Anna Gałasiewicz

„Podmiotowość jednostki w cyfrowym państwie. Prawne standardy przejrzystości systemów AI jako gwarancja praw obywatelskich”

1. CYFROWA PODMIOTOWOŚĆ JEDNOSTKI

Fundamentem współczesnych porządków normatywnych, osadzonych w tradycji demokratycznego państwa prawnego, jest podmiotowość jednostki, wywiedziona z niezbywalnej godności ludzkiej. Podmiotowość ta konstytuuje imperatyw kategoryczny, zgodnie z którym człowiek winien być traktowany jako cel sam w sobie, a nie instrumentalnie jako środek do realizacji określonych postulatów. W dobie paradygmatu cyfrowej transformacji sfery publicznej, tak ukształtowana koncepcja podlega procesom redefinicji i zostaje wystawiona na istotną próbę. Postępująca algorytmizacja procesów decyzyjnych w administracji publicznej niesie ze sobą ryzyko depersonalizacji. Zjawisko to objawia się tendencją do postrzegania indywiduum jako „obiektu danych”, zapominając o jego unikalnej tożsamości. Widoczne stają się napięcia na linii godność-efektywność, gdzie techniczna optymalizacja procedur może stać się barierą dla pełnej realizacji praw obywatela.

Realia społeczeństwa medialnego, opartego na wszechobecności rozwiązań cyfrowych, wymagają nadania aktywności obywatelskiej nowego, informacyjno-komunikacyjnego charakteru. Proces mediatyzacji sprawia, że media i algorytmy przestają być jedynie narzędziami, a stają się pośrednikiem w kształtowaniu obrazu rzeczywistości oraz niemal każdej sfery ludzkiej aktywności. Prawo do zachowania kontroli nad informacją o sobie samym staje się fundamentem ochrony godności obywatela w relacji z cyfrowym państwem[1].

Algorytmy uczenia maszynowego coraz częściej wspierają sektor publiczny, przyjmując postać systemów autonomicznych bądź narzędzi wspomagających decyzje urzędnika. Choć algorytm w swojej istocie jest precyzyjnym ciągiem operacji mających na celu rozwiązanie problemu, to proces jego uczenia i testowania, oparty na masowym przetwarzaniu danych, budzi istotne wątpliwości natury etycznej i prawnej. Granica między usprawnieniem administracji a systemem kontroli społecznej staje się cienka, czego ekstremalnym przykładem jest model chiński (*Social Credit System* - system zaufania społecznego). Uczenie maszynowe, bazujące na całkowitym wglądzie w aktywność jednostki, może stać się narzędziem naruszającym podstawowe wolności w obszarze informacyjnym[2].

[1] K. Ciesiołkiewicz, *Podmiotowość informacyjno-komunikacyjna w środowisku mediów cyfrowych jako cel edukacji*, „Forum Pedagogiczne” 2025, t. 15, nr 1, s. 124, DOI: 10.21697/fp.2025.1.11.
[2] M. Sakowska-Baryła, *Sztuczna inteligencja w sektorze publicznym* [w:] *Prawo sztucznej inteligencji i nowych technologii 3*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2023, s.34-35.

Choć definicje sztucznej inteligencji różnią się w zależności od dyscypliny nauki, na użytek dyskusji prawniczej wystarczające jest rozumienie jej jako zdolności maszyn do imitowania ludzkiej inteligencji poprzez zaimplementowane oprogramowanie[3]. Cechą tych systemów jest naśladowanie ludzkiej percepcji oraz zdolność do stałego rozwoju w oparciu o nowe dane. Programy te nieustannie ewoluują, co sprawia, że w sektorze publicznym mogą one generować rozstrzygnięcia trudne do przewidzenia nawet dla ich twórców[4]. Niesie to ze sobą bezpośrednie niebezpieczeństwo cyfrowej alienacji. Stan ten przejawia się nie tylko w sferze teoretycznej, ale przede wszystkim w codziennej relacji z państwem. Poczucie alienacji potęguje fakt, że cyfrowe zarządzanie często redukuje obywatela do „obiektywnych" danych statystycznych. Prowadzi to do dysfunkcji infrastruktury, w której jednostka, pozostawiona bez rzetelnej informacji, jest zmuszona radzić sobie na własną rękę, by zminimalizować skutki systemowej niewydolności[5]. Konieczność „omijania" nieefektywnych mechanizmów władzy pogłębia podziały społeczne. Obywatel, choć technicznie połączony z siecią, staje się wyobcowany wobec nieprzejrzystych dla niego algorytmów. Gwarancja sprawstwa w dobie AI musi być zatem rozumiana jako prawo do bycia „wysłuchanym" przez system, co wymaga pełnej transparentności procedur. Przejrzystość systemów sztucznej inteligencji nie jest więc jedynie postulatem; staje się warunkiem koniecznym do zachowania kontroli nad własnym losem. Tylko systemy zrozumiałe i otwarte na weryfikację mogą zapobiec redukcji obywatela do roli statystycznego obiektu.

2. STANDARDY INFORMACYJNE SYSTEMÓW WYSOKIEGO RYZYKA

Odpowiedzią na zagrożenia związane z cyfrową alienacją jest wprowadzenie standardów przejrzystości w ramach unijnego rozporządzenia w sprawie sztucznej inteligencji (AI Act)[6]. Akt ten opiera się na analizie ryzyka. Z punktu widzenia obywatela najważniejszą kategorię stanowią systemy wysokiego ryzyka, wykorzystywane w sektorze publicznym. Znajdują one zastosowanie przy przyznawaniu świadczeń, zarządzaniu infrastrukturą czy w obszarze wymiaru sprawiedliwości.

Zgodnie z art. 6 ust. 1 AI Act, pierwszą grupę stanowią systemy będące elementami bezpieczeństwa produktów, co wymaga zdefiniowania „związanego z bezpieczeństwem elementu". Zgodnie z terminologią przyjętą w rozporządzeniu, pojęcie to odnosi się do komponentu, który pełni funkcje ochronne w ramach danego systemu lub którego ewentualna dysfunkcja mogłaby bezpośrednio

[3] D. Flisak, *Sztuczna inteligencja - jak chronić prawa autorskie twórczości robotów*, „Rzeczpospolita" (22.05.2017), http://www.rp.pl/Opinie/305229984-Sztuczna-inteligencja--jak-chronic-prawa-autorskie-tworczosci-robotow.html (dostęp: 17.03.2026).
[4] P.P. Juściński, *Prawo autorskie w obliczu rozwoju sztucznej inteligencji*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Intelektualnego" 2019, nr 1, s. 6-7.
[5] E. Bendyk, *Metropolia w sieci*, „Samorząd Terytorialny" 2010, nr 6, s. 58.
[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).

zagrażać życiu, zdrowiu bądź mieniu. Ten warunek materializuje się m.in. w pojazdach autonomicznych (algorytmy hamowania awaryjnego) oraz w sektorze medycznym. Przykładem o szczególnym znaczeniu są algorytmy sterujące urządzeniami do radioterapii, które muszą gwarantować precyzyjne dawkowanie promieniowania; każda dewiacja od założonej normy - zarówno niedoszacowanie, jak i przekroczenie dawki niesie ze sobą drastyczne skutki dla zdrowia pacjenta[7].

Z perspektywy relacji z państwem, istotniejsza jest jednak druga kategoria, zdefiniowana w art. 6 ust. 2, która odsyła do katalogu obszarów wrażliwych wymienionych w Załączniku III. Obejmuje on systemy AI bezpośrednio wpływające na trajektorię życiową obywatela, w tym narzędzia wykorzystywane w edukacji i usługach publicznych. Należy jednak podkreślić, że klasyfikacja ta nie ma charakteru absolutnego - art. 6 ust. 3 wprowadza odstępstwo dla zadań czysto proceduralnych, jednak wyjątek ten ulega wyłączeniu w sytuacji, gdy system dokonuje profilowania osób fizycznych. W takim przypadku, ze względu na stopień ingerencji w autonomię, system zawsze kwalifikowany jest jako rozwiązanie wysokiego ryzyka.

Włączenie powyższych rozwiązań do kategorii wysokiego ryzyka uzasadnia konieczność stosowania standardów z art. 13 i 14 AI Act. Skoro błąd maszyny może mieć charakter nieodwracalny, przejrzystość jej logiki staje się nadrzędnym wymogiem prawnym. Fundamentem ochrony niezależności decyzyjnej jest art. 13 AI Act, który nakłada na dostawców obowiązek projektowania systemów w taki sposób, aby ich działanie było „wystarczająco przejrzyste" dla użytkownika i obywatela. W doktrynie wskazuje się, że wymóg ten nie powinien być interpretowany jednowymiarowo. Można go rozpatrywać na trzech kluczowych płaszczyznach: konstrukcyjnej (powiązanie algorytmów), procesowej (sposób generowania wyników) oraz interpretacyjnej (zrozumiałość wyniku). Dzięki temu można precyzyjnie rozgraniczyć obowiązki dostawcy systemu od kompetencji podmiotu stosującego technologię w administracji publicznej[8].

Głównym filarem w tym obszarze jest obowiązek informacyjny w systemach wchodzących w bezpośrednią interakcję z osobami fizycznymi. Użytkownik musi zostać wyraźnie powiadomiony, że komunikuje się z chatbotem[9], co stanowi istotne dopełnienie standardów przejrzystości przewidzianych również w akcie o usługach cyfrowych. Ma to na celu zapobieganie manipulacji, co gwarantuje prawo do świadomego wyboru formy komunikacji.

Równie istotne znaczenie dla przejrzystości przestrzeni cyfrowej ma obowiązek znakowania treści syntetycznych (obrazów, dźwięków czy wideo) w formacie nadającym się do odczytu maszynowego. Regulacja ta staje się niezbędna w obliczu dynamicznego rozwoju technologii typu *deepfake*, które mogą wprowadzać odbiorców w błąd co do autentyczności przekazu. Wprowadzenie wymogu ujawniania sztucznego pochodzenia materiałów, które mogą sprawiać wrażenie prawdziwych,

---

[7] W. Rzepiński [w:] *AI Act. Akt w sprawie sztucznej inteligencji. Komentarz*, red. M. Jędrzejczak, Ł. Szoszkiewicz, J. Wydra, Warszawa 2025, str. 222-223.
[8] J. Wydra [w:] *AI Act. Akt w sprawie sztucznej inteligencji. Komentarz*, red. M. Jędrzejczak, Ł. Szoszkiewicz, J. Wydra, Warszawa 2025, str. 263-268.
[9] M. Gumularz (red.), *Akt o usługach cyfrowych. Komentarz,* Warszawa 2024, s. 308.

służy nie tylko ochronie rynku dóbr kultury, ale przede wszystkim zapewnia bezpieczeństwo obrotu informacyjnego. Pozwala to na „uświadomioną konsumpcję" treści, co w dobie dezinformacji stanowi ważny element ochrony podmiotowości jednostki w środowisku cyfrowym[10].

3. PRAWO DO WYJAŚNIENIA

Ewolucja standardów ochrony w relacji z systemami algorytmicznymi opiera się na fundamencie praw gwarancyjnych i kontrolnych, które są zawarte m.in. w art. 15 RODO.
W doktrynie podkreśla się, że przyznane na gruncie tego przepisu uprawnienia informacyjne mają charakter bezwarunkowy, gdyż ich realizacja nie wymaga wykazania interesu prawnego ani faktycznego, a ich głównym celem jest umożliwienie użytkownikom weryfikacji zgodności przetwarzania danych z prawem[11]. Kluczowym aspektem tego uprawnienia, stanowiącym bezpośredni pomost do regulacji AI Act, jest prawo do uzyskania informacji o zasadach zautomatyzowanego podejmowania decyzji, w tym o znaczeniu i przewidywanych konsekwencjach procesu dla osoby, której dane dotyczą. Jak zauważa J. Denka, pojęcia „decyzji" na gruncie art. 86 AI Act nie należy utożsamiać wyłącznie z aktem administracyjnym w rozumieniu krajowego prawa procesowego. Termin ten ma samoistny status i obejmuje szeroki wachlarz rozstrzygnięć podejmowanych zarówno przez organy publiczne, jak i podmioty prywatne (np. w procesie oceny zdolności kredytowej czy rekrutacji), o ile sprawują one kontrolę nad systemem AI. Co istotne, prawo to przysługuje nie tylko w przypadku wystąpienia bezpośrednich skutków prawnych, ale również wtedy, gdy decyzja oddziałuje na zdrowie, bezpieczeństwo lub prawa podstawowe zapisane w Karcie Praw Podstawowych[12].

Suwerenność decyzyjna wymaga, aby wyjaśnienie nie było jedynie zbiorem parametrów statystycznych, lecz logicznym uzasadnieniem, które pozwoli laikowi zrozumieć związek przyczynowo-skutkowy między jego sytuacją faktyczną a wynikiem wygenerowanym przez system. Obywatel musi wiedzieć, które z jego cech lub zachowań zaważyły na negatywnym rozstrzygnięciu, by móc zweryfikować, czy system nie oparł się na nieprawdziwych lub dyskryminujących danych.

Wymóg, aby wyjaśnienie było „jasne i merytoryczne", nakłada obowiązek wykroczenia poza ogólną informację techniczną. Wyjaśnienie musi dawać realną podstawę do skorzystania z praw, co oznacza konieczność przedstawienia roli systemu AI w procedurze oraz wskazania głównych elementów, które zaważyły na końcowym wyniku. Bez transparentności prawo do skutecznej ochrony sądowej stałoby się iluzoryczne.

---

[10] D. Flisak, *Akt w sprawie sztucznej inteligencji*, komentarz praktyczny, wersja elektroniczna LEX (dostęp: 17.03.2026).
[11] J. Łuczak [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 507-516.
[12] J. Denka [w:] *AI Act. Akt w sprawie sztucznej inteligencji. Komentarz*, red. M. Jędrzejczak, Ł. Szoszkiewicz, J. Wydra, Warszawa 2025, s. 625-630.

4. MECHANIZMY NADZORU NAD AUTOMATYZACJĄ

Fundamentem bezpieczeństwa jednostki w relacji z algorytmiczną administracją jest zasada nadzoru ludzkiego, realizowana w modelu *human-in-the-loop (*człowiek w pętli)[13]. Zgodnie z założeniami art. 14 AI Act, system sztucznej inteligencji wysokiego ryzyka musi być projektowany tak, aby nie uniemożliwiać osobie fizycznej sprawowania nad nim rzeczywistej kontroli. W doktrynie wskazuje się, że nadzór ten nie może być jedynie „symbolicznym gestem", lecz musi być sprawowany przez osobę posiadającą realne uprawnienia do zmiany lub uchylenia decyzji wygenerowanej przez algorytm. Takie ujęcie zbliża regulację AI Act do standardów wyznaczonych przez art. 22 RODO, kładąc nacisk na podmiotową rolę człowieka w procesie decyzyjnym[14].

Istotną gwarancją tej kontroli jest przeciwdziałanie zjawisku błędu automatyzacji (*automation bias*). Polega ono na psychologicznej skłonności ludzi do bezkrytycznego ufania sugestiom maszyny, nawet jeśli są one sprzeczne z ich własną wiedzą lub intuicją. Aby nadzór był realny, urzędnik musi być wyposażony w narzędzia pozwalające na krytyczną ocenę wyników AI. W sferze praktycznej art. 14 ust. 4 AI Act wyposaża osobę sprawującą nadzór w konkretne kompetencje: prawo do ignorowania, unieważnienia lub odwrócenia wyniku, jeśli uzna go za niesprawiedliwy lub nieuwzględniający indywidualnych okoliczności sprawy. Istotnym bezpiecznikiem jest również wymóg zapewnienia możliwości przerwania pracy systemu w dowolnym momencie (tzw. *stop button*).

W sytuacjach o szczególnym znaczeniu dla wolności obywatelskich, takich jak zdalna identyfikacja biometryczna, ustawodawca wprowadza jeszcze bardziej rygorystyczne środki - konieczność odrębnej weryfikacji wyniku przez co najmniej dwie wykwalifikowane osoby fizyczne. Nadzór ludzki gwarantuje, że za każdą decyzją stoi konkretny funkcjonariusz lub organ. Możliwość personalizacji odpowiedzialności jest warunkiem koniecznym do realizacji prawa do sądu i naprawienia ewentualnej szkody, co chroni przed poczuciem bezradności wobec „anonimowej" digitalizacji.

Zabezpieczenie interesów osób fizycznych w starciu z systemami AI nie ma charakteru incydentalnego, lecz musi stanowić proces ciągły, obejmujący cały cykl życia wsparcia systemowego. Uzupełnieniem bezpośredniego nadzoru ludzkiego jest mechanizm monitorowania systemu po wprowadzeniu do obrotu (*post-market monitoring*), statuowany w art. 72 AI Act. Przepis ten nakłada na dostawców obowiązek aktywnego i systematycznego zbierania oraz analizowania danych dotyczących skuteczności działania algorytmów wysokiego ryzyka. Jak wskazuje J. Jakubowicz, celem tej regulacji jest zapewnienie permanentnej zgodności systemu z wymogami bezpieczeństwa i praw podstawowych, co ma istotne znaczenie w przypadku innowacji, które „uczą się" i ewoluują już po ich wdrożeniu do administracji publicznej[15]. Ta funkcja wczesnego ostrzegania umożliwia szybkie podjęcie działań

[13] C.O. Retzlaff i in., *Human-in-the-Loop Reinforcement Learning: A Survey and Position on Requirements, Challenges, and Opportunities*, „Journal of Artificial Intelligence Research" 2024, t. 79, s. 360-365.
[14] W. Rzepiński [w:] *AI Act. Akt w sprawie sztucznej inteligencji*. Komentarz, red. M. Jędrzejczak, Ł. Szoszkiewicz, J. Wydra, Warszawa 2025, s. 270-275.
[15] J. Jakubowicz [w:] *AI Act. Akt w sprawie sztucznej inteligencji. Komentarz*, red. M. Jędrzejczak, Ł. Szoszkiewicz, J. Wydra, Warszawa 2025, s. 570-574.

naprawczych w sytuacji, gdy system zacznie generować wyniki odbiegające od ustalonych wcześniej założeń. Istotnym elementem tego procesu jest identyfikowalność, czyli możliwość jednoznacznego przypisania wyników działania AI konkretnemu podmiotowi, co stanowi warunek konieczny do pociągnięcia go do odpowiedzialności prawnej. Wprowadzenie obowiązku dokumentowania i raportowania anomalii sprawia, że państwo nie pozostaje biernym użytkownikiem cyfrowych rozwiązań, lecz posiada instrumenty do ich stałej ewaluacji.

5. PODSUMOWANIE

Wnioski płynące z analizy Aktu w sprawie sztucznej inteligencji wskazują, że mamy do czynienia z historycznym zwrotem w podejściu do podmiotowości prawa. Sztuczna inteligencja jako przedmiot prawa charakteryzuje się unikalnymi cechami, takimi jak rosnąca autonomia, nieprzejrzystość oraz tzw. efekt „czarnej skrzynki". Te specyficzne właściwości prowadzą do naruszenia klasycznych konstrukcji prawnych - niezależność działań AI może bowiem skutkować zerwaniem związku przyczynowego między deweloperem a końcowym działaniem produktu, co sprawia, że określenie jednoznacznej odpowiedzialności za błąd staje się niezwykle trudne[16].

W obliczu tych wyzwań, unijny ustawodawca przyjął podejście regulacyjne oparte na wartościach, definiując fundamenty tzw. „godnej zaufania AI". Według założeń AI Act, dobrze zaprojektowany system musi opierać się na sześciu filarach: nadzorze ludzkim szanującym autonomię człowieka, technicznej wytrzymałości minimalizującej szkody, rygorystycznym zarządzaniu danymi i prywatnością, przejrzystości umożliwiającej śledzenie procesów decyzyjnych, a także na sprawiedliwości i wrażliwości na dobro społeczne[17]. Dzięki temu regulacje stanowią niezbędną odpowiedź na złożoność algorytmów, a sztuczna inteligencja staje się narzędziem, za którego skutki ostateczną odpowiedzialność zawsze ponosi człowiek.

W ramach postulatów *de lege ferenda* należy zaproponować tworzenie ustandaryzowanych „kart informacyjnych algorytmów". Karty te, wzorowane na unijnych wymogach przejrzystości, powinny być formułowane prostym językiem, dostępnym dla przeciętnego obywatela. Dokumenty powinny w sposób klarowny wyjaśniać, jakie dane są przetwarzane oraz jakie są ograniczenia danego systemu. Prezentacja praw i obowiązków pozwoli na realną kontrolę swoich interesów i skuteczne korzystanie z prawa do wyjaśnienia.

Konkludując, proces cyfryzacji państwa nie może prowadzić do uprzedmiotowienia obywatela. Cyfrowe państwo musi zachować swój służebny charakter, a nie stać się samosterownym systemem algorytmów. Technologia, mimo rosnącej niezależności operacyjnej i złożoności, powinna być

[16] P. Dolniak i in., *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*, Warszawa 2024, s. 115.
[17] P. Dolniak i in., *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*, Warszawa 2024, s.126-127.

postrzegana wyłącznie jako narzędzie wspierające ludzki intelekt i empatię, a nie jako ich substytut. Tylko poprzez utrzymanie prymatu nad maszyną, zarówno w sferze nadzoru, jak i odpowiedzialności, możliwe jest zbudowanie nowoczesnej administracji, która wykorzystuje innowacje, nie tracąc przy tym z oczu przyrodzonej godności ludzkiej.

BIBLIOGRAFIA

- Bendyk E., *Metropolia w sieci*, „Samorząd Terytorialny" 2010, nr 6.
- Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa: Wolters Kluwer Polska 2018.
- Ciesiołkiewicz K., *Podmiotowość informacyjno-komunikacyjna w środowisku mediów cyfrowych jako cel edukacji*, „Forum Pedagogiczne" 2025, t. 15, nr 1, DOI: http://doi.org/10.21697/fp.2025.1.11.
- Dolniak P. i in., *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*, Warszawa: Wolters Kluwer Polska 2024.
- Fischer B., Pązik A., Świerczyński M. (red.), *Prawo sztucznej inteligencji i nowych technologii 3*, Warszawa: Wolters Kluwer Polska 2023.
- Flisak D., *Akt w sprawie sztucznej inteligencji*, komentarz praktyczny, wersja elektroniczna LEX (dostęp: 17.03.2026).
- Flisak D., *Sztuczna inteligencja - jak chronić prawa autorskie twórczości robotów,* „Rzeczpospolita" (22.05.2017), http://www.rp.pl/Opinie/305229984-Sztuczna-inteligencja--jak-chronic-prawa-autorskie-tworczosci-robotow.html (dostęp: 17.03.2026).
- Gumularz M. (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa: Wolters Kluwer Polska 2024.
- Jędrzejczak M., Szoszkiewicz Ł., Wydra J. (red.), *AI Act. Akt w sprawie sztucznej inteligencji. Komentarz*, Warszawa: Wolters Kluwer Polska 2025.
- Juściński P., *Prawo autorskie w obliczu rozwoju sztucznej inteligencji,* „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Intelektualnego" 2019, z. 1 (143).
- Kozłowski J., *Akt w sprawie sztucznej inteligencji w praktyce - charakterystyka unijnej regulacji opartej na ryzyku*, „Europejski Przegląd Sądowy", grudzień 2024.
- Kuriata N., *Słownik pojęć ze świata sztucznej inteligencji*, komentarz praktyczny, wersja elektroniczna LEX (dostęp: 17.03.2026).

- Martyniuk-Placha J., Miszczuk R., *Sztuczna inteligencja w administracji samorządowej*, komentarz praktyczny, wersja elektroniczna LEX (dostęp: 17.03.2026).
- Retzlaff C.O. i in., *Human-in-the-Loop Reinforcement Learning: A Survey and Position on Requirements, Challenges, and Opportunities*, „Journal of Artificial Intelligence Research" 2024, t. 79, DOI: https://doi.org/10.1613/jair.1.15348.
- Tischner A., *Sztuczna inteligencja i prawo wzorów przemysłowych - wybrane problemy*, „Europejski Przegląd Sądowy", grudzień 2025.
- Żabiński M. L., Guz H., *Emergentne AI. Jak samorząd lokalny adaptuje się do rewolucji AI*, „Samorząd Terytorialny" 2025, nr 4.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).