie wykorzystano blockchain do rejestracji praw własności nieruchomości – odnotowano skrócenie czasu potrzebnego na finalizację transakcji oraz wzrost pewności obrotu prawnego. Innym obszarem, w którym blockchain może pomóc, jest monitorowanie zamówień publicznych i zwalczanie korupcji. Gdyby każdy etap przetargu (ogłoszenie, oferty, wybór wykonawcy, realizacja umowy) był zapisywany w rozproszonym rejestrze dostępnym do wglądu publicznego, wzrosłaby przejrzystość procesu i utrudniono by dokonywanie niejawnych zmian czy manipulacji.

Koncepcja tzw. smart contracts (inteligentnych umów) – samowystępujących programów działających na blockchainie – mogłaby automatyzować realizację niektórych świadczeń administracji. Na przykład wypłata dotacji lub zasiłku mogłaby zostać zaprogramowana jako smart contract uruchamiający przelew po spełnieniu określonych warunków (np. dostarczeniu wymaganych dokumentów), co ograniczyłoby uznaniowość i opóźnienia. Ponadto technologia blockchain bywa proponowana jako rozwiązanie dla głosowania elektronicznego. Choć to zagadnienie budzi kontrowersje, zwolennicy wskazują, że blockchain może zapewnić równocześnie anonimowość oddanego głosu i pewność, że głosy nie zostały sfałszowane lub zmienione po oddaniu. W warunkach polskich trwa ostrożna dyskusja nad możliwością wprowadzenia e-głosowania w przyszłości, a ewentualne wdrożenie musiałoby być poprzedzone dokładnymi testami i gwarancjami bezpieczeństwa.

Pomimo obiecujących możliwości zastosowanie blockchain w administracji publicznej napotyka również poważne bariery. Jedną z nich jest zgodność z przepisami o ochronie danych osobowych. Wspomniana niezmienną danych w łańcuchu bloków stoi na pozór w sprzeczności z prawem do ich sprostowania lub usunięcia, gwarantowanym przez RODO. Jeśli dane osobowe obywatela zostaną zapisane na blockchainie, usunięcie ich (np. na żądanie obywatela lub z powodu upływu wymaganego okresu przechowywania) jest technicznie bardzo trudne – każdy blok jest powiązany kryptograficznie z poprzednim, więc proste wykasowanie informacji

naruszyłoby integralność całego rejestru. Proponuje się różne obejścia tego problemu, takie jak szyfrowanie danych osobowych (aby „usunięcie” polegało na zniszczeniu klucza deszyfrującego) albo przechowywanie w blockchainie jedynie skrótów kryptograficznych danych (hashy), podczas gdy właściwe dane znajdują się w tradycyjnej bazie. Tak czy inaczej przed szerszym wdrożeniem tej technologii prawodawca musi rozstrzygnąć, jak pogodzić jej właściwości z wymogami ochrony prywatności. Kolejna kwestia to standardy interoperacyjności i skalowalność. Obecnie istnieje wiele różnych platform blockchain (publicznych i prywatnych), a ich implementacja w administracji wymagałaby uzgodnienia wspólnych norm tak, by systemy różnych urzędów mogły się komunikować. Trzeba także brać pod uwagę wydajność – klasyczne łańcuchy bloków (jak np. Bitcoin) przetwarzają jedynie kilka transakcji na sekundę, co może być niewystarczające przy masowych usługach państwowych.

Należy wreszcie pamiętać, że technologia jest tylko narzędziem. Wprowadzenie nawet najbezpieczniejszych rozwiązań nie zagwarantuje sukcesu, jeśli nie będzie im towarzyszyć odpowiednie otoczenie prawne i organizacyjne. Przykładowo, przechowywanie aktów stanu cywilnego na blockchainie może zapewnić ich niezmienność, ale wciąż konieczne jest istnienie procedur korygowania ewentualnych błędów (np. literówek) zgodnie z przepisami prawa o aktach stanu cywilnego. Podobnie jawność blockchained może kolidować z prawnie chronioną tajemnicą (np. dane wrażliwe nie powinny być widoczne dla nieuprawnionych). Dlatego implementacja rozwiązań opartych na tej technologii musi być poprzedzona wnikliwą analizą prawną i pilotażami. Niemniej wielu ekspertów wskazuje, że blockchain – obok AI – może stać się jednym z filarów przyszłej e-administracji, zwiększającym jej wiarygodność i efektywność<sup>18</sup>.

#### 4. Cyfrowa partycypacja obywatelska i e-demokracja

Wykorzystanie narzędzi cyfrowych wpływa nie tylko na wewnętrzne funkcjonowanie administracji i jakość usług, ale także na relacje między państwem a obywatelami w kontekście demokratycznym. Mówiąc o cyfrowej partycypacji obywatelskiej, mamy na myśli angażowanie obywateli w procesy decyzyjne i życie publiczne za pomocą technologii – od konsultacji społecznych online, przez petycje składane drogą elektroniczną, po udział w głosowaniach czy budżetach obywatelskich za pomocą Internetu. Cyfryzacja administracji może stać się katalizatorem rozwoju e-demokracji, pod warunkiem że obywatele rzeczywiście skorzystają z nowych możliwości zabierania głosu.

##### 4.1. Transparentność i narzędzia e-demokracji

Jednym z fundamentów demokracji jest transparentność działania władzy oraz dostęp obywateli do informacji publicznej. W Polsce prawo to zostało wyniesione do rangi konstytucyjnej – art. 61 Konstytucji RP zapewnia każdemu obywatelowi dostęp do informacji o działalności

---

<sup>18</sup> R. Binns, *Fairness in machine learning: Lessons from political philosophy*, December 8, 2017. Conference on Fairness, Accountability, and Transparency, New York, Forthcoming, Proceedings of Machine Learning Research, Vol. 81, p. 1–11, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=3086546>, s. 150–155.

organów władzy publicznej. Cyfryzacja stwarza zupełnie nowe sposoby realizacji tej zasady. Dzięki portalom internetowym, platformom otwartych danych i transmisjom online z posiedzeń organów kolegialnych obywatele mogą na bieżąco śledzić działania rządu i samorządu, analizować wydatki publiczne czy zapoznawać się z projektami aktów prawnych. Przykładem dobrej praktyki jest Estonia, gdzie cały proces legislacyjny odbywa się w systemie elektronicznym e-Justice dostępnym publicznie – obywatele mogą sprawdzić aktualne brzmienie każdego procedowanego projektu ustawy, zgłoszone poprawki oraz stanowiska poszczególnych instytucji, co zapewnia niespotykaną wcześniej przejrzystość procesu prawotwórczego. W Polsce wdrożenie podobnego systemu (e-Doręczenia i e-Legisłacja) jest w toku i ma na celu usprawnienie konsultacji międzyresortowych i publicznych nad projektami aktów prawnych.

Cyfrowe kanały komunikacji ułatwiają też bieżący dialog obywateli z administracją. Coraz popularniejsze stają się elektroniczne konsultacje społeczne – projekty ustaw, uchwał lokalnych czy planów zagospodarowania przestrzennego są publikowane w Internecie wraz z formularzem, za pomocą którego każdy zainteresowany może zgłosić swoje uwagi. Dzięki temu osoby, które nie miałyby możliwości wzięcia udziału w tradycyjnym zebraniu czy wysłuchaniu publicznym, mogą wyrazić opinię z domu. Administracja zyskuje natomiast szansę dotarcia z konsultacjami do szerszego grona odbiorców, szczególnie młodszych pokoleń komunikujących się głównie online. Cyfrowe narzędzia partycypacyjne obejmują także platformy budżetu obywatelskiego (umożliwiające zgłaszanie i wybór lokalnych projektów finansowanych ze środków gminy), portale do składania petycji obywatelskich czy aplikacje służące zgłaszaniu problemów w przestrzeni publicznej (uszkodzona infrastruktura, dzikie wysypiska itp.).

Wszystkie te inicjatywy mają wspólny mianownik: wzmacniają wpływ obywateli na sprawy publiczne i wiążą się ze wzrostem odpowiedzialności organów za podejmowane decyzje. Administracja coraz częściej musi uzasadniać publicznie swoje działania i reagować na opinie wyrażane online. Jeżeli obywatele otrzymują narzędzia pozwalające włączyć się w proces rządzenia, władza staje się bardziej oddolnie kontrolowana. Możliwość śledzenia postępów załatwiania własnych spraw poprzez profile obywatela (np. informacja o etapie rozpatrywania wniosku paszportowego czy pozwolenia na budowę) zwiększa z kolei zaufanie do urzędu – petent widzi, że jego sprawa jest w toku, a system może go automatycznie powiadamiać o dokonanych czynnościach. Taka przejrzystość proceduralna również wynika pośrednio z konstytucyjnego prawa do informacji oraz z idei prawa do dobrej administracji.

#### 4.2. Bariery i przyszłość e-partycypacji

Mimo niewątpliwych zalet budowanie e-demokracji napotyka też istotne bariery. Pierwsza z nich to wspomniane wykluczenie cyfrowe – jeżeli znaczna część społeczeństwa nie ma możliwości lub umiejętności, by zabierać głos online, wówczas głosy obywateli zaangażowanych cyfrowo mogą nie odzwierciedlać poglądów ogółu. Badania pokazują, że uczestnikami e-konsultacji czy e-głosowań częściej są osoby młodsze i lepiej wykształcone, podczas gdy seniorzy czy mieszkańcy peryferyjnych regionów pozostają mniej aktywni<sup>19</sup>. Drugim problemem

---

<sup>19</sup> G. Faith, V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, Picador, St Martin's Press, New York 2018, "Law, Technology and Humans" 2019 1 (November):162-64. <https://doi.org/10.5204/lthj.v1i0.1386>.

jest niski poziom zaangażowania części obywateli. Nawet jeśli narzędzia są dostępne, wielu ludzi nie przejawia zainteresowania udziałem w dyskusjach publicznych. Przyczyny bywają różne: brak czasu, przekonanie o braku realnego wpływu na decyzje lub po prostu słaba promocja dostępnych mechanizmów. Samo stworzenie platformy partycypacyjnej nie gwarantuje, że obywatele tłumnie z niej skorzystają – potrzebna jest kultura obywatelskiego uczestnictwa, którą buduje się latami poprzez edukację i sukcesywne zachęcanie do współdecydowania (np. poprzez pokazywanie realnych efektów zgłoszonych postulatów).

Kolejnym wyzwaniem w cyfrowej przestrzeni debaty publicznej jest dezinformacja i manipulacja. Internet niestety ułatwia rozpowszechnianie nieprawdziwych lub zmanipulowanych informacji, które mogą wpływać na opinie społeczne i decyzje obywateli. W skrajnych przypadkach zorganizowane kampanie dezinformacyjne mogą próbować wypaczyć wynik konsultacji czy głosowania, wykorzystując fałszywe profile, boty, masowe szerzenie plotek itp. Administracja musi być świadoma tego zagrożenia – stąd m.in. wymogi weryfikacji tożsamości przy głosowaniach online albo moderacja forów konsultacyjnych (usuwanie wpisów obraźliwych, ewidentnie nieprawdziwych). Zapewnienie wiarygodności procesów e-partycypacji jest kluczowe dla utrzymania zaufania do nich.

Patrząc w przyszłość, można stwierdzić, że cyfryzacja administracji publicznej ma potencjał, by znacząco wzmocnić demokrację, pod warunkiem przezwyciężenia wymienionych barier. Kluczowe znaczenie będzie mieć edukacja – już w szkołach warto kształtować postawy aktywnego obywatelstwa i uczyć, jak mądrze korzystać z narzędzi e-demokracji. Równoległe administracja powinna inwestować w tworzenie bardziej przyjaznych i interaktywnych platform angażowania obywateli. Przykładowo, konsultacje mogłyby być wzbogacane przez inteligentne chatboty wyjaśniające w przystępny sposób skomplikowane zagadnienia projektu ustawy, tak aby więcej osób mogło świadomie zabrać głos. Ponadto niezbędne jest zapewnienie bezpieczeństwa procesów demokratycznych online – tu znów może pomóc blockchain, gwarantując integralność ewentualnych głosowań internetowych czy archiwów dokumentów udostępnianych obywatelom.

Cyfrowa partycypacja obywatelska stanowi ważny element nowoczesnego modelu administracji określanego niekiedy mianem governance 2.0. Oznacza on odejście od jednostronnej komunikacji „władza–obywatel” na rzecz modelu wielokierunkowego, w którym obywatele są partnerami współdecydującymi o sprawach publicznych. Już teraz widać, że tam, gdzie zastosowano narzędzia e-partycypacji, wzrosła frekwencja w konsultacjach oraz liczba pomysłów zgłaszanych przez mieszkańców do realizacji (np. w ramach budżetu obywatelskiego). To pozytywny trend, który należy wzmacniać. W miarę jak kolejne pokolenia – wychowane w środowisku cyfrowym – wchodzi w rolę uczestników życia publicznego, oczekiwanie możliwości załatwienia każdej sprawy i wyrażenia opinii drogą elektroniczną staje się normą. Rolą administracji jest wyjść naprzeciw tym oczekiwaniom, pamiętając jednak o zapewnieniu, by żaden obywatel nie został pozostawiony w tyle.

## **Zakończenie**

Cyfryzacja administracji publicznej w Polsce jest procesem złożonym i długofalowym, który wymaga równoczesnych działań na wielu płaszczyznach. Z jednej strony konieczna jest modernizacja infrastruktury oraz wdrażanie nowoczesnych systemów informatycznych, z drugiej – stałe dostosowywanie prawa do zmieniającej się rzeczywistości cyfrowej, a także budowanie społecznej akceptacji i zaufania do nowych rozwiązań. Przeprowadzona analiza

prowadzi do kilku kluczowych wniosków. Po pierwsze, fundamentem cyfryzacji muszą pozostać gwarancje konstytucyjne – prawo obywateli do informacji publicznej oraz prawo do prywatności i ochrony danych osobowych. Wdrażając e-usługi, organy władzy powinny każdorazowo weryfikować ich zgodność z art. 61 i 51 Konstytucji RP oraz ustawami takimi jak o dostępie do informacji publicznej, o ochronie danych osobowych czy o informatyzacji działalności podmiotów publicznych. Po drugie, niezbędne jest utrzymanie równowagi między efektywnością a inkluzywnością – cyfrowe usługi muszą być dostępne dla wszystkich, niezależnie od kompetencji czy sytuacji użytkownika, a jednocześnie zapewniać szybkie i wygodne załatwianie spraw. Po trzecie, nowe technologie powinny być wprowadzane rozsądnie, z poszanowaniem zasad państwa prawa: automatyzacja procesów nie może odbierać obywatelom prawa do rzetelnego procesu i kontroli decyzji, a decentralizacja danych musi iść w parze z ochroną prywatności.

Mając na uwadze powyższe, można wskazać kilka rekomendacji, których wdrożenie przyczyni się do skuteczniejszej i bardziej przyjaznej obywatelom cyfryzacji administracji:

- **Zharmonizowanie procedur e-dostępności.** Należy opracować i wdrożyć jednolite standardy świadczenia usług administracyjnych dostosowanych do potrzeb osób z niepełnosprawnościami oraz mieszkańców obszarów zagrożonych wykluczeniem cyfrowym (np. zapewnienie wsparcia asystenckiego, mobilnych punktów obsługi, uproszczonych interfejsów użytkownika).
- **Podniesienie kompetencji urzędników.** Wprowadzić obowiązkowe szkolenia z zakresu cyberbezpieczeństwa, ochrony danych osobowych oraz obsługi nowych systemów teleinformatycznych dla pracowników administracji publicznej na wszystkich szczeblach. Pozwoli to ograniczyć ryzyko błędów ludzkich i incydentów bezpieczeństwa oraz zwiększyć efektywność wykorzystania e-narzędzi.
- **Jasne zasady odpowiedzialności algorytmicznej.** Ustanowić w przepisach transparentne reguły odpowiedzialności za decyzje administracyjne podejmowane przy udziale systemów AI. Doprecyzować, że obywatel ma prawo do uzyskania uzasadnienia takiej decyzji oraz do odwołania rozpatrzonego przez człowieka. Rozważyć stworzenie mechanizmu certyfikacji algorytmów używanych w sektorze publicznym pod kątem zgodności z prawem i zasadami etyki.
- **Nadzór konstytucyjny nad informatyzacją.** Powołać (lub wzmocnić istniejące) organy monitorujące proces informatyzacji administracji z punktu widzenia ochrony praw obywatelskich (np. komisję ds. społeczeństwa informacyjnego przy Rzeczniku Praw Obywatelskich). Mechanizmy kontroli powinny obejmować audyt działania kluczowych systemów (profil zaufany, rejestry publiczne itp.) oraz ocenę wpływu wdrażanych technologii na prawa podstawowe.
- **Wspieranie cyfrowej partycypacji.** Rozwijać i promować narzędzia e-demokracji, dbając o ich bezpieczeństwo i dostępność. Wprowadzać platformy konsultacji online, głosowań obywatelskich czy zgłaszania inicjatyw z wykorzystaniem zabezpieczonych technologii (takich jak uwierzytelnianie przez eID i rozwiązania blockchain zapewniające integralność głosów). Równolegle prowadzić kampanie informacyjne zachęcające obywateli do korzystania z tych form uczestnictwa w życiu publicznym.

Realizacja powyższych postulatów wymaga współpracy ustawodawcy, administracji wykonawczej oraz społeczeństwa obywatelskiego. Cyfryzacja nie jest celem samym w sobie, lecz narzędziem do budowy sprawniejszego, bardziej przejrzystego i przyjaznego państwa. Odpowiedzialne wykorzystanie technologii – przy jednoczesnym poszanowaniu

zasad demokratycznego państwa prawnego – może przynieść trwałe korzyści zarówno obywatelom, jak i samej administracji, czyniąc ją bardziej wydajną i odporną na wyzwania XXI wieku.

## Bibliografia

- Bannister F. & Connolly, R., *The effects of transparency on public sector performance*, „Government Information Quarterly” 2014, nr 31(1), s. 101–110.
- Binns R., *Fairness in machine learning: Lessons from political philosophy* [w:] *Proceedings of the 1st Conference on Fairness, „Accountability and Transparency”* 2018, Vol. 81, s. 149–159.
- Dunleavy P., Margetts, H., Bastow, S. & Tinkler, J., *Digital era governance: IT corporations, the state, and e-government*, Oxford University Press 2006.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (dyrektywa NIS2). Dz. U. UE L 333/80, 27.12.2022.
- European Union Agency for Cybersecurity, ENISA Threat Landscape 2021, <https://www.enisa.europa.eu>, dostęp: 5 sierpnia 2025 r.
- Eurostat, *Digital economy and society statistics – households and individuals*, 2021, Pobrano, <https://ec.europa.eu/eurostat>, dostęp: 5 sierpnia 2025 r.
- Faith G., V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, Picador, St Martin's Press, New York 2018, „Law, Technology and Humans” 2019 1 (November):162-64. <https://doi.org/10.5204/lthj.v1i0.1386>.
- Górka S., *Nowoczesne technologie w administracji publicznej*, Wydawnictwo Wolters Kluwer, 2022 s. 88–95.
- Janssen M., Kuk, G. & Baltaci, C., *Digital government: Beyond modernization*, „Government Information Quarterly” 2020, 37(3), art. 101477.
- Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. Dz. U. 1997 Nr 78, poz. 483 z późn. zm.
- Korczak J., *E-administracja i prawo administracyjne*, 2021, (s. 45–52).
- Ministerstwo Cyfryzacji, Elektroniczna Platforma Usług Administracji Publicznej (ePUAP) – komunikat, 3 czerwca 2020 r., <https://www.gov.pl>, dostęp: 5 sierpnia 2025 r.
- Rozporządzenie Ministra Cyfryzacji z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, Dz. U. 2017 poz. 2247.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych ... (RODO). Dz. U. UE L 119/1, 04.05.2016.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania ... (eIDAS). Dz. U. UE L 257/73, 28.08.2014.
- Tapscott, D. & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Portfolio.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018 poz. 1000, t.j. Dz. U. 2019 poz. 1781.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, tekst jedn.: 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.

Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz. U. 2016 poz. 1579.

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. 2022 poz. 902.

## SUMMARY

Łukasz Dudarski

### **Digitalization of public administration in Poland: challenges and prospects**

This article provides a concise overview of the legal foundations and European framework for the digitalization of Polish administration, highlighting the need for compliance with eIDAS, GDPR, and NIS2. It identifies three main challenges: data security, cyber-threats, and digital exclusion. The authors emphasize the potential of AI, blockchain, and e-democracy tools, while also emphasizing the need for algorithm transparency and inclusive service design. The conclusion includes recommendations: training of officials, certification of algorithms, uniform accessibility standards, and maintaining alternative channels for serving citizens.

**Key words:** digitalization of public administration, e-government, personal data protection, cybersecurity, digital exclusion, digital accessibility, artificial intelligence, blockchain, civic e-participation, administrative law.

Data wpływu artykułu: 16.01.2025

Data akceptacji artykułu: 8.07.2025