Zdrowie Publiczne i Zarządzanie 2025; 23 (1): 11–19
www.ejournals.eu/czasopismo/zdrowie-publiczne-i-zarzadzanie, doi:10.4467/20842627OZ.25.003.22048

Informatyzacja systemu ochrony zdrowia – aspekty etyczne i prawne zastosowania sztucznej inteligencji. Część II

Szczepan Jakubowski https://orcid.org/0000-0001-6419-9686
Anna Maj https://orcid.org/0009-0006-4232-9957
Artur Romaszewski https://orcid.org/0000-0003-3416-716X
Mariusz Duplaga https://orcid.org/0000-0001-6963-8414

Zakład Promocji Zdrowia i e-Zdrowia, Instytut Zdrowia Publicznego, Wydział Nauk o Zdrowiu, Uniwersytet Jagielloński Collegium Medicum

Adres do korespondencji: Szczepan Jakubowski, Zakład Promocji Zdrowia i e-Zdrowia, Instytut Zdrowia Publicznego, ul. Skawińska 8, 31-066 Kraków, Polska, szczepan.jakubowski@uj.edu.pl

Abstract

Healthcare digitalisation – ethical and legal aspects of artifical intelligence. Part II

The integration of artificial intelligence (AI) into healthcare is rapidly transforming clinical practice. While AI offers significant potential for improving diagnosis, treatment, and patient outcomes, it also raises complex ethical and legal challenges. This paper explores the ethical considerations surrounding AI in healthcare, including bias in algorithms, data privacy, and allocation of responsibility for AI-related errors. The authors also examine the legal frameworks governing AI in the European Union and Poland, focusing on the recently adopted AI Act. The study highlights the need for a comprehensive regulatory framework that balances the benefits of AI with the protection of patient rights and public safety. Key issues discussed include the risk of algorithmic bias, the importance of transparency as well as accountability, and the challenges of assigning liability for AI-related harms.

Keywords: **AI, artificial intelligence, AIA, ethics, healthcare, law of new technologies**

Słowa kluczowe: **AIA, etyka, ochrona zdrowia, prawo nowych technologii, SI, sztuczna inteligencja**

Wstęp

Niniejsza praca jest kolejnym artykułem koncentrującym się na informatyzacji systemu ochrony zdrowia. W pierwszym artykule [1] poświęconym elektronicznym usługom zaufania opisano nowe inicjatywy Unii Europejskiej (UE) zawarte w rozporządzeniu eIDAS (electronic IDentification, Authentication and trust Services) 2.0 [2]. W tym artykule natomiast omówione zostaną aspekty etyczne stosowania sztucznej inteligencji (SI) w ochronie zdrowia, ze szczególnym uwzględnieniem odpowiedzialności za błędy i szkody medyczne oraz kwestie prawne stosowania SI w UE oraz w Polsce.

Definicja SI określa, że jest to „skomputeryzowany system, który jest wyposażony w zdolność do wykonywania zadań lub procesów rozumowania, które zwykle kojarzymy z poziomem inteligencji człowieka" [3]. Jedna z definicji systemów stosujących SI zaproponowana przez Organizację Współpracy Gospodarczej i Rozwoju w 2023 roku mówi:

> System sztucznej inteligencji to system maszynowy, który dla celów jawnych lub niejawnych wnioskuje na podstawie

otrzymanych danych wejściowych, w jaki sposób generować dane wyjściowe, takie jak prognozy, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne. Różne systemy sztucznej inteligencji różnią się poziomem autonomii i zdolności adaptacyjnych po wdrożeniu [4].

Sztuczna inteligencja w ochronie zdrowia jest obecnie najczęściej wykorzystywana w celu poprawy skuteczności, jakości i wydajności procedur diagnostycznych oraz terapeutycznych [5–6]. Typowym przykładem zastosowania SI są systemy wspomagania decyzji klinicznych wspierające personel medyczny w trakcie leczenia pacjentów [7]. Zastosowanie rozwiązań opartych na SI pozwala także zautomatyzować czasochłonne i powtarzalne zadania realizowane w placówce medycznej, takie jak opisywanie wyników badań [8].

Kolejne generacje systemów opartych na SI wykazują coraz większą precyzję, co znacząco podnosi ich przydatność w procesach diagnostycznych. Przykładem mogą być rozwiązania SI wykorzystywane do rozpoznawania uszkodzonych naczyń w oku, które charakteryzują się wysoką czułością i swoistością – miarami dokładności testów diagnostycznych – w wykrywaniu retinopatii cukrzycowej na podstawie zdjęć dna oka [8–10].

Szersze stosowanie systemów wykorzystujących SI może się przyczynić do zwiększenia dostępności usług zdrowotnych. Systemy SI umożliwiają analizę rozległych i złożonych zbiorów danych, których ocena przekracza możliwości człowieka [11–12]. Jednak w tym momencie przepisy prawne obowiązujące w Unii Europejskiej nie pozwalają jeszcze, aby takie systemy były wykorzystywane do autonomicznych diagnoz bez udziału klinicysty [13]. Pomimo dynamicznego rozwoju i nowych możliwości, jakie dają systemy SI, ich stosowanie rodzi również wątpliwości etyczne. Dotyczą one szczególnie kwestii odpowiedzialności za decyzje podejmowane przez pracowników ochrony zdrowia na podstawie podpowiedzi systemu SI [14]. Kolejnym zagrożeniem jest brak reprezentatywności danych wykorzystywanych w procesie modelowania systemów. Z uwagi na niepełność danych użytych do uczenia systemów SI mogą one faworyzować określone grupy, na przykład ze względu na pochodzenie etniczne [14]. Innym istotnym wyzwaniem, szczególnie w przypadku zastosowań w opiece zdrowotnej, jest brak transparencji. Większość systemów SI, szczególnie współczesnych, działa na zasadzie efektu „czarnej skrzynki". Systemy SI generują właściwe i precyzyjne diagnozy, rokowania lub decyzje, ale nie umożliwiają wglądu w mechanizm podejmowania decyzji, co utrudnia zrozumienie, poznanie, wytłumaczenie, dlaczego i jak do tego doszło. Ze względu na bezpieczeństwo pacjenta klinicysta może natomiast oczekiwać wyjaśnienia i przedstawienia procesu rozumowania stojącego za sugerowaną diagnozą lub proponowanym leczeniem.

W wielu przypadkach innowacyjne rozwiązania SI są stosowane w ochronie zdrowia po raz pierwszy w obszarach, które nie zostały uregulowane prawnie. W efekcie dochodzi do sytuacji, w której przepisy prawne nie nadążają za praktycznymi zastosowaniami SI [15]. Z kolei brak jednolitych i powszechnie stosowanych ram określających SI może być źródłem problemów w przypadku roszczeń prawnych. Dodatkowo niejednoznaczna odpowiedzialność za skutki wynikające z zastosowania SI w trakcie udzielania świadczeń zdrowotnych jest istotnym problemem w sytuacji, w której nie jest znany mechanizm działania systemu, pomimo wiedzy na temat wykorzystanych danych i dostępu do wygenerowanych odpowiedzi [16].

Etyczne aspekty stosowania SI w ochronie zdrowia

Zastosowanie SI w ochronie zdrowia budzi wątpliwości etyczne, zwłaszcza w kontekście zasad sprawiedliwości społecznej i równości szans, które mogą zostać naruszone przez nierówny dostęp do technologii lub utrwalanie nierówności. Dokładność systemów SI oraz użyteczność uzyskiwanych za ich pomocą wyników zależy od jakości zbiorów danych, na których były one uczone. Okazuje się, że systemy wykorzystujące SI mogą prowadzić do utrwalania nierówności związanych z płcią, przynależnością etniczną, statusem społecznym i materialnym, o ile zostały one opracowane na podstawie zbiorów danych zawierających takie dysproporcje [6, 17].

Wyniki generowane przez SI mogą być obarczone błędami wynikającymi z ograniczeń danych wejściowych. Błędy te, takie jak niekompletność informacji czy brak reprezentatywności dla różnych grup społeczno-ekonomicznych, mogą prowadzić do wniosków, które nie są wiarygodne i uniwersalne [6]. Dobrym przykładem takiego błędu jest sytuacja użycia systemu SI dokonującego oceny ryzyka zdrowotnego do identyfikacji pacjentów potrzebujących pomocy i wykorzystywanego w Stanach Zjednoczonych dla 200 milionów pacjentów rocznie, który dostarczał fałszywych prognoz uwarunkowanych przynależnością do różnych grup etnicznych [18]. Na podstawie tego narzędzia w placówkach medycznych podejmowano decyzje o skierowaniu pacjentów do specjalnych programów zdrowotnych. Błędne prognozy doprowadziły do sytuacji, w której liczba Afroamerykanów kierowanych do wspomnianych specjalnych programów zmniejszyła się o połowę, pomimo że ich faktyczny stan zdrowia był gorszy niż pozostałych grup etnicznych. Problem wynikał z tego, że system SI do oceny potrzeb zdrowotnych wykorzystywał dane o kosztach związanych z leczeniem, a nie dane o faktycznym stanie zdrowia. Systemowo mniej pieniędzy było wydawanych na pacjentów pochodzenia afroamerykańskiego, mimo że mieli oni co najmniej taki sam poziom potrzeb zdrowotnych jak inne grupy etniczne. System przyjął, że skoro Afroamerykanie generują niższe koszty zdrowotne, to są zdrowsi [18]. Opisane zjawisko, w którym system komputerowy podejmuje decyzje w sposób systematycznie dyskryminujący albo faworyzujący pewne grupy ludzi, określa się błędem algorytmicznym (*algorithmic bias*) [18].

Problemami mogą być również powtarzalność i odtwarzalność[1] badań nad wykorzystaniem SI. Często zbiory danych, kod źródłowy oprogramowania i mechanizm uczenia systemów SI nie są udostępniane publicznie. Uniemożliwia to innym naukowcom przeprowadzenie weryfikacji i sprawdzenie uzyskanych wyników [19–21].

Morley i współpracownicy zwracają także uwagę na ryzyko nadmiernego uzależnienia klinicystów od SI, w miarę jak takie systemy będą wykorzystywane do realizacji coraz większej liczby zadań w placówkach medycznych [22]. Może to także prowadzić do poczucia zmniejszenia własnych umiejętności wśród personelu medycznego, a także ograniczenia bezpośrednich kontaktów z pacjentami. Z perspektywy pacjentów niepokojące może być wprowadzenie formalnego obowiązku stosowania się do zaleceń generowanych przez urządzenia wyposażone w SI [22]. Jak się wydaje, celem implementacji systemów SI w ochronie zdrowia powinna być poprawa wydajności usług zdrowotnych, a nie zastępowanie ludzkiego wymiaru relacji pacjent–lekarz [8].

Szczególne zagrożenie pojawia się również w związku z ciągłym uczeniem się (często automatycznym) systemów SI. Istnieje potencjalne ryzyko, że dostęp do nowych danych i dostosowywanie się do zmian w populacjach pacjentów mogą się wiązać z ryzykiem nadpisania wcześniej wyuczonych lub pojawienia się nowych błędów we wzorcach [23]. Zazwyczaj organy regulacyjne zatwierdzają tylko jeden zamknięty zbiór danych do uczenia SI (jeżeli mieści się to w ich kompetencjach). To podejście nie uwzględnia jednak konieczności aktualizacji systemów SI, a struktura danych zmienia się ze względu na zmiany w populacjach pacjentów, a także nowe narzędzia wykorzystywane do gromadzenia i zarządzania danymi [14].

Rajpurkar i współpracownicy wskazują, że do najważniejszych etycznych wyzwań związanych z wykorzystaniem systemów SI w ochronie zdrowia należą: niepewność predykcji, zapewnienie poufności i bezpieczeństwa danych, ryzyko marginalizowania niektórych grup ludności, powielanie nierówności w zdrowiu, a także kwestia odpowiedzialności za decyzje podejmowane na podstawie wskazań SI w praktyce klinicznej [14].

Różne formy regulacji i nadzoru SI mogą natomiast pomóc w uniknięciu problemów etycznych w ochronie zdrowia. Odpowiedzią instytucji międzynarodowych na wyzwania etyczne wynikające z rozwoju systemów SI są dwie ważne inicjatywy. 8 kwietnia 2019 roku Grupa Ekspertów ds. Sztucznej Inteligencji powołana przez Komisję Europejską (KE) przedstawiła dokument zatytułowany *Wytyczne etyczne dotyczące godnej zaufania sztucznej inteligencji* [24]. SI godną zaufania (*trustworthy AI*) zdefiniowano jako technologię, która przez cały cykl funkcjonowania zachowuje trzy atrybuty: jest zgodna z prawem, tj. zapewnia poszanowanie wszystkich obowiązujących przepisów ustawowych i wykonawczych; jest etyczna, tzn. zapewnia zgodność z zasadami i wartościami etycznymi; jest solidna zarówno z technicznego, jak i społecznego punktu widzenia. W dokumencie podkreślono, że systemy SI mogą wywoływać niezamierzone szkody nawet wówczas, gdy korzysta się z nich w dobrej wierze [24].

Z kolei Światowa Organizacja Zdrowia w raporcie z 2021 r. pt. *Etyka i zarządzanie sztuczną inteligencją dla zdrowia: Wytyczne ŚOZ* zaproponowała sześć zasad, które musi spełniać rozwiązanie oparte na SI, aby w sposób etyczny służyć poprawie jakości i bezpieczeństwa pacjentów (25). Należą do nich wymienione poniżej kwestie.

- Ochrona ludzkiej autonomii. Korzystanie z SI nie może naruszać niezależności człowieka, czyli prowadzić do sytuacji, gdy uprawnienia decyzyjne są powierzone systemom SI. Placówki medyczne powinny posiadać informacje niezbędne do bezpiecznego i skutecznego korzystania z systemów SI oraz rozumieć, jaką rolę takie systemy odgrywają w opiece zdrowotnej.
- Promowanie ludzkiego dobrostanu, bezpieczeństwa oraz interesu publicznego. Twórcy technologii SI powinni spełniać wymogi regulacyjne dotyczące bezpieczeństwa, skuteczności i jakości rozwiązań technologicznych. Systemy SI nie mogą powodować szkód psychicznych i fizycznych, których można byłoby uniknąć poprzez zastosowanie alternatywnej praktyki.
- Zapewnienie przejrzystości rozwiązań SI. Nowe technologie powinny być zrozumiałe dla twórców, pracowników medycznych, pacjentów i organów regulacyjnych. Ten wymóg dotyczy publikowania informacji przed zaprojektowaniem lub wdrożeniem technologii wystarczających do określenia sposobu prawidłowego i nieprawidłowego korzystania.
- Zapewnienie równego dostępu. Rozwiązania SI dla zdrowia powinny być zaprojektowane tak, aby nie wykluczać osób lub grup ze względu na wiek, płeć, dochód, pochodzenie etniczne, orientację seksualną, niepełnosprawność, przynależność do krajów o niższych dochodach lub inne cechy chronione na mocy kodeksów praw człowieka. Systemy SI nie powinny powielać uprzedzeń wobec możliwych do zidentyfikowania grup, zwłaszcza tych, które są marginalizowane.
- Promowanie responsywnych i zrównoważonych rozwiązań. Należy zapewnić możliwość określenia, czy narzędzie wykorzystujące SI reaguje w sposób adekwatny do sytuacji, zgodnie z uzasadnionymi oczekiwaniami i wymaganiami. Korzystanie z SI powinno być spójne z globalnymi wysiłkami na rzecz zmniejszenia wpływu człowieka na środowisko, ekosystemy i klimat. Zrównoważony rozwój wymaga współpracy między rządami, twórcami SI i innymi interesariuszami. Wspólnie muszą znaleźć rozwiązania, które pozwolą na wykorzystanie potencjału nowych technologii przy jednoczesnym minimalizowaniu ryzyka utraty miejsc pracy, również w sektorze zdrowia.
- Wspieranie odpowiedzialności. Ta zasada oznacza konieczność ustanowienia punktów nadzoru obsadzonych przez ludzi oraz mechanizmów umożliwiających dochodzenie roszczeń przez osoby i grupy, które doświadczyły negatywnych konsekwencji decyzji opartych na systemach SI (szerzej opisane w rozdziale „Odpowiedzialność za błędy i szkody medyczne w wyniku stosowania SI”).

Do głównych zadań etyków na obecnym etapie rozwoju technologii SI w ochronie zdrowia należy doprecyzowanie i wyjaśnienie znaczenia zasad etycznych oraz pomoc pracownikom naukowym i technicznym w transformacji tych zasad z poziomu międzynarodowego do poziomu instytucjonalnego, na przykład placówki medycznej [26]. Etycy powinni pomagać naukowcom w rozwiązywaniu konkretnych i szczegółowych problemów praktycznych. Aby zidentyfikować te problemy, odpowiednie podmioty, w tym instytucje naukowo-technologiczne i sektor przemysłu, powinny najpierw identyfikować i następnie

zarządzać ryzykiem wynikającym z korzystania z SI oraz wyjaśniać obowiązki każdego podmiotu w zakresie kontroli tego ryzyka [26].

Obecne i przyszłe regulacje dotyczące SI w UE powinny być ukierunkowane na zapewnienie bezpieczeństwa innowacyjnych technologii. Harmonizacja zasad ochrony danych i etyczności SI jest złożonym, ale pożądanym celem, szczególnie w zakresie usług opieki zdrowotnej i badań medycznych [27].

Odpowiedzialność za błędy i szkody medyczne w wyniku stosowania SI

Potencjał systemów opartych na SI w ochronie zdrowia umożliwia wprowadzenie innowacyjnych rozwiązań do praktyki klinicznej. Jednak ich implementacja wymaga dokładnej analizy istniejących ram prawnych oraz ustanowienia odpowiednich przepisów regulujących obszar granic odpowiedzialności dotyczących zastosowania SI w ochronie zdrowia [28].

Obecnie na gruncie prawa polskiego SI nadal nie została sklasyfikowana jako przedmiot bądź podmiot prawa, dlatego rodzi to problem w zakresie klasyfikacji skutków czynu dziejącego się przy jej użyciu. Trudność w ustaleniu strony odpowiedzialnej za skutek działania SI oraz ustalenie granic jej odpowiedzialności powoduje wątpliwości w określeniu ścieżki prawnej w przypadku wystąpienia błędu medycznego lub szkody wobec pacjenta. Dlatego też w polskim porządku prawnym istnieje kilka możliwości porządkujących kwestię odpowiedzialności SI w ochronie zdrowia [29].

Uznanie SI jako przedmiot umożliwiałoby ustalenie jej odpowiedzialności na zasadzie produktu wadliwego, jednak SI z uwagi na swoją innowacyjność i niewystępujące jak dotąd cechy produktów, takie jak autonomiczność, oraz pewną nieprzewidywalność działania odbiega od standardowych kryteriów kwalifikujących poszczególne rzeczy jako standardowe produkty [29]. Drugą możliwość stanowi uznanie SI jako podmiot prawa, co daje jej tym samym zdolność prawną, a w konsekwencji możliwość bycia stroną w ewentualnym postępowaniu [29]. Jednak w przypadku technologii SI podejmujących decyzje w sposób mechaniczny oraz wyuczony zgodnie z zaimplementowanymi danymi nie można jej w pełni kwalifikować jako podmiot działający w sposób samodzielny, co wywołuje tym samym skutek prawny [29].

Na terenie UE na mocy rezolucji Parlamentu Europejskiego z 16 lutego 2017 roku, zawierającej zalecenia w sprawie przepisów prawa cywilnego dotyczących medycyny, zostali wyszczególnieni operatorzy systemów SI, którzy zgodnie z rekomendacjami powinni ponosić odpowiedzialność opartą na winie (wymagającej udowodnienia lub domniemanej) [30]. W kwestii producentów systemów SI odpowiedzialność powinna obejmować sytuację, w której na skutek wystąpienia ryzyka nie istnieje możliwość zwolnienia się z odpowiedzialności za wyrządzoną szkodę, nawet przez wykazanie braku swojej winy. Jednak odpowiedzialność oparta na winie nie może dotyczyć systemu wykorzystującego SI z uwagi na sposób jego działania, który niekiedy jest nieprzewidywalny, oraz w sytuacji braku bezpośredniego wpływu na wynik działania systemu SI. W przypadku odpowiedzialności producenta na zasadzie ryzyka jest to możliwe jedynie wtedy, gdy podmiot (w przedmiotowym przypadku leczniczy) funkcjonuje przy użyciu sił przyrody[2], co w ochronie zdrowia na ogół nie występuje, ponieważ podstawowa działalność podmiotów leczniczych, taka jak udzielanie świadczeń zdrowotnych, realizowana jest za pośrednictwem personelu medycznego [31].

Wracając w rozważaniach do Polski, zwyczajowo, odpowiedzialność za wyrządzone szkody w ochronie zdrowia, takie jak błędy medyczne występujące podczas procesu diagnostyczno-leczniczego, jak dotąd w głównej mierze opierała się na zasadzie winy niż ryzyka [31]. Jednak oparcie kwestii odszkodowawczych na zasadzie winy w przypadku skutków działania systemu SI nie stanowi w pełni adekwatnego rozwiązania w ujęciu praktycznym, ponieważ w toku dochodzenia roszczeń to na pacjencie będzie ciążył obwiązek udowodnienia tej winy. Może to wówczas stanowić znaczącą trudność, a nawet niemożność udowodnienia nieprawidłowości wyrządzonych przez SI pacjentowi z uwagi na brak posiadanej wiedzy specjalistycznej w obszarze technologicznym i informatycznym. Problem braku biegłości w obrębie wspomnianych dziedzin może również dotyczyć osób reprezentujących pacjentów w postępowaniach sądowych i administracyjnych [32].

Opcjonalnie w zakresie stosowania SI w ochronie zdrowia istnieje możliwość zastosowania odpowiedzialności za produkt niebezpieczny. W takiej sytuacji to producent nadrzędnie staje się odpowiedzialny za stworzenie oprogramowania, które gwarantuje bezpieczeństwo jego użytkowników [31]. Ochroną zostaliby wówczas objęci zarówno pacjenci, jak i personel medyczny, a w sytuacji, gdy wytyczone standardy bezpieczeństwa nie zostaną spełnione i dojdzie do powstania jakiejkolwiek szkody, producent ponosiłby odpowiedzialność niezależnie od winy. Odpowiedzialność producentów może być determinowana ich bezpośrednim wpływem na dobór zbioru danych wykorzystywanych do uczenia poszczególnych systemów SI, a w konsekwencji precyzyjności i poprawności działania systemu SI. Dotyczy to kwestii zarówno związanych z procesem implementacji zbioru danych wejściowych systemu przed dopuszczeniem do użytkowania, jak i z nadzorem nad doskonaleniem pracy systemu SI. Takie rozwiązanie wydaje się korzystne zarówno dla pacjentów, jak i personelu medycznego, jednak producenci wówczas mogliby niechętnie podejmować się wytwarzania takich produktów z uwagi na zbyt duże ryzyko podczas powstania szkody i związane z tym kwestie odszkodowań [31].

Podmioty lecznicze potrzebują solidnego i dobrze zdefiniowanego systemu prawnego, aby móc w sposób jednoznaczny rozstrzygać spory w przypadku nieprawidłowych diagnoz lub błędów popełnionych na skutek zastosowania SI. Ustanowienie zrozumiałych przepisów prawnych jest kluczowe dla zabezpieczenia interesów pacjentów i placówek medycznych, zapewniając podstawę do uczciwego i sprawiedliwego rozstrzygania w przypadkach zdarzeń niepożądanych dziejących się z wykorzystaniem SI [33].

Regulacja stosowania SI w UE a sektor ochrony zdrowia

W związku z tym, że użycie systemów SI może budzić wątpliwości natury etycznej, Parlament UE 12 lipca 2024 r. opublikował rozporządzenie w sprawie SI (*Artificial Intelligence Act*, AIA)[3] [34]. Wybrane zapisy tego rozporządzenia weszły w życie 2 lutego 2025 r., natomiast całe rozporządzenie zacznie obowiązywać dopiero od 2 sierpnia 2026 r. [34].

Celem AIA jest zapewnienie odpowiednich warunków dla rozwoju i wykorzystania SI do usprawnienia opieki zdrowotnej, zapewnienia bezpieczniejszego i czystszego transportu, wydajniejszej produkcji oraz tańszej i bardziej zrównoważonej energii [34]. Rozporządzenie AIA wymaga, aby systemy SI wykorzystywane w różnych obszarach oceniać i klasyfikować zgodnie z ryzykiem, jakie stwarzają dla użytkowników. Poszczególne poziomy ryzyka wiążą się z koniecznością spełnienia określonych wytycznych [34].

Rozporządzenie ma zapewnić, że systemy SI wykorzystywane w UE będą bezpieczne, transparentne, identyfikowalne i niedyskryminujące. W AIA podkreślono również, że systemy SI nie powinny być w pełni autonomiczne, ale pozostawać pod nadzorem czynnika ludzkiego. Ma to zapobiec ewentualnym szkodliwym skutkom ich działania na populacjach i środowisku. Owe rozporządzenie przyczyniło się także do ustanowienia formalnej, neutralnej technologicznie i jednolitej definicji SI. Brzmi ona następująco:

> system SI oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne [34].

Według nowego rozporządzenia obowiązki twórców i dostawców zależą od poziomu ryzyka, jakie stwarza dana technologia SI. Systemy SI, które charakteryzują się „**niedopuszczalnym ryzykiem**", stwarzają zagrożenie dla społeczeństwa i są zakazane. Należą do nich rozwiązania, które stosują [34–35]:

- poznawczo-behawioralną manipulację w stosunku do pojedynczych osób lub grup wrażliwych (dzieci, seniorów). Przykładem mogą być zabawki aktywowane głosem, które zachęcają dzieci do niebezpiecznych zachowań;
- punktację społeczną (*social scoring*) do klasyfikowania ludzi na podstawie ich zachowań, statusu społeczno-ekonomicznego lub cech osobistych;
- identyfikację biometryczną w czasie rzeczywistym i na odległość, na przykład rozpoznawanie twarzy. W wyjątkowych sytuacjach systemy z tej kategorii mogą być użyte w celu ścigania poważnych przestępstw, ale tylko po zatwierdzeniu użycia takiego systemu przez sąd.

Systemy SI, które mogą negatywnie wpływać na bezpieczeństwo, zdrowie lub prawa podstawowe, zostały uznane za systemy „**wysokiego ryzyka**". Aby dany system zaliczyć do tej kategorii, musi on dotyczyć jednego z ośmiu obszarów określonych w AIA i podlega obowiązkowej rejestracji w specjalnym rejestrze stworzonym przez organy UE. Do tych obszarów należą: 1) biometryczna identyfikacja i kategoryzacja osób fizycznych (w dozwolonym zakresie); 2) zarządzanie i eksploatacja infrastruktury krytycznej; 3) edukacja i szkolenie zawodowe; 4) zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia; 5) dostęp i korzystanie z podstawowych usług prywatnych oraz publicznych; 6) ściganie przestępstw; 7) zarządzanie migracją, azylem i kontrolą granic; 8) pomoc w interpretacji i stosowaniu prawa [34]. Wszystkie systemy SI zakwalifikowane do kategorii „wysokiego ryzyka" powinny podlegać ocenie przed wprowadzeniem na rynek i przez cały okres ich funkcjonowania [34–35].

W rozporządzeniu wyróżniono również kategorię systemów SI o „**wymaganej przejrzystości**". Powinny one być na tyle transparentne, aby pozwolić użytkownikom na podejmowanie świadomych decyzji. Oczekuje się, że po interakcji z takimi systemami użytkownik powinien mieć prawo do podjęcia decyzji, czy chce nadal z nich korzystać. Użytkownicy powinni być świadomi tego, że wchodzą w interakcję ze SI. Do tej kategorii należą systemy generatywnej SI, np. ChatGPT, gdyż pozwalają one na generowanie lub manipulowanie treściami graficznymi, audio i wideo, w skrajnej postaci przyjmujące postać zjawiska *deepfake*[4] [34, 36]. Minimalne wymogi przejrzystości oznaczają, że wygenerowane treści powinny być oznaczone jako stworzone przez SI. Natomiast system musi zawierać mechanizmy, które blokują tworzenie nielegalnych materiałów. Ponadto powinna być dostępna informacja o tym, jakie dane chronione prawem autorskim wykorzystano do uczenia systemu SI [34].

W przypadku niektórych systemów SI nie będzie obowiązku ich monitorowania. Dotyczy to systemów użytych w grach wideo i w filtrach antyspamowych w skrzynkach mailowych. Według KE obecnie zdecydowana większość systemów SI używanych na terenie UE należy do tej kategorii [34–35].

Według zapisów AIA oprogramowanie SI w wyrobach medycznych[5] będzie należeć do kategorii „wysokiego ryzyka" [37]. Takie produkty są rozumiane jako narzędzia, aparatura, urządzenia, oprogramowanie, implanty, odczynniki, materiały lub inne artykuły przewidziane przez producenta do stosowania – pojedynczo lub łącznie – u ludzi do wspierania, diagnozowania, profilaktyki, leczenia choroby / niepełnosprawności / stanu fizjologicznego oraz dostarczania informacji poprzez badanie in vitro [37]. Obecnie wyroby medyczne podlegają dwóm rozporządzeniom: nr 2017/745 [37] i nr 2017/746 [38]. Przepisy tych rozporządzeń określają zasady, w jaki sposób należy tworzyć i korzystać z wyrobów medycznych, oraz nakładają obowiązek testowania tych urządzeń przed wprowadzeniem na rynek. Część aktywności monitorujących powinna być realizowana również po dopuszczeniu do obrotu w celu oceny występowania zdarzeń niepożądanych [37–38].

Zdaniem niektórych ekspertów proponowana w AIA ocena systemów SI może prowadzić do zbyt pochopnej klasyfikacji wielu programów zainstalowanych w wyrobach medycznych jako systemy „wysokiego ryzyka",

nawet jeśli są to produkty niestwarzające zagrożenia dla podstawowych praw, zdrowia i bezpieczeństwa [39]. Stąd propozycje modyfikacji schematu klasyfikacji ryzyka dla systemów SI tak, aby można było wykrywać istotne zagrożenia dla wspomnianych wartości. Rozwiązaniem może być dodanie niektórych kategorii systemów medycznych do wykazu systemów „wysokiego ryzyka" oraz określenie zasad klasyfikacji specyficznych dla SI już na poziomie oceny wyrobów medycznych. Przykładowo do takiej kategorii powinny trafić „chatboty terapeutyczne"[6], których używanie może nieść ze sobą pewne zagrożenia zdrowotne w przypadku błędnych porad [40–41].

Należy dodać, że również rozporządzenie o ochronie danych osobowych (RODO) w pewnym stopniu odnosi się do systemów SI wykorzystywanych w ochronie zdrowia [13]. W obecnej formie RODO zakazuje stosowania systemów opierających się na zautomatyzowanym podejmowaniu decyzji, na przykład systemów automatycznie uruchamiających wypis pacjenta ze szpitala bez konieczności akceptacji przez personel medyczny albo profilujących pacjentów na podstawie danych medycznych w celu przewidywania wystąpienia chorób. Wyjątkiem są systemy, na których zastosowanie pacjent wyraził świadomą zgodę, lub systemy działające w interesie publicznym [13]. Dodatkowo RODO nakłada na twórców systemów elektronicznych (w tym systemów SI) obowiązek ochrony danych osobowych i projektowania ich w taki sposób, aby zapewnić prywatność danych pacjentów [13].

Rekomendacje Parlamentu UE w sprawie robotyki[7] kładą nacisk na rozwój technologii, które mają wspierać pracę personelu medycznego, a nie zastępować go rozwiązaniami, takimi jak te oparte na SI [30]. Dlatego też wszelkie innowacje wprowadzane do sektora ochrony zdrowia należy implementować w sposób zapewniający sprawowanie kontroli ludzkiej nad technologią SI, szczególnie tej dostarczającej wyniki diagnostyczne bądź wspomagającej proces leczniczy pacjenta [30].

Nieuregulowanym obszarem pozostaje raportowanie wykorzystania medycznej SI [42]. Innowacje medyczne przed wprowadzeniem do praktyki klinicznej muszą przejść rygorystyczny proces oceny, a potrzeby regulacyjne odgrywają kluczową rolę w tym procesie. Duża różnorodność typów zbiorów danych i zadań realizowanych przez SI w różnych obszarach ochrony zdrowia stanowi istotne wyzwanie podczas opracowywania wytycznych w tej dziedzinie. Wyniki metaanalizy przygotowanej przez Kolbingera i współpracowników wskazują, że większość obecnych wytycznych dotyczących raportowania wykorzystania SI została opracowana z pominięciem sformalizowanego procesu [42]. Ponadto duża ich część dotyczyła raportowania badań przedklinicznych i translacyjnych[8], a nie walidacji klinicznych systemów [43]. Wreszcie, nadal część naukowych czasopism medycznych i informatycznych o wysokim wskaźniku oddziaływania nie wymaga przestrzegania jakichkolwiek wytycznych podczas opracowania wyników uzyskanych za pomocą SI [42].

Aspekty prawne stosowania SI w ochronie zdrowia w Polsce

Dynamiczny rozwój nowych technologii z wykorzystaniem SI w ochronie zdrowia jest zauważalny również w Polsce [44]. Możliwość implementacji systemów wykorzystujących SI w polskiej ochronie zdrowia dotyczy zwiększenia jakości udzielanych świadczeń zdrowotnych oraz odciążenia personelu medycznego od czynności administracyjnych, dzięki czemu będą mogli przeznaczyć więcej czasu dla pacjentów [44]. SI może również wesprzeć sektor farmaceutyczny w produkcji leków generycznych, których Polska jest ważnym producentem, oraz w personalizacji procesu leczniczego na podstawie zgromadzonych danych pacjentów [44].

Pewnych wskazówek, w jaki sposób lekarze mogą wykorzystywać SI w praktyce klinicznej w Polsce, dostarcza Kodeks Etyki Lekarskiej (KEL). W art. 12 KEL zostały określone zasady korzystania ze SI w trakcie procesu diagnostyczno-leczniczego oraz wymogi informacyjne, które wskazują na obowiązek lekarza o poinformowaniu pacjenta, że przy stawianiu diagnozy będzie wykorzystana SI.

Zgodnie z KEL, zanim pacjent zgodzi się na leczenie z użyciem SI, musi zrozumieć, jak ta technologia będzie wykorzystana w jego przypadku, i wyrazić świadomą zgodę na jej zastosowanie. Ponadto dopuszczone jest stosowanie wyłącznie rozwiązań bazujących na narzędziach SI, które w sposób poprawny przeszły proces certyfikacji wyrobów medycznych, z zastrzeżeniem, że ostateczną decyzję w zakresie diagnozy bądź wytyczonej terapii podejmuje każdorazowo lekarz [45].

W Polsce drogą ustawy z 7 kwietnia 2022 r. o wyrobach medycznych uregulowano stosowanie oprogramowania (także systemów SI) i zakwalifikowano je jako wyrób medyczny [46]. Skutkuje to obowiązkiem stosowania tożsamych wymogów i procedur wobec oprogramowania wykorzystującego SI jak te, którym podlega aparatura medyczna. Określone wymagania polegają głównie na prowadzeniu okresowej lub doraźnej obsługi serwisowej, konieczności aktualizacji oprogramowania oraz wykonywania obowiązkowych przeglądów technicznych [46].

Jednym z istotnych aspektów prawnych jest również obowiązek zapewnienia ochrony danych osobowych przetwarzanych przez systemy oparte na SI wykorzystywane w podmiotach leczniczych. Powinno się to odbywać zgodnie z przepisami ustawy z 10 maja 2018 r. o ochronie danych osobowych [47]. Kluczowe jest tutaj zabezpieczenie danych w aspekcie technicznym, informatycznym oraz organizacyjnym. Zabezpieczenia techniczne i informatyczne mają na celu zabezpieczenie dostępu do danych zawartych bezpośrednio w systemach SI przez osoby nieuprawnione i uniknięcie naruszeń ich bezpieczeństwa, natomiast zabezpieczenie danych o charakterze organizacyjnym uwzględnia stworzenie reguł i określenie procedur postępowania w podmiocie leczniczym w związku z przetwarzaniem danych osobowych, które następuje w przypadku przesyłania danych pomiędzy poszczególnymi systemami wykorzystującymi SI [47].

W literaturze można napotkać propozycje ustanowienia odpowiednich przepisów dotyczących działań

kontrolujących SI w Polsce. Według Zalewskiej nadzór nad urządzeniami medycznymi wykorzystującymi SI powinien być sprawowany przez wykwalifikowane osoby posiadające interdyscyplinarne kwalifikacje w zakresie inżynierii klinicznej oraz informatyki [6]. Ponadto monitorowanie wdrożonych rozwiązań SI powinno przebiegać przy ścisłej współpracy pomiędzy jednostkami klinicznymi, organami regulacyjnymi i producentami rozwiązań wykorzystujących SI. Jednocześnie w toku współpracy instytucje zaangażowane w monitorowanie i nadzór powinny wspólnie gromadzić i archiwizować dane w zakresie działania SI, aby następnie możliwa była ich analiza w przydatku wystąpienia zdarzeń niepożądanych [48].

Przepisy prawne obowiązujące w Polsce jak dotąd tylko w ograniczony sposób odnoszą się do implementacji systemów opartych na SI w ochronie zdrowia. Brakuje regulacji, które pozwalałaby na finansowanie ze środków publicznych świadczeń zdrowotnych udzielonych bezpośrednio przez urządzenia wykorzystujące systemy SI [49].

Ministerstwo Cyfryzacji prowadzi prace umożliwiające stosowanie na gruncie prawa krajowego przepisów z AIA [50]. W październiku 2024 roku wspomniane ministerstwo opublikowało projekt ustawy o systemach SI oraz przeprowadziło konsultacje publiczne. W efekcie zgłoszono ponad dwa tysiące uwag i propozycji zmian. Najistotniejsze zmiany ujęte w projekcie ustawy obejmują powołanie nowego organu nadzoru, który sprawowałby kontrolę nad rynkiem wykorzystującym systemy oparte na SI, umożliwiając składanie skarg za naruszenie przepisów zwłaszcza w kwestii praktyk zakazanych. Wskazano również ministra właściwego do spraw informatyzacji jako organu odpowiedzialnego za notyfikowanie jednostek oceniających zgodność systemów SI oraz uwzględniono możliwość nakładania kar administracyjnych za ewentualne naruszenie przepisów [51].

Podsumowanie

Zastosowanie SI w ochronie zdrowia rodzi wiele wątpliwości natury etycznej. Jak się wydaje, rozwiązania oparte na SI mogą powielać nierówności mające odzwierciedlenie w zbiorach danych używanych do ich modelowania. Podejmowane są inicjatywy na rzecz zagwarantowania etyki rozwiązań SI. Istotną inicjatywą jest propozycja zasad mających poprawić jakość i bezpieczeństwo rozwiązań wykorzystujących SI w ochronie zdrowia, opracowana przez Światową Organizację Zdrowia. Ewolucja systemów SI wymaga współpracy wszystkich interesariuszy oraz zastosowania takich rozwiązań w ochronie zdrowia, które umożliwią jej właściwe nadzorowanie. Obecnie systemy SI są już wykorzystywane w wielu obszarach ochrony zdrowia, jednak brakuje przejrzystych regulacji określających granice odpowiedzialności za decyzje podjęte przez systemy autonomiczne SI oraz te, które dostarczają wartości diagnostycznych służących podejmowaniu decyzji klinicznych przez personel medyczny. Wykorzystanie SI na terenie UE będzie podlegało zasadom określonym w AIA. Kładzie się w nim nacisk na klasyfikację ryzyka, jakie niesie ze sobą stosowanie różnych systemów SI. Oprogramowanie opierające się na SI stosowane w wyrobach medycznych zostało zakwalifikowane do kategorii „wysokiego ryzyka". Obowiązujące w Polsce powszechne przepisy tylko w ograniczonym jak dotąd zakresie umożliwiają implementację SI w praktyce klinicznej i nie odnoszą się szczegółowo do możliwości publicznego finansowania świadczeń zdrowotnych realizowanych ze wsparciem systemów SI.

Przypisy końcowe

1 Powtarzalność oznacza otrzymanie tego samego wyniku przy użyciu tej samej metody, natomiast odtwarzalność to zgodność pomiarów wykonanych przez różne osoby.
2 Procesy polegające na przetwarzaniu energii elementarnej (energii elektrycznej, pary, paliwa, gazu itp.) na pracę lub inne postacie energii, co wymaga użycia maszyn i innych urządzeń przetwarzających (art. 435 kc).
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 (akt w sprawie sztucznej inteligencji).
4 Dowolne materiały elektroniczne, szczególnie wideo, które zostały zmanipulowane cyfrowo w celu przekonującego zastąpienia podobieństwa jednej osoby podobizną innej osoby.
5 Dla wyrobów medycznych klasy IIa lub wyższej – klasyfikacja pochodzi z rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych.
6 „Chatboty terapeutyczne" wykorzystują SI do śledzenia nastroju i intensywności objawów, takich jak lęk, oraz podejmowania odpowiednich działań interwencyjnych w przypadku pogorszenia stanu emocjonalnego użytkownika.
7 Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (Dz. U. UE C z dnia 18 lipca 2018 r.).
8 Oznaczających przeniesienie wyników badania „od stołu laboratoryjnego do łóżka chorego".

Piśmiennictwo

1. Romaszewski A., Jakubowski S., Duplaga M., *Informatyzacja systemu ochrony zdrowia – problemy i wyzwania. Część I*, „Zdrowie Publiczne i Zarządzanie" 2024; 20 (4): 148–153.
2. Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej. Nr 52021PC0281.
3. Petersson L., Larsson I., Nygren J.M., Nilsen P., Neher M., Reed J.E. et al, *Challenges to Implementing Artificial Intelligence in Healthcare: a Qualitative Interview Study with Healthcare Leaders in Sweden*, „BMC Health Services Research" 2022; 22 (1): 1–16.
4. OECD, *Explanatory Memorandum on the Updated OECD Definition of an AI System*, „OECD Artificial Intelligence Papers" 2024; 8: 1–11.
5. Amisha M.P., Pathania M., Rathaur V.K., *Overview of Artificial Intelligence in Medicine*, „ Journal of Family Medicine and Primary Care" 2019; 8 (7): 2328–2331.
6. Zalewska E., *Sztuczna inteligencja w inżynierii klinicznej – postęp i wyzwania*, „Inżynier i Fizyk Medyczny" 2023; 12 (1): 13–17.
7. Sutton R.T., Pincock D., Baumgart D.C., Sadowski D.C., Fedorak R.N., Kroeker K.I., *An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success*, „NPJ Digital Medicine" 2020; 3 (1): 1–17.
8. Bajwa J., Munir U., Nori A., Williams B., *Artificial Intelligence in Healthcare: Transforming the Practice of Medicine*, „Future Healthcare Journal" 2021; 8 (2): e188–194.
9. Islam M.M., Yang H.C., Poly T.N., Jian W.S., (Jack) Li Y.C., *Deep Learning Algorithms for Detection of Diabetic Retinopathy in Retinal Fundus Photographs: A Systematic Review and Meta-Analysis*, „Computer Methods and Programs in Biomedicine" 2020; 191; 105320: 1–16.
10. Gulshan V., Peng L., Coram M., Stumpe M.C., Wu D., Narayanaswamy A. et al., *Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs*, „Journal of the American Medical Association" 2016; 316 (22): 2402–2410.
11. Patrzyk S., Woźniacka A., *Sztuczna inteligencja w medycynie*, t. 6, Wydawnictwo Uniwersytetu Medycznego w Łodzi, Łódź 2022: 1–30.
12. Cambridge Dictionary, *algorithm*, https://dictionary.cambridge.org/dictionary/english/algorithm (dostęp: 19.06.2024).
13. 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; tekst mający znaczenie dla EOG). Nr 32016R0679.
14. Rajpurkar P., Chen E., Banerjee O., Topol E.J., *AI in Health and Medicine*, „Nature Medicine" 2022; 28 (1): 31–38.
15. Rejmaniak R., *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Roczniki Nauk Prawnych" 2021; 31 (3): 95–113.
16. Kusznieruk P., Zemke-Górecka A., *Aspekty i ramy prawne sztucznej inteligencji na gruncie prawa Unii Europejskiej. Część 2*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024; 1–2: 129–140.
17. Larrazabal A.J., Nieto N., Peterson V., Milone D.H., Ferrante E,. *Gender Imbalance in Medical Imaging Datasets Produces Biased Classifiers for Computer-Aided Diagnosis*, „Proceedings of the National Academy of Sciences of the United States of America" 2020; 117 (23): 12592–12594.
18. Obermeyer Z., Powers B., Vogeli C., Mullainathan S., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, „Science" 2019; 366 (6464): 447–453.
19. Beam A.L., Manrai A.K., Ghassemi M., *Challenges to the Reproducibility of Machine Learning Models in Health Care*, „Journal of the American Medical Association" 2020; 323 (4): 305–306.
20. Liu C., Grundy J., Yang X., Gao C., Xia X., Lo D. et al., *On the Reproducibility and Replicability of Deep Learning in Software Engineering*, „ACM Transactions on Software Engineering and Methodology" 2021; 31 (1): 1–46.
21. StatSoft, *Poradnik statystyczny*, https://www.statsoft.pl/textbook/stathome_stat.html?https%3A%2F%2Fwww.statsoft.pl%2Ftextbook%2Fadvans8.html (dostęp: 27.01.2025).
22. Morley J., Machado C., Burr C., Cowls J., Taddeo M., Floridi L., *The Debate on the Ethics of AI in Health Care: A Reconstruction and Critical Review*, „SSRN Electronic Journal" 2019: 1–35.
23. Lee C.S., Lee A.Y., *Clinical Applications of Continual Learning Machine Learning*, „The Lancet Digital Health" 2020; 2 (6): e279–281.
24. Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (dostęp: 28.06.2024).
25. World Health Organization, *Ethics and Governance of Artificial Intelligence for Health*, vol. 1, 2021, https://www.who.int/publications/i/item/9789240029200 (dostęp: 19.06.2024).
26. Zhang J., Zhang Z.M., *Ethics and Governance of Trustworthy Medical Artificial Intelligence*, „BMC Medical Informatics and Decision Making" 2023; 23 (1): 1–15.
27. Meszaros J., Minari J., Huys I., *The Future Regulation of Artificial Intelligence Systems in Healthcare Services and Medical Research in the European Union,* „Frontiers in Genetics" 2022; 13; 927721: 1–10.
28. Mennella C., Maniscalco U., De Pietro G., Esposito M., *Ethical and Regulatory Challenges of AI Technologies in Healthcare: A Narrative Review*, „Heliyon" 2024; 10(4); e26297: 1–20.
29. Kusznieruk P., Zemke-Górecka A., *Aspekty prawne sztucznej inteligencji na gruncie prawa Unii Europejskiej. Część 1*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2024; 4: 63–81.
30. Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103, INL).
31. Bączyk-Rozwadowska K., *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego" 2022; 3 (3–4): 5–35.

32. Kaczan D., *Odpowiedzialność odszkodowawcza za funkcjonowanie sztucznej inteligencji w medycynie*, „Annales Universitatis Paedagogicae Cracoviensis. Studia de Cultura" 2022; 14 (2): 145–160.
33. Bindra S., Jain R., *Artificial Intelligence in Medical Science: a Review*, „Irish Journal of Medical Science" 2024; 193 (3): 1419–1429.
34. 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). Nr 32024R1689.
35. *Regulatory Framework Proposal on Artificial Intelligence. Shaping Europe's Digital Future*, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (dostęp: 18.12.2023).
36. Oxford English Dictionary, *Deepfake*, 2023, https://www.oed.com/dictionary/deepfake_n?tl=true (dostęp: 18.12.2023).
37. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Tekst mający znaczenie dla EOG). Nr 32017R0745.
38. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Tekst mający znaczenie dla EOG). Nr 32017R0746.
39. Quaranta M., Amantea I.A., Grosso M., *Obligation for AI Systems in Healthcare: Prepare for Trouble and Make it Double?*, „The Review of Socionetwork Strategies" 2023; 17 (2): 275–295.
40. Hauglid M.K., Mahler T., *Doctor Chatbot: The EU's Regulatory Prescription for Generative Medical AI*, „Oslo Law Review" 2023; 10 (1): 1–23.
41. Kubecka A., Książek J., Styła R., *Przyszłość nowych technologii w diagnozie psychologicznej i psychoterapii. Analiza jakościowa na podstawie metody delfickiej*, „Psychiatria" 2021; 18 (4): 275–281.
42. Kolbinger F.R., Veldhuizen G.P., Zhu J., Truhn D., Kather J.N., *Reporting Guidelines in Medical Artificial Intelligence: a Systematic Review and Meta-Analysis*, „Communications Medicine" 2024; 4 (1): 1–10.
43. Żaczek A., Budyńko Ł., *Specyfika Translational Research*, https://poradnik-naukowy.gumed.edu.pl/42023.html (dostęp: 2.07.2024).
44. Ministerstwo Cyfryzacji, *Ekspertyza ws. aktualizacji Polityki AI w Polsce*, 2024, https://www.gov.pl/web/cyfryzacja/ekspertyza--ws-aktualizacji-polityki-ai-w-polsce (dostęp: 27.01.2025).
45. Naczelna Izba Lekarska, *Kodeks Etyki Lekarskiej. Załącznik do uchwały nr 5 Nadzwyczajnego XVI Krajowego Zjazdu Lekarzy z dnia 18 maja 2024 r.*
46. Ustawa z dnia 7 kwietnia 2022 r. o wyrobach medycznych. Dz.U. 2022, poz. 974.
47. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018, poz. 1000.
48. Bajwa J., Munir U., Nori A., Williams B., *Artificial Intelligence in Healthcare: Transforming the Practice of Medicine*, „Future Healthcare Journal" 2021; 8 (2): e188–194.
49. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Dz.U. 2004 nr 210, poz. 2135.
50. Ministerstwo Cyfryzacji, *Europejski AI Act opublikowany*, 2024, https://www.gov.pl/web/cyfryzacja/europejski-ai-act-opublikowany (dostęp: 31.07.2024).
51. Projekt ustawy o systemach sztucznej inteligencji, 2024, https://legislacja.rcl.gov.pl/projekt/12390551/katalog/13087901 (dostęp: 27.01.2025).