

ETYCZNE I PRAWNE ASPEKTY WYKORZYSTANIA SZTUCZNEJ INTELIGENCJI W DOKUMENTACJI MEDYCZNEJ

ETHICAL AND LEGAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN MEDICAL DOCUMENTATION

Mgr Beata Walczak-Kowalik

Uniwersytet Jana Długosza w Częstochowie, Polska
e-mail: b.walczak@ujd.edu.pl; <https://orcid.org/0000-0001-5011-4477>

Abstrakt

W artykule podjęto problem badawczy dotyczący warunków i ograniczeń etyczno-prawnych wykorzystania sztucznej inteligencji w ochronie zdrowia, ze szczególnym uwzględnieniem przetwarzania danych medycznych. Postawiono hipotezę, że wdrożenie rozwiązań opartych na sztucznej inteligencji w systemach opieki zdrowotnej, przy jednoczesnym zapewnieniu wysokich standardów ochrony danych i przejrzystości algorytmów, może znacząco poprawić jakość, dostępność i efektywność usług medycznych, bez naruszania podstawowych praw pacjenta. Celem badań jest identyfikacja kluczowych korzyści i wyzwań związanych ze stosowaniem sztucznej inteligencji w gromadzeniu, analizie i wykorzystaniu danych zdrowotnych oraz wskazanie ram prawnych i etycznych, które umożliwiają zrównoważone wdrażanie tych technologii. Metodologia opiera się na analizie dogmatycznoprawnej przepisów dotyczących ochrony danych osobowych oraz na przeglądzie literatury przedmiotu. W artykule zastosowano również metodę studium przypadku w odniesieniu do wybranych praktycznych zastosowań sztucznej inteligencji, takich jak systemy wspomagania diagnozy, elektroniczna dokumentacja medyczna oraz algorytmy predykcyjne. Wyniki analizy wskazują, że skuteczne wdrażanie sztucznej inteligencji w ochronie zdrowia wymaga nie tylko spełnienia wymogów prawnych dotyczących ochrony danych, lecz także przyjęcia zasad etyki

projektowania technologii, obejmujących transparentność, odpowiedzialność, nie-dyskryminację oraz nadzór człowieka nad procesami decyzyjnymi.

Słowa kluczowe: sztuczna inteligencja, etyka, dokumentacja medyczna

Abstract

The article addresses the research problem concerning the ethical and legal conditions and limitations of using artificial intelligence in healthcare, with particular emphasis on the processing of medical data. It puts forward the hypothesis that the implementation of AI-based solutions in healthcare systems while simultaneously ensuring high standards of data protection and algorithmic transparency can significantly improve the quality, accessibility, and efficiency of medical services without infringing patients' fundamental rights. The aim of the study is to identify the key benefits and challenges associated with the use of artificial intelligence in the collection, analysis, and utilisation of health data, and to indicate the legal and ethical frameworks that enable the sustainable deployment of these technologies. The methodology is based on a dogmatic-legal analysis of personal data protection regulations as well as a review of the relevant literature. The article also applies a case-study approach with regard to selected practical applications of artificial intelligence, such as diagnostic decision-support systems, electronic medical records, and predictive algorithms. The findings indicate that the effective implementation of artificial intelligence in healthcare requires not only compliance with legal requirements on data protection, but also the adoption of ethical design principles, including transparency, accountability, non-discrimination, and human oversight of decision-making processes.

Keywords: artificial intelligence, ethics, medical records

Wstęp

Sztuczna inteligencja (SI) zmieniła sposób funkcjonowania wielu krajów, firm, jednostek, jak i organizacji [Sameer, Mohamed, Babu, i in. 2020, 3]. Liczne zastosowania SI, które jeszcze niedawno pozostawały w sferze rozważań teoretycznych, stały się obecnie realnie dostępne. Przykłady obejmują rozwiązania w obszarze medycyny, pojazdów autonomicznych, systemów monitoringu, technologii bioidentyfikacji oraz innych zaawansowanych dziedzin [Krawiec 2019].

Wykorzystanie zaawansowanych technologii w administracji publicznej rodzi pytania o konieczność zachowania równowagi pomiędzy wdrażaniem

nowych możliwości technologicznych, a przestrzeganiem fundamentalnych norm i wartości etycznych, które stanowią podstawę funkcjonowania państwa i jego instytucji. Wymaga to uwzględnienia zasad równego traktowania obywateli, przejrzystości procedur, ochrony prywatności oraz zapewnienia sprawiedliwości i odpowiedzialności w procesach decyzyjnych wspieranych przez SI [Drab-Kurowska i Kuściński 2024, 232].

Zagadnienia etyczne związane z funkcjonowaniem systemów SI są trwałym elementem międzynarodowej debaty prawnej. Na całym świecie prowadzone są liczne inicjatywy mające na celu promowanie etycznego i bezpiecznego rozwoju SI, w które angażują się m.in. organizacje takie jak OpenAI, Pervade, Partnership on AI, Future of Life Institute czy AI for Good Summit, a także uczelnie wyższe, w tym Uniwersytet Kalifornijski w Berkeley, Harvard, Oxford i Cambridge. AI Now Institute zwraca uwagę, że żadna z firm technologicznych nie monitoruje w sposób systematyczny, w jakim stopniu sama przestrzega przyjętych zasad etycznych. Z kolei raport firmy Infosys dotyczący wykorzystania sztucznej inteligencji w ochronie zdrowia wskazuje na potrzebę wypracowania przez branżę i poszczególne organizacje dokładnie sformułowanych standardów etycznych i określenia związanych z nimi obowiązków, choć dokument nie precyzuje, jak miałyby one wyglądać. W sektorze medycznym istnieje potencjalna możliwość celowego konstruowania algorytmów w sposób nieetyczny, np. tak, aby rekomendacje dotyczące opieki nad pacjentem były uzależnione od posiadanego ubezpieczenia lub statusu materialnego [Topol 2021, 130-31].

Jak wskazuje *Human Rights Council* nowe rozwiązania cyfrowe zwiększają dostępność i jakość usług medycznych. SI znajduje coraz szersze zastosowanie w medycynie i staje się stopniowo nieodłącznym elementem współczesnych systemów opieki zdrowotnej [Zalewski 2020, 14]. Urządzenia medyczne wykorzystujące algorytmy SI odgrywają istotną rolę we wspieraniu pracy lekarzy, przyczyniając się przede wszystkim do znacznego skrócenia procesów diagnostycznych i terapeutycznych poprzez szybsze identyfikowanie źródeł choroby, dokładniejszą interpretację wyników badań oraz umożliwienie trafniejszego doboru metod leczenia.

Rzeczywistość technologii opartych na SI otwiera nowe perspektywy dla systemów ochrony zdrowia, w szczególności w zakresie gromadzenia, analizy i przetwarzania danych medycznych. Wprowadzenie narzędzi SI do praktyki

klinicznej i administracyjnej, takich jak elektroniczna dokumentacja medyczna, systemy wspomagania decyzji diagnostycznych czy predykcyjnych algorytmów oceny ryzyka, może znacząco podnieść jakość i efektywność świadczonych usług.

Rola SI w dokumentacji medycznej szybko ewoluuje od prostych narzędzi automatyzujących zapis wizyty po złożone systemy wspierające lekarzy w czasie rzeczywistym. Jak wskazuje Liu, zastosowanie tzw. „AI scribes” pozwoliło w badanych placówkach na znaczące skrócenie czasu przeznaczonego na ręczne wprowadzanie danych, co przełożyło się na poprawę jakości opieki i satysfakcji pacjentów [Liu 2024]. Transformacja wymaga równoczesnego wzmocnienia mechanizmów ochrony prywatności oraz przejrzystości działania algorytmów, aby zapewnić zgodność z zasadami etyki i przepisami RODO [Leung 2025, 7].

1. Pojęcie danych medycznych i ich szczególny charakter

Dane medyczne to wszelkie dane osobowe dotyczące stanu zdrowia danej osoby, dane mające oczywisty i ścisły związek ze zdrowiem (historie chorób, odbyte wizyty lekarskie, zażywane leki, badania laboratoryjne, wyroby medyczne itp.) oraz z danymi genetycznymi są kategorią danych osobowych, która powinna podlegać ochronie na wysokim poziomie [Jagielski 2016, 9]. Do danych dotyczących zdrowia zalicza się informacje dotyczące zdrowia fizycznego i psychicznego danej osoby, obejmujące choroby, objawy, uzależnienia, jak również korzystanie z urlopów zdrowotnych czy zwolnień lekarskich¹.

Dane dotyczące zdrowia należą do szczególnych kategorii danych osobowych i podlegają szczególnym zasadom przetwarzania oraz powinny podlegać szczególnej ochronie ze strony ich administratorów, a w sytuacji wystąpienia naruszenia ochrony danych osobowych powodują powstanie wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej, co obliuguje administratora do zawiadomienia takiej osoby o naruszeniu ochrony danych osobowych².

¹ Wyrok Trybunału Sprawiedliwości UE z 6 dnia listopada 2003 r., C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, ECLI:EU:C:2003:596.

² 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*

Rozważania dotyczące ochrony danych osobowych oraz etyki w medycynie stanowią ważny punkt odniesienia dla wykorzystania SI w dokumentacji medycznej. Rozporządzenie (UE) 2024/1689 ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji³ wprowadza podejście oparte na ryzyku, dzieląc systemy sztucznej inteligencji na cztery kategorie: systemy niedopuszczalne, systemy wysokiego ryzyka, systemy ograniczonego ryzyka, systemy minimalnego ryzyka. Systemy SI wykorzystywane w medycynie, w tym w dokumentacji medycznej, diagnostyce czy wspomaganiu decyzji klinicznych są klasyfikowane jako systemy wysokiego ryzyka. Podlegają one najbardziej rygorystycznym wymogom, m.in.: 1) system zarządzania ryzykiem – obowiązek identyfikacji i kontroli ryzyk związanych z bezpieczeństwem pacjentów i ochroną danych; 2) jakość danych treningowych – konieczność zapewnienia wysokiej jakości, reprezentatywnych i wolnych od uprzedzeń danych, co jest kluczowe w kontekście dokumentacji medycznej; 3) dokumentacja techniczna i audyt – producenci systemów muszą prowadzić szczegółową dokumentację i poddawać systemy procedurom oceny zgodności; 4) nadzór człowieka – SI nie może w pełni zastąpić lekarza, a decyzje medyczne muszą podlegać ludzkiej kontroli; 5) obowiązki w zakresie transparentności – pacjent powinien być informowany o wykorzystywaniu systemów SI w procesie leczenia czy dokumentowania. Podmioty medyczne wykorzystujące SI w dokumentacji pacjentów nie mogą ograniczyć się jedynie do przestrzegania RODO i zasad etyki zawodowej, ale muszą także zapewnić zgodność z wymogami AI Act. Ponadto rozporządzenie przewiduje system sankcji za naruszenia, w tym kary finansowe sięgające nawet 35 mln euro lub 7% rocznego obrotu (art. 99 rozporządzenia (UE) 2024/1689 AI Act).

2. Sztuczna inteligencja w ochronie zdrowia – typowe zastosowania

Nie ma wątpliwości, że zastosowania SI w medycynie będą obejmować coraz szersze obszary. Wiele zastosowań SI, które jeszcze kilka lat temu

swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L 119/1 [dalej: RODO].

³ 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, Dz. Urz. UE L 2024/1689.

wydawały się być tylko hipotetyczne, jest teraz osiągalnych. Należą do nich aplikacje w dziedzinie medycyny, pojazdów autonomicznych, monitoringu, bioidentyfikacji i innych. W wielu dziedzinach wymagających specjalistycznej wiedzy i zaawansowanej analizy wykorzystuje się systemy ekspertowe, czyli systemy komputerowe odtwarzające proces podejmowania decyzji charakterystyczny dla człowieka eksperta. Przykładowym obszarem ich zastosowań jest diagnostyka medyczna [Sempryk 2023, 72].

Potencjał zastosowania SI w medycynie jest niezwykle szeroki. Szczególnie widoczny jest w przypadku wykorzystania metod opartych na uczeniu maszynowym, które stanowią istotny komponent innowacyjnych rozwiązań wdrażanych w ostatnich latach. Przykładem takich zastosowań są systemy analizujące dokumentację medyczną pacjentów w celu rekomendowania optymalnych strategii terapeutycznych, dostosowanych do indywidualnych potrzeb i historii leczenia⁴.

Systemy SI posiadają zdolność analizowania obrazów np. radiologicznych, jak również wyników badań oraz innych danych medycznych, co stwarza szansę na stawianie szybszych i bardziej trafnych diagnoz [Davenport i Kalakota 2019, 95]. Systemy monitorujące zdrowie, wykorzystujące algorytmy SI do analizy danych zdrowotnych, mogą prowadzić do wcześniejszego rozpoznawania chorób, lepszego dostosowania diety i aktywności fizycznej, a także wsparcia w zarządzaniu różnorodnymi stanami zdrowia [Alowais, Alghamdi, Alsuhbany, i in. 2023]. Dzięki zastosowaniom sztucznej inteligencji lekarze mogą personalizować leczenie, dopasowując je do konkretnego pacjenta [Davenport i Kalakota 2019, 96].

„Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nieautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie” (art. 4 pkt 2 RODO). Czynność przetwarzania wykonywana automatycznie to czynność dokonywana za pośrednictwem urządzenia np. komputera. Natomiast

⁴ IBM, Clinical Decision Support, <https://www.ibm.com/watson-health/solutions/clinical-decision-support> [dostęp: 07.07.2025].

przetwarzanie wykonywane w sposób nieautomatyzowany polega na dokonywaniu czynności metodami tradycyjnymi (ręcznie) [Gudowska-Natanek i Kuca 2024, 39].

Dane zdrowotne podlegają przetwarzaniu w różnych obszarach życia społecznego i gospodarczego, w tym w systemach ubezpieczeń zdrowotnych, świadczeń społecznych oraz w działalności podmiotów sektora farmaceutycznego i Narodowego Funduszu Zdrowia. Coraz częściej dane te gromadzone są również przez dostawców usług cyfrowych np. aplikacje zdrowotne na podstawie zgody osoby, której dane dotyczą [Łakomiec 2020, 161].

W ochronie zdrowia SI coraz częściej znajduje zastosowania wykraczające poza klasyczną diagnostykę. Dynamicznie rozwijają się systemy analizujące elektroniczną dokumentację medyczną, które potrafią automatycznie wychwytywać nieprawidłowości w zapisach klinicznych i wspierać proces kontroli jakości danych [Perkins 2024, 38-40]. Równolegle coraz większą wagę przykładą się do tworzenia solidnych ram etycznych, mających ograniczać ryzyko błędów systematycznych i stronniczości algorytmów wykorzystywanych w patomorfologii i diagnostyce cyfrowej [Hanna 2025, 89].

3. Etyczne wyzwania przetwarzania danych przez sztuczną inteligencję

W wytycznych dotyczących etyki eksperci wskazali trzy zasadnicze cechy, którymi powinna odznaczać się godna zaufania SI: zgodność z prawem, etyczność oraz solidność – zarówno w aspekcie technicznym, jak i społecznym. Dokument ten podkreśla również cztery kluczowe zasady etyczne, które powinny być uwzględnione w projektowaniu i wdrażaniu technologii opartych na SI: poszanowanie autonomii człowieka, zapobieganie wyrządzaniu szkód, sprawiedliwość oraz możliwość wyjaśnienia decyzji podejmowanych przez system SI. W wytycznych określono także siedem wymogów, które powinny spełniać systemy wykorzystujące SI. Należą do nich: solidność techniczna i bezpieczeństwo (zapewnienie bezpieczeństwa użytkowników, niezawodności oraz zdolności do radzenia sobie z błędami), ochrona prywatności i danych osobowych, przejrzystość (zarówno w zakresie działania algorytmów, jak i procesu decyzyjnego), odpowiedzialność, niedyskryminacja i sprawiedliwość. Podkreślono również,

że technologie SI powinny wspierać dobrostan społeczny i środowiskowy, a nadzór nad ich funkcjonowaniem musi sprawować człowiek⁵.

Kwestia etycznego wykorzystania SI jest złożona i często analizowana w trzech obszarach: 1) uprzedzenia w algorytmach – problem ten dotyczy sytuacji, w których algorytmy odtwarzają i utrwalają istniejące stereotypy oraz uprzedzenia społeczne, zjawisko to rodzi pytania o odpowiedzialność projektantów systemów SI oraz konieczność wdrażania mechanizmów zapewniających równe traktowanie i eliminowanie dyskryminacji algorytmicznej [Sempryk 2023, 77]. Wykorzystanie algorytmów predykcyjnych w opiece zdrowotnej budzi obawy związane z etyką i równością jak zapewnić, by SI nie faworyzowała ani dyskryminowała ze względu na pochodzenie rasowe czy ekonomiczne [O’Neil 2016, 21]; 2) brak przejrzystości działania – w wielu przypadkach nie jest możliwe dokładne przesledzenie, w jaki sposób algorytmy dochodzą do określonych wniosków na podstawie dostarczonych danych, odpowiedzi na to wyzwanie rozwijane są koncepcje Explainable AI (XAI), których celem jest zapewnienie zrozumiałości i przejrzystości procesów decyzyjnych realizowanych przez systemy SI [Sempryk 2023, 77]. Badania naukowe pokazują, że algorytmy i SI nie posiadają pełnej obiektywności. Technologia zawsze odzwierciedlała istniejące w społeczeństwach uprzedzenia i stereotypy, ponieważ bazy danych, na których się opiera i uczy, optymalizują oraz wdrażają ludzie [Górska i Jemielniak 2023]. Wyeliminowanie tego ludzkiego pierwiastka w systemach jest niemożliwe [Mittermaier, Raza, i Kvedar 2023, 1-8]; 3) ochrona danych osobowych – dane wykorzystywane przez systemy SI często obejmują informacje wrażliwe, objęte ochroną prawną. Zapewnienie ich bezpieczeństwa i zgodności przetwarzania z obowiązującymi regulacjami, takimi jak RODO, stanowi ważny aspekt etyczny i prawny. Wśród rozwiązań technicznych wspierających ochronę danych wskazuje się anonimizację, pseudonimizację oraz wdrażanie przejrzystych zasad przetwarzania i udostępniania informacji [Sempryk 2023, 77].

Rozwinięciem tych ogólnych postulatów są koncepcje *privacy by design* – ochrona danych w fazie projektowania oraz *privacy by default* – domyślna ochrona danych, które w sektorze dokumentacji medycznej wymagają

⁵ Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, <https://op.europa.eu/pl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1> [dostęp: 07.07.2025].

szczegółowych rozwiązań praktycznych. W ramach *privacy by design* można wskazać m.in.: szyfrowanie danych pacjentów zarówno w bazach, jak i podczas transmisji; segmentację dostępu (lekarz ma dostęp wyłącznie do dokumentacji swoich pacjentów); logowanie każdej operacji i rejestrację zmian; anonimizację danych w celach badawczych; a także zasadę minimalizacji danych – przechowywanie wyłącznie informacji niezbędnych do leczenia.

Z kolei *privacy by default* oznacza, że każdy nowy rekord pacjenta jest domyślnie dostępny wyłącznie dla lekarza prowadzącego i uprawnionego personelu, funkcje udostępniania danych online są domyślnie wyłączone, a system zawiera mechanizmy przypominające o konieczności uzyskania zgody pacjenta oraz politykę retencji danych ograniczoną do minimalnego wymaganego prawem okresu.

Rozwój SI skłania do refleksji nad zakresem autonomii systemów w podejmowaniu decyzji oraz nad etyczno-prawnymi granicami, które należy im wyznaczyć [Rahwan 2018, 8]. Lekarz zobowiązany jest do udzielenia pacjentowi informacji o stanie jego zdrowia, rozpoznaniu, wynikach leczenia oraz rokowaniu [Ciszewski 2002, 45-47]. Jednym z aspektów etycznego projektowania SI jest dążenie do jej transparentności. Oznacza to, że sposób działania algorytmów powinien być możliwy do zrozumienia zarówno dla użytkowników, jak i dla wszystkich stron zaangażowanych. Przejrzystość ta jest niezbędna nie tylko dla zapewnienia kontroli nad technologią, lecz także dla budowania społecznego zaufania [Gebru 2021, 86-92].

W dobie rozwoju SI kluczowe znaczenie zyskuje ochrona prywatności oraz danych osobowych użytkowników. Projektanci systemów SI powinni nie tylko przestrzegać obowiązujących regulacji prawnych, takich jak RODO, lecz także wdrażać zasady ochrony danych już na etapie projektowania systemu – zgodnie z koncepcją *privacy by design*, która zakłada proaktywne i prewencyjne podejście do ochrony prywatności [Cavoukian 2009, 3].

Wśród algorytmów wykorzystywanych do przetwarzania danych szczególnie istotne z punktu widzenia analizy prawnej i etycznej są algorytmy oparte na SI. Systemy informacyjne wykorzystujące SI nie ograniczają się wyłącznie do gromadzenia danych i ekstrakcji informacji, lecz coraz częściej generują nową wiedzę i podejmują decyzje mające doniosłe znaczenie normatywne. Przesunięcie ciężaru decyzyjnego z człowieka na algorytm rodzi pytania o zakres odpowiedzialności prawnej, zgodność z zasadą

legalizmu oraz zapewnienie prawa do rzetelnego i sprawiedliwego postępowania administracyjnego.

W kontekście ochrony danych osobowych szczególnie istotne jest ryzyko naruszenia prywatności pacjentów i poufności informacji medycznych. Choć proces anonimizacji danych stanowi środek ograniczający to ryzyko, nie zapewnia pełnej ochrony. Zaawansowane algorytmy SI potrafią wykrywać ukryte wzorce i korelacje, co w praktyce może prowadzić do częściowej rekonstrukcji danych osobowych i ujawnienia informacji wrażliwych. Wymaga to szczególnej ostrożności ustawodawcy i organów administracji publicznej w zakresie tworzenia i stosowania przepisów prawa materialnego i procesowego regulujących wykorzystanie SI w sektorze zdrowia [Morawski 2022, 23].

4. Odpowiedzialność za decyzje podejmowane z udziałem sztucznej inteligencji

Wraz z postępem technologicznym SI coraz częściej uczestniczy w procesach decyzyjnych, które dotąd były zarezerwowane wyłącznie dla ludzi. Powstaje zatem pytanie, czy i w jakim zakresie SI może rzeczywiście decydować, czy jedynie wspomagać człowieka w podejmowaniu decyzji. W przyszłości pojawią się nowe dylematy etyczne, dotyczące m.in. stopnia autonomii maszyn, zakresu ich odpowiedzialności, a nawet koncepcji „praw maszyn”. Szczególnie istotne będą rozważania nad tym, jak rozwój SI wpłynie na ludzką autonomię, wolność wyboru oraz odpowiedzialność moralną. Sposób, w jaki społeczeństwo i ustawodawcy odpowiedzą na te wyzwania, będzie miał fundamentalne znaczenie dla kształtu relacji człowiek-technologia w nadchodzących dekadach [Bostrom 2014, 115-23].

Posługiwanie się SI w podejmowaniu decyzji może podnieść pytania dotyczące odpowiedzialności za dane i decyzje podejmowane przez algorytmy. Warto rozważyć, jakie dane są gromadzone, przetwarzane oraz wykorzystywane, jakie mają wpływ na decyzje i jak zapewnić odpowiedzialne i etyczne podejście do zarządzania tymi danymi [Frączek 2023, 296].

Jednym z aspektów etycznych związanych z rozwojem SI jest ryzyko wykorzystania jej do unikania odpowiedzialności za podejmowanie trudnych decyzji. W kontekście takich zastosowań roboty medyczne problem ten sprowadza się do przeniesienia ciężaru odpowiedzialności z człowieka na algorytmy, co rodzi pytania o granice odpowiedzialności prawnej

i moralnej użytkowników oraz projektantów tych systemów. Problemem jest odpowiedzialność za decyzje podejmowane przez maszyny, które z natury nie posiadają świadomości ani moralnego podmiotu w tradycyjnym tego słowa znaczeniu [Kosiak 2023, 341-50].

W celu pogłębienia analizy warto zaprezentować konkretne modele odpowiedzialności, które są już stosowane lub szeroko dyskutowane w doktrynie prawa medycznego i prawa nowych technologii. Po pierwsze, wskazuje się na odpowiedzialność cywilną lekarza za decyzję medyczną podjętą przy wsparciu systemu sztucznej inteligencji, gdy system pełni jedynie rolę narzędzia pomocniczego. W takim przypadku lekarz odpowiada na zasadach klasycznych – kontraktowych bądź deliktowych – z uwzględnieniem obowiązku zachowania należytej staranności w doborze i nadzorze nad oprogramowaniem [Wałdoch 2024, 216; Bączyk-Rozwadowska 2022, 28-30]. Po drugie, rozważana jest odpowiedzialność producenta systemu AI w razie wady konstrukcyjnej lub błędu działania systemu, który spełnia definicję „produktu” w rozumieniu dyrektywy 85/374/EWG o odpowiedzialności za produkt niebezpieczny, a w przyszłości także projektowanej dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję [Deptalski i Dziewałtowski-Gintowt 2024, 39-60; Kaczan 2022, 145-53]. Po trzecie, w przypadku naruszeń ochrony danych osobowych generowanych lub przetwarzanych przez systemy SI, aktualizuje się odpowiedzialność administratora danych medycznych na podstawie art. 82 RODO, który przyznaje osobie, której dane dotyczą, prawo do odszkodowania za szkody spowodowane naruszeniem przepisów o ochronie danych.

Zakończenie

Mimo licznych korzyści wynikających z wykorzystania SI w dokumentacji medycznej takich jak usprawnienie analizy danych pacjentów, automatyczne wypełnianie formularzy czy wsparcie diagnostyczne nie można ignorować związanych z tym wyzwań etycznych i prawnych. Kluczowe kwestie obejmują ochronę prywatności pacjentów, bezpieczeństwo danych wrażliwych oraz zgodność przetwarzania informacji z obowiązującymi przepisami o ochronie danych osobowych. Szczególne znaczenie ma zapewnienie transparentności działania algorytmów wspierających decyzje kliniczne oraz możliwość weryfikacji ich rekomendacji przez personel medyczny. Potrzebne są w tym zakresie odpowiednie regulacje prawne i wytyczne etyczne, które

zagwarantują poszanowanie praw pacjenta, bezpieczeństwo danych medycznych oraz odpowiedzialne wdrażanie rozwiązań SI w ochronie zdrowia.

Najnowsze analizy wskazują, że trwałe zakorzenienie SI w praktyce medycznej wymaga nie tylko ram prawnych, lecz także bieżącego monitorowania skutków jej stosowania. W miarę integracji SI z opieką kliniczną priorytetem staje się ciągła ocena wpływu algorytmów na bezpieczeństwo pacjentów, jakość dokumentacji i równość w dostępie do świadczeń zdrowotnych. Takie podejście łączące innowację z odpowiedzialnością staje się kluczowym wyznacznikiem dalszego, zrównoważonego rozwoju technologii SI w ochronie zdrowia [Weiner 2025, 14-20].

Rozwój SI wymaga wypracowania spójnych standardów etycznych oraz jasnego określenia zasad odpowiedzialności za decyzje i działania podejmowane przez systemy autonomiczne. Kluczowe jest zapewnienie, aby technologie SI były zgodne z wartościami humanistycznymi i nie stwarzały zagrożenia dla ludzi ani dla środowiska naturalnego. Na zakończenie warto przywołać ideę zawartą w wytycznych etycznych opublikowanych przez AI High-Level Expert Group: „AI nie jest celem samym w sobie, lecz obiecującym środkiem do zwiększenia ludzkiego dobrostanu, wspierania indywidualnego i społecznego rozwoju oraz dobra wspólnego, a także stymulowania postępu i innowacji”⁶. W związku z tym głęboko wierzę, że SI może być skutecznie wykorzystana jako narzędzie służące dobru publicznemu.

PIŚMIENNICTWO

- Alowais, Shuroug A., Sahar S. Alghamdi, Nada Alsuhebany, i in. 2023. „Revolutionizing healthcare: the role of artificial intelligence in clinical practice.” *Alowais et al. BMC Medical Education* 23:1-15. <https://doi.org/10.1186/s12909-023-04698-z>
- Bączyk-Rozwadowska, Katarzyna. 2022. „Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie.” *Przegląd Prawa Medycznego* 3, nr 3-4:5-35. <https://doi.org/10.70537/z7xnk378>
- Bostrom, Nick. 2014. *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.
- Cavoukian, Ann. 2009. *Privacy by Design: The 7 Foundational Principles*. Toronto: Information and Privacy Commissioner of Ontario.

⁶ *Ethics guidelines for trustworthy AI*, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> [dostęp: 09.07.2025].

- Ciszewski, Jerzy. 2002. *Prawa pacjenta w aspekcie odpowiedzialności lekarza za niektóre szkody medyczne*. Gdańsk: Wydawnictwo Arche.
- Davenport, Thomas, i Rajeev Kalakota. 2019. „The Potential for Artificial Intelligence in Healthcare.” *Future Healthcare Journal* 6, nr 2:94-98. <https://doi.org/10.7861/futurehosp.6-2-94>
- Deptalski, Mikołaj, i Piotr Dziewałtowski-Gintowt. 2024. „Tortious liability regime for medical devices using artificial intelligence: Analysis of current solutions.” *Transformacje Prawa Prywatnego* 2:37-64.
- Drab-Kurowska, Agnieszka, i Michał Kuściński. 2024. „Wykorzystanie AI w administracji publicznej.” *Biuletyn Gospodarki i Biblioteki Publicznej* nr 383:227-40.
- Frączek, Michał, i Krzysztof Spaliński. 2023. „Bezpieczeństwo informacji w dobie sztucznej inteligencji: analiza ryzyka i wyzwania związane z ChatGPT.” *Zeszyty Naukowe Pro Publico Bono* 1, nr 1:287-302. <https://doi.org/10.5604/01.3001.0054.1726>
- Gebru, Timnit. 2021. „Datasheets for Datasets.” *Communications of the ACM* 64, nr 12:86-92. <https://doi.org/10.1145/3458723>
- Górska, Aleksandra, i Dariusz Jemielniak. 2023. „The Invisible Women: Uncovering Gender Bias in AI-Generated Images of Professionals.” *Feminist Media Studies* 23, nr 8:4370-375. <https://doi.org/10.1080/14680777.2023.2263659>
- Gudowska-Natanek, Elżbieta, i Grzegorz Kuca. 2024. „Przetwarzanie danych osobowych.” W *Prawo ochrony danych osobowych i prawo do informacji publicznej*, red. Elżbieta Gudowska-Natanek, i Grzegorz Kuca, 35-54. Warszawa: Wydawnictwo C.H. Beck.
- Hanna, Matthew. 2025. „Ethical and Bias Considerations in AI-ML in Pathology.” *Seminars in Diagnostic Pathology* 42, nr 2:85-92. <https://doi.org/10.1016/j.semdp.2025.01.004>
- Jagielski, Mariusz. 2016. „Pojęcie danych medycznych i zasady ich ochrony.” W *Ochrona danych osobowych medycznych*, red. Krzysztof Wojsyk, Paweł Litwiński, Mariusz Jagielski, i in., 1-44. Warszawa: Wydawnictwo C.H. Beck.
- Kaczan, Damian. 2022. „Odpowiedzialność odszkodowawcza za funkcjonowanie sztucznej inteligencji w medycynie.” *Annales Universitatis Paedagogicae Cracoviensis. Studia de Cultura* 14, nr 2:145-60.
- Kosiak, Piotr. 2023. „Etyczne aspekty rozwoju i wykorzystania sztucznej inteligencji.” *International Journal of New Economics and Social Sciences* 5(21):341-50. <https://doi.org/10.5604/01.3001.0054.8421>
- Krawiec, Krzysztof. 2019. „Sztuczna inteligencja w świecie obrazów.” <https://www.sztuczna-inteligencja.org.pl/sztuczna-inteligencja-w-swiecie--obrazow/> [dostęp: 16.06.2025].

- Leung, Tiffany. 2025. „AI Scribes in Health Care: Balancing Transformative Potential and Risk.” *NPJ Digital Medicine* 8:1-9. <https://doi.org/10.1038/s41746-025-00123-4>
- Liu, Tsai-Ling. 2024. „AI-Powered Clinical Documentation and Clinicians’ Experiences.” *JAMA Network Open* 7(9):e2432460. <https://doi.org/10.1001/jamanetworkopen.2024.32460>
- Łakomiec, Katarzyna. 2020. *Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia*. Warszawa: Wydawnictwo C.H. Beck.
- Mittermaier, Maximilian, Mariam M. Raza, i Joseph C. Kvedar. 2023. „Bias in AI-Based Models for Medical Applications: Challenges and Mitigation Strategies.” *NPJ Digital Medicine* 6, nr 1:1-8. <https://doi.org/10.1038/s41746-023-00885-9>
- Morawski, Ryszard. 2022. „Etyczne wyzwania techno-nauki – techniki informacyjne.” *Nauka* 2:7-33. <https://doi.org/10.24425/nauka.2022.140329>
- O’Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.
- Perkins, Scott. 2024. „Improving Clinical Documentation with Artificial Intelligence: A Systematic Review.” *Journal of AHIMA* 95, nr 2:33-45.
- Rahwan, Iyad. 2018. „Society-in-the-Loop: Programming the Algorithmic Social Contract.” *Ethics and Information Technology* 20, nr 1:5-14. <https://doi.org/10.1007/s10676-017-9430-8>
- Sameer Hoosain, Mohamed, Babu Sena Paul, Seeram Ramakrishna, i in. 2020. „The Impact of 4IR Digital Technologies and Circular Thinking on the United Nations Sustainable Development Goals.” *Sustainability* 12, nr 23:1-19.
- Sempryk, Joanna. 2023. „Implikacje etyczne na temat sztucznej inteligencji.” *Studia – Prace Badawcze – Dokumenty z Zakresu Nauki Społecznej Społeczeństwo* 33, nr 2:69-81.
- Topol, Eric. 2021. *Medycyna głęboka. Jak sztuczna inteligencja może ponownie uczynić opiekę zdrowotną ludzką?* Warszawa: ITEM Publishing.
- Wałdoch, Katarzyna. 2024. „Verification error and supervision error – new types of medical errors resulting from the use of artificial intelligence systems occurring during the provision of health services.” *Studia Iuridica Toruniensia* 34, nr 1:209-26. <https://doi.org/10.12775/SIT.2024.011>
- Weiner, Ellison. 2025. „Ethical Challenges and Evolving Strategies in the Clinical Integration of AI.” *Health Care Ethics* 33, nr 1:12-27.
- Zalewski, Tomasz. 2020. „Definicja sztucznej inteligencji.” W *Prawo sztucznej inteligencji*, red. Luigi Lai, i Marek Świerczyński, 1-14. Warszawa: Wydawnictwo C.H. Beck.