

E-administracja

**Wyzwania
dla cyfrowych
usług publicznych
w Unii Europejskiej**

E-Government

**Challenges
for Digital
Public Services
in the EU**

REDAKCJA / EDITED BY

Sławomir Dudzik · Inga Kawka · Renata Śliwa

Krakow Jean Monnet Research Papers



E-administracja

E-Government

**Wyzwania
dla cyfrowych
usług publicznych
w Unii Europejskiej**

**Challenges
for Digital
Public Services
in the EU**

Krakow Jean Monnet Research Papers

3

E-administracja E-Government

Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej Challenges for Digital Public Services in the EU

REDAKCJA / EDITED BY

Sławomir Dudzik • Inga Kawka • Renata Śliwa



Kraków 2024

Sławomir Dudzik 
Uniwersytet Jagielloński, Kraków
✉ s.dudzik@uj.edu.pl

Inga Kawka 
Uniwersytet Jagielloński, Kraków
✉ inga.kawka@uj.edu.pl

Renata Śliwa 
Uniwersytet Komisji Edukacji Narodowej, Kraków
✉ renata.sliwa@up.krakow.pl

© Copyright by individual authors and Księgarnia Akademicka, 2024

Recenzja: dr hab. Grzegorz Krawiec, prof. UKEN

Opracowanie redakcyjne: Artur Foryt (j. francuski), Dorota Ilnicka (j. polski), Christopher Thornton (j. angielski)

Projekt okładki: Marta Jaszczyk

ISBN 978-83-8368-025-5
<https://doi.org/10.12797/9788383680255>

Publikacja dofinansowana przez Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego oraz Uniwersytet Komisji Edukacji Narodowej w Krakowie

With the support of Jean Monnet Activities within ERASMUS+ Programme of the European Union



Wsparcie Komisji Europejskiej dla produkcji tej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie może zostać pociągnięta do odpowiedzialności za jakiegokolwiek wykorzystanie informacji w niej zawartych.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl

Księgarnia internetowa: akademicka.pl

SPIS TREŚCI | TABLE OF CONTENTS

Słowo wstępne	7
---------------------	---

CZĘŚĆ I

OCHRONA UNIJNYCH WARTOŚCI I PRAW PODSTAWNYCH JAKO ODPOWIEDŹ NA RYZYKO ZWIĄZANE Z CYFRYZACJĄ USŁUG PUBLICZNYCH

CHRISTINE MENGÈS-LE PAPE

Immigration en France : garanties et risques des procédures administratives et judiciaires dématérialisées. Migration et e-administration en France.....	13
---	----

MARTA GRABOWSKA

Cyfryzacja administracji publicznej w Unii Europejskiej w świetle <i>Berlin Declaration on Digital Society and Value-Based Digital Government, 2020</i>	29
---	----

KINGA SABINA ZIELIŃSKA

E-administracja działająca w granicach prawa i godna zaufania. Prawo do prywatności i ochrona danych osobowych jako wyzwanie dla rozwoju e-administracji	45
---	----

CZĘŚĆ II

INKLUZYWNE CYFROWE USŁUGI PUBLICZNE

PART I

PROTECTING EU VALUES AND FUNDAMENTAL RIGHTS IN RESPONSE TO RISKS ASSOCIATED WITH THE DIGITIZATION OF PUBLIC SERVICES

PART II

INCLUSIVE DIGITAL PUBLIC SERVICES

INGA KAWKA

Włączenie cyfrowe w prawie Unii Europejskiej	67
--	----

AGATA CEBERA

Wykluczenie cyfrowe osób starszych a rozwój e-usług w administracji w Polsce	87
--	----

JAKUB GRZEGORZ FIRLUS

Dostępność cyfrowa jako standard e-usług polskiej administracji publicznej – zarys problemu.....	107
---	-----

TOMASZ KOSICKI

Publiczna usługa hybrydowa jako instrument przeciwdziałania wykluczeniu cyfrowemu i usprawniania ogólnego postępowania administracyjnego – wybrane zagadnienia	131
--	-----

CZĘŚĆ III

PERSPEKTYWY ROZWOJU CYFROWYCH USŁUG PUBLICZNYCH W EUROPIE

MIOMIRA P. KOSTIĆ

Development of Smart Cities and On-line Public Services Due to Quality
of the Citizens' Criminal Policy Protection..... 153

IRYNA FYSHCHUK

Strengthening Municipalities' Resilience against Cyber Attacks in Ukraine..... 171

AGNIESZKA KASTELIK-SMAZA

Sztuczna inteligencja w edukacji – szanse, zagrożenia, ramy prawne..... 189

RENATA ŚLIWA

Infrastructure-driven Approach to Digital Transition..... 215

YULIIA VOLKOVA, YULIIA LEHEZA

Digitalization of the Environmental Protection..... 229

PART III

PROSPECTS FOR THE DEVELOPMENT OF DIGITAL PUBLIC SERVICES IN EUROPE

CZĘŚĆ IV

WYZWANIA DLA ROZWOJU E-USŁUG PUBLICZNYCH W POLSCE

PIOTR RUCZKOWSKI

Cyfryzacja administracji na przykładzie projektowanych zmian w przepisach
o cmentarzach i chowaniu zmarłych..... 253

TOMASZ GRZYBOWSKI, JACEK JAŚKIEWICZ

E-formalizm procedur jurysdykcyjnych w perspektywie zasady zaufania do władzy
publicznej..... 263

MONIKA KAWCZYŃSKA

The Access to Open Data and Re-use of Public Sector Information:
The Polish Perspective..... 281

AGATA NODŹAK

Informatyzacja administracyjnego postępowania egzekucyjnego i jej wpływ
na skuteczność egzekucji administracyjnej..... 301

ALEKSANDRA SOŁTYSIŃSKA

Digitalization of Appeal Proceedings in Public Procurement in Poland..... 325

ALAN BEROUD

E-działania w obszarze wsparcia przewozu pasażerskiego na przykładzie
Szybkiej Kolei Miejskiej w Warszawie..... 345

PART IV

CHALLENGES IN THE DEVELOPMENT OF PUBLIC E-SERVICES IN POLAND

Indeks osób..... 359

AGNIESZKA KASTELIK-SMAZA¹

SZTUCZNA INTELIGENCJA W EDUKACJI – SZANSE, ZAGROŻENIA, RAMY PRAWNE

ABSTRAKT: Przedmiotem opracowania jest analiza wybranych kwestii dotyczących zastosowania sztucznej inteligencji w edukacji, płynących z tego szans, a także propozycji unijnych ram prawnych, będących odpowiedzią na potencjalne zagrożenia.

Systemy sztucznej inteligencji mogą odegrać ważną rolę w unowocześnieniu edukacji, prowadząc do poprawy jakości kształcenia i zwiększenia jego dostępności dla odbiorców. Mogą także sprzyjać włączeniu społecznemu, w szczególności w zakresie kształcenia osób z mniejszych miejscowości, niepełnosprawnych czy z innych względów zagrożonych wykluczeniem.

Jednocześnie wykorzystywanie sztucznej inteligencji i danych może mieć negatywny wpływ na szereg praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej. Proponowane na poziomie Unii Europejskiej regulacje prawne mają na celu uwzględnienie różnych źródeł ryzyka i zagwarantowanie wysokiego poziomu ochrony praw podstawowych wobec systemów AI. Służy temu w szczególności sformułowanie zestawu wymogów dotyczących wiarygodnej sztucznej inteligencji oraz proporcjonalnych obowiązków nałożonych na wszystkich uczestników obrotu.

Projektowane uregulowania mogą generować obciążenie dla szkół, które z jednej strony będą zmagać się z opanowaniem zastosowania nowych technologii w procesie edukacji, a z drugiej – z wypełnieniem licznych obowiązków prawnych.

¹ Dr Agnieszka Kastelik-Smaza, adwokat, wykładowca szkolenia aplikantów adwokackich Izby Adwokackiej w Bielsku-Białej.

SŁOWA KLUCZOWE: sztuczna inteligencja, edukacja cyfrowa, prawa podstawowe, prawo do kształcenia, zasada niedyskryminacji, włączenie społeczne

ARTIFICIAL INTELLIGENCE IN EDUCATION – OPPORTUNITIES, THREATS, LEGAL FRAMEWORK

ABSTRACT: The subject of this paper is an analysis of selected issues concerning the application of artificial intelligence in education, the opportunities arising therefrom, as well as proposals for an EU legal framework in response to potential threats.

Artificial intelligence systems can play an important role in the modernization of education, leading to an improvement in the quality of education and making it more accessible to the public. They can also foster social inclusion, particularly in the education of people from smaller towns, people with disabilities or otherwise being at risk of exclusion.

At the same time, the use of artificial intelligence and data may have a negative impact on a number of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. Proposed regulations at the European Union level aim to address various sources of risk and guarantee a high level of protection of fundamental rights against AI systems. This is particularly served by a set of requirements for reliable artificial intelligence and proportionate obligations imposed on all participants concerned.

The proposed regulations may generate a burden for schools, which will struggle to master the application of new technologies in the educational process on the one hand, and to fulfill numerous legal obligations on the other.

KEYWORDS: artificial intelligence, digital education, fundamental rights, right to education, principle of non-discrimination, social inclusion

1. Wprowadzenie

Przedmiotem niniejszego opracowania jest analiza wybranych kwestii dotyczących zastosowania sztucznej inteligencji (dalej także: AI) w edukacji, płynących z tego szans, a także propozycji unijnych ram prawnych, będących odpowiedzią na potencjalne zagrożenia.

Sztuczna inteligencja od wielu lat jest już obecna w naszym codziennym życiu, często w sposób niezauważalny. Opierają się na niej wyszukiwarki internetowe, tłumacze, chatboty, wirtualni asystenci czy pojazdy autonomiczne. Wykorzystują ją także sklepy internetowe w swoich strategiach marketingowych. Ponadto podejmuje się coraz więcej działań zmierzających do rozwiązania przy jej pomocy istotnych problemów

gospodarczych czy społecznych, takich jak wczesne diagnozowanie i leczenie chorób, zapobieganie wypadkom na drogach czy zmianom klimatycznym, zapewnienie cyberbezpieczeństwa, wprowadzenie uprawnień w rolnictwie².

Także w dziedzinie edukacji dyskusja na temat sztucznej inteligencji toczy się już od jakiegoś czasu. Niewątpliwie jedną z przyczyn jej zintensyfikowania stało się uruchomienie serwisu internetowego o nazwie ChatGPT, który w krótkim czasie podbił serca młodzieży szkolnej na całym świecie, stając się chętnie wykorzystywaną pomocą w odrabianiu zadań domowych czy pisaniu wypracowań³.

Komisja Europejska zwróciła uwagę, że:

[...] sztuczna inteligencja ma ogromny potencjał, by zmienić kształcenie i szkolenie dla uczniów, nauczycieli i pracowników szkół. Może pomóc uczniom z trudnościami w uczeniu się i wspierać nauczycieli poprzez nauczanie zindywidualizowane. Jednak wykorzystanie sztucznej inteligencji i danych wiąże się z zagrożeniami dla prywatności, bezpieczeństwa i ochrony, zwłaszcza w przypadku młodych ludzi⁴.

Zastosowanie w praktyce sztucznej inteligencji w edukacji na masową skalę, które wyprzedziło opracowanie właściwych ram prawnych w celu zapobiegania zagrożeniom dla uczniów, nauczycieli i całego systemu kształcenia, staje się niewątpliwie wyzwaniem dla prawodawców unijnych i krajowych oraz dla podmiotów będących uczestnikami tego systemu, jego organizatorami oraz organami nadzoru.

2. Czym jest sztuczna inteligencja?

Rozważając problematykę dotyczącą stosowania systemów sztucznej inteligencji w edukacji, należy w pierwszej kolejności zdefiniować przedmiot tychże rozważań. Warto podkreślić, że w projektowanych obecnie aktach prawnych oraz w dokumentach przygotowywanych przez różne instytucje i organizacje można znaleźć odmienne definicje systemów sztucznej inteligencji. Wynika to z faktu, że rozwiązania oparte

² Komunikat Komisji, *Sztuczna inteligencja dla Europy*, Bruksela, dnia 25.04.2018 r., COM(2018) 237 final.

³ Por. „Sztuczna Inteligencja w edukacji”. Wywiad... ze Sztuczną Inteligencją, https://elearning.uj.edu.pl/aktualnosci/-/journal_content/56_INSTANCE_VYFRNklOU5HR/153579096/153958753 (5.01.2024); *Chat GPT w szkole. Szanse i zagrożenia*, Zintegrowana Platforma Edukacyjna Ministerstwa Edukacji i Nauki, <https://zpe.gov.pl/chat-gpt> (15.06.2023).

⁴ Wypowiedź komisarz do spraw innowacji, badań naukowych, kultury, edukacji i młodzieży Marii Gabriel w artykule *Sztuczna inteligencja w szkole*, https://poland.representation.ec.europa.eu/news/sztuczna-inteligencja-w-szkole-2022-10-26_pl (15.06.2023).

na sztucznej inteligencji podlegają ciągłemu i bardzo szybkiemu rozwojowi oraz znajdują zastosowania w coraz to nowszych narzędziach, produktach czy usługach. Nie jest zatem łatwo sformułować definicję, która byłaby odporna na nieustający postęp technologiczny.

W projekcie Aktu w sprawie sztucznej inteligencji, zaproponowanym przez Komisję Europejską⁵, wskazano, że przez „system sztucznej inteligencji” należy rozumieć oprogramowanie, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję. Doprecyzowano przy tym, że chodzi o oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I. Wskazano tam w pierwszej kolejności mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego. Następnie wymieniono metody oparte na logice i wiedzy, takie jak reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe. Wyszczególniono także podejścia statystyczne, estymację bayesowską, metody wyszukiwania i optymalizacji. Zakładano, że wykaz sformułowany w załączniku I będzie aktualizowany w świetle rozwoju sytuacji rynkowej i postępu technologicznego w drodze aktów delegowanych przyjmowanych przez Komisję⁶.

Parlament Europejski zmodyfikował tę niewątpliwie skomplikowaną i mało zrozumiałą dla przeciętnego odbiorcy definicję⁷, zmierzając do nadania jej szerszego i bardziej uniwersalnego charakteru. Zgodnie z wprowadzoną poprawką „system sztucznej inteligencji oznacza system maszynowy, który został zaprojektowany do działania

⁵ Komisja Europejska, Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, Bruksela, dnia 21.04.2021 r., COM(2021) 206 final [dalej: AI Act].

⁶ Por. J. Rzymowski, *Definicja prawnicza sztucznej inteligencji na podstawie projektu rozporządzenia w sprawie sztucznej inteligencji*, „Prawo Nowych Technologii” 2023, nr 1, s. 19-23, Legalis; M. Nowakowski, *O moralnej odpowiedzialności HAL-a 9000, czyli etyka sztucznej inteligencji w praktyce. Czy potrzebujemy definicji sztucznej inteligencji?*, „Prawo Mediów Elektronicznych” 2022, nr 1, s. 4-10, Legalis.

⁷ Poprawki przyjęte przez Parlament Europejski w dniu 14 czerwca 2023 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html (15.06.2023) [dalej: AI Act w wersji PE]. Obecnie akt znajduje się na etapie negocjacji międzyinstytucjonalnych.

z różnym poziomem autonomii i który może – do wyraźnych lub dorozumianych celów – generować wyniki, takie jak przewidywania, zalecenia lub decyzje wpływające na środowiska fizyczne lub wirtualne”. Zrezygnowano przy tym z doprecyzowania technik i podejść w załączniku I. Należy zwrócić uwagę, że definicja zaproponowana przez Parlament Europejski ma w założeniu nawiązywać do standardów wypracowanych w tej dziedzinie na arenie międzynarodowej⁸.

Kluczowymi cechami sztucznej inteligencji są jej zdolności do uczenia się⁹, rozumowania i modelowania, co odróżnia ją od prostszych systemów czy podejść do programowania¹⁰. Systemy AI mogą być zaprojektowane tak, aby działały w sposób przynajmniej częściowo autonomiczny, czyli poza kontrolą człowieka i niezależnie od jego interwencji. Są one wykorzystywane jako samodzielne rozwiązania lub jako element określonego produktu, będąc z nim fizycznie zintegrowane (wbudowane) lub też służąc realizacji pewnych jego funkcji.

Parlament zauważył konieczność uwzględnienia w AI Act zagrożeń związanych z nowymi zjawiskami w postaci modeli generatywnych oraz systemów sztucznej inteligencji ogólnego przeznaczenia¹¹. Zgodnie z zaproponowanymi definicjami model generatywny (*foundation model*) oznacza „model systemu sztucznej inteligencji, który jest trenowany na szerokiej skali danych, jest zaprojektowany z myślą o ogólnym charakterze wyników i może być dostosowany do szerokiego zakresu odrębnych zadań”. Z kolei system sztucznej inteligencji ogólnego przeznaczenia to „system, który może

⁸ Jest ona bliska ujęciu tej problematyki wynikającemu m.in. z rekomendacji OECD, *Recommendation of the Council on Artificial Intelligence*, 22.05.2019, <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#mainText> (15.06.2023). Odmienne definicja została natomiast przyjęta w projekcie konwencji Rady Europy, przy czym jest ona określana jako bardzo szeroka i nieprecyzyjna, odbiegająca od standardów wynikających z innych aktów prawnych. Por. Committee on Artificial Intelligence (CAI), *Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, <https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f> (15.06.2023); M. Ręgorowicz, P. Konieczny, *Konwencja Rady Europy w sprawie sztucznej inteligencji*, <https://www.traple.pl/konwencja-rady-europy-w-sprawie-sztucznej-inteligencji/> (15.06.2023).

⁹ Systemy sztucznej inteligencji mają często zdolność do uczenia maszynowego, obejmującego m.in. uczenie nadzorowane, uczenie bez nadzoru i uczenie przez wzmocnienie przy zastosowaniu różnorodnych metod, w tym uczenia głębokiego z wykorzystaniem sieci neuronowych. Owa autonomiczność stwarza ryzyko przejęcia kontroli przez systemy sztucznej inteligencji. Por. motyw 6a AI Act w wersji PE.

¹⁰ Por. na ten temat J. Byrski, *Oprogramowanie zawierające elementy sztucznej inteligencji. Wybrane zagadnienia prawne*, [w:] *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple*, P. Kostański, P. Podrecki, T. Targosz (red.), Warszawa 2017, s. 1334-1343.

¹¹ Wcześniej kwestia ta została wskazana w Podejściu ogólnym przyjętym przez Radę Unii Europejskiej, Bruksela, dnia 25.11.2022 r., <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/pl/pdf> (15.06.2023).

być wykorzystywany i dostosowany do szerokiego zakresu zastosowań, do których nie został celowo i specjalnie zaprojektowany”. Głównym celem wspomnianych uregulowań jest odpowiedź na rosnące zainteresowanie i coraz powszechniejsze korzystanie z narzędzi typu ChatGPT, DALL-E, Bard czy LaMDA. Obejmują one m.in. duże modele językowe (*large language models*, LLM), trenowane na ogromnych zbiorach danych w celu wypracowania umiejętności przetwarzania tekstu, odpowiadania na pytania i generowania własnych treści. Są przy tym stworzone do wykonywania wielorakiego rodzaju zadań, zdolne do myślenia abstrakcyjnego oraz posiadają umiejętności uczenia się i adaptowania do nowych sytuacji, przez co różnią się od wcześniejszej sztucznej inteligencji wąskiego zastosowania (np. systemów rozpoznawania obrazu i mowy) oraz wymagają dodatkowych ram prawnych¹².

Należy podkreślić, że omawiana problematyka jest niezwykle złożona. Z uwagi na to, że funkcje systemów sztucznej inteligencji oraz generowane przez nie wyniki opierają się na abstrakcyjnych relacjach matematycznych, nawet osobom z odpowiednim wykształceniem trudno jest zrozumieć wewnętrzne działanie systemu sztucznej inteligencji. W wielu przypadkach mimo znajomości danych wyjściowych oraz wyniku działań brak jest możliwości uzyskania informacji o tym, w jaki sposób sztuczna inteligencja osiągnęła określony rezultat, przy czym kwestia ta pozostaje niejasna nawet dla twórców danego systemu¹³. Owo zagadnienie złożoności (w tym skomplikowania algorytmów przekraczającego zdolności poznawcze człowieka) i nieprzejrzystości określane jest jako problem „czarnej skrzynki” (*black box*). Z tego powodu w kontekście stosowania narzędzi opartych na AI w edukacji podkreśla się, że „zamiast starać się zrozumieć pełne funkcjonowanie systemów sztucznej inteligencji, ważniejsze jest, aby nauczyciele byli świadomi podstawowych mechanizmów i ograniczeń systemów sztucznej inteligencji oraz sposobów, w jakie systemy sztucznej inteligencji mogą być wykorzystywane do wspierania nauczania i uczenia się w bezpieczny i etyczny sposób”¹⁴.

¹² T. Madiega, *General-Purpose Artificial Intelligence*, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA\(2023\)745708_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf) (15.06.2023). Na temat sztucznej inteligencji w wąskim i szerokim ujęciu por. także P. Juściński, *Prawo autorskie w obliczu rozwoju sztucznej inteligencji*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2019, nr 1, s. 6–8.

¹³ M. Rojszczak, *Prawne aspekty systemów sztucznej inteligencji – zarys problemu*, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2019, s. 4.

¹⁴ Komisja Europejska, Dyrekcja Generalna ds. Edukacji, Młodzieży, Sportu i Kultury, *Wytoczne etyczne dla nauczycieli dotyczące wykorzystania sztucznej inteligencji i danych w nauczaniu i uczeniu się*, Luksemburg 2022 [dalej: Wytoczne KE dla nauczycieli].

3. Zastosowanie sztucznej inteligencji w edukacji

Kluczową rolę w rozwoju różnych form działalności przy użyciu sztucznej inteligencji odgrywają dane, w tym również dane osobowe¹⁵. Szkoły zazwyczaj przetwarzają znaczne ilości danych edukacyjnych, w szczególności o uczniach, rodzicach czy pracownikach, np. osiągnięcia szkolne, nazwiska rodziców, oceny. Także uczniowie, korzystając w trakcie nauki z różnego rodzaju urządzeń podłączonych do internetu i systemów informacyjnych online, generują ślady cyfrowe w postaci otwartych stron internetowych, kliknięć myszką, czasu naciśnięć klawiszy. Tego rodzaju dane, stanowiące źródło wielu istotnych informacji na temat procesu uczenia się, w tym jego skuteczności czy uzyskiwanych wyników, są zbierane i wykorzystywane do szkolenia algorytmów uczenia maszynowego. Algorytmy analizują przekazane im dane trenin-gowe, znajdują związki między nimi i podejmują na ich podstawie decyzje, biorąc pod uwagę rozpoznane potrzeby, preferencje, potencjał czy trudności konkretnych uczniów. Dzięki temu sztuczna inteligencja może zostać wykorzystana w pozytywny sposób dla celów edukacyjnych, prowadząc do lepszego zrozumienia potrzeb uczniów, umożliwiając opracowanie indywidualnych programów nauczania oraz zwiększając elastyczność i wydajność procesów uczenia¹⁶.

Rola sztucznej inteligencji w edukacji została zauważona w dokumentach wydanych przez instytucje Unii Europejskiej. W Rezolucji Parlamentu Europejskiego z dnia 19 maja 2021 r. w sprawie sztucznej inteligencji w sektorze edukacji i kultury oraz w sektorze audiowizualnym¹⁷ podkreślono, że „technologie te mogą w ogromnym stopniu przyczynić się do osiągnięcia [...] wspólnego celu, jakim jest polepszenie życia obywateli i wspieranie dobrobytu w Unii [...], ponieważ mogą one pomóc opracować lepsze strategie i innowacje w wielu dziedzinach, a mianowicie w edukacji, kulturze i sektorze audiowizualnym”. Także preambuła do AI Act¹⁸ zwraca uwagę, że rozwiązania bazujące na sztucznej inteligencji mają potencjał, aby wspierać wyniki korzystne

¹⁵ Por. A. Rapcewicz et al., *Sztuczna inteligencja w kontekście ochrony danych osobowych. Materiały pokonferencyjne*, <https://uodo.gov.pl> (15.06.2023); D. Lubasz, A. Szkurlat, *Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy” 2022, nr 21, dodatek, Legalis.

¹⁶ Por. L. Chen, P. Chen, Z. Lin, *Artificial Intelligence in Education: A Review*, „IEEE Access 2020”, nr 8, s. 75269; W.D. Heaven, *ChatGPT Is Going to Change Education, Not Destroy It*, MIT Technology Review, 6.04.2023, <https://www.technologyreview.com/2023/04/06/1071059/chatgpt-change-not-destroy-education-openai/> (15.06.2023).

¹⁷ Rezolucja Parlamentu Europejskiego z dnia 19 maja 2021 r. w sprawie sztucznej inteligencji w sektorze edukacji i kultury oraz w sektorze audiowizualnym, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0238_PL.html (15.06.2023) [dalej: Rezolucja PE].

¹⁸ Motyw 3.

z punktu widzenia kwestii społecznych, w tym kształcenia i szkolenia. Wskazuje się przy tym na rolę AI i powiązanych z nią technologii we wsparciu działań mających na celu wyrównanie szans edukacyjnych, zapewnienie lepszego dostępu do edukacji i podniesienie jakości kształcenia. Niewątpliwie narzędzia oparte na sztucznej inteligencji mogą ułatwić osiąganie postępów w różnych dziedzinach, w szczególności takich jak nauka języków i matematyka.

Wytyczne KE dla nauczycieli dzielą systemy sztucznej inteligencji pod kątem ich wykorzystania w edukacji na „ukierunkowane na ucznia”, „ukierunkowane na nauczyciela” i „ukierunkowane na system”. Do pierwszej kategorii zaliczono m.in. inteligentne systemy wspierające kształcenie, pozwalające uczniom na zdobywanie umiejętności poprzez wykonywanie zadań na podstawie indywidualnych instrukcji i informacji zwrotnych generowanych przez system bez konieczności interwencji ze strony nauczyciela, a także systemy oparte na dialogu, które wydają uczniom polecenia i odpowiadają na pytania w języku naturalnym. Warto zauważyć, że inaczej niż w tradycyjnym nauczaniu, opartym wyłącznie na zasobach ludzkich, chatboty potrafią dostosować się do indywidualnego tempa nauki, dzięki czemu proces kształcenia może być bardziej spersonalizowany i lepiej odpowiadać na potrzeby konkretnych uczniów, w tym rozwijać ich zdolności i wspierać obszary deficytowe. Wydaje się także, że dzięki zastosowaniu AI proces edukacji może być bardziej odporny na zmiany kadrowe, ponieważ wyniki nauczania i poziom zaawansowania poszczególnych uczniów będą mogły zostać utrwalone i kontynuowane przez kolejne osoby.

Systemy ukierunkowane na nauczyciela mają za zadanie udzielać nauczycielom wsparcia w różnorodnych czynnościach w procesie edukacji. W szczególności AI może ułatwić określenie obszarów, w których uczniowie mają problemy lub odnoszą sukcesy, i w ten sposób pomóc zrozumieć indywidualne potrzeby uczniów i opracować strategie indywidualnej nauki. Zgromadzone dane o uczniach pozwalają na rekomendowanie konkretnych działań lub zasobów edukacyjnych w zależności od postępów czy potrzeb uczniów oraz umożliwiają generowanie potrzebnych materiałów edukacyjnych, np. testów lub quizów. Narzędzia oparte na sztucznej inteligencji umożliwiają także prowadzenie kontroli w procesie nauczania, w tym ocenianie prac pisemnych na podstawie zidentyfikowanych cech (takich jak użycie konkretnych słów, gramatyka i struktura zdania) czy monitorowanie aktywności uczniów w trakcie zadań wykonywanych online.

Jeśli chodzi o wsparcie systemu, sztuczna inteligencja może zostać wykorzystana do ułatwienia diagnostyki i planowania. Chodzi w szczególności o przydział zasobów kadrowych, w tym tworzenie klas, układanie podziału godzin i przypisywanie nauczycieli do poszczególnych zespołów. Diagnostyka występujących trudności w uczeniu się oraz rozpoznanie potencjału uczniów i ich preferencji pozwalają na ocenę zapotrzebowania

zarówno na kształcenie specjalne czy zajęcia wyrównawcze, jak i na kursy rozwijające zainteresowania. Zebrane dane będą mogły zostać wykorzystane także do przewidywania ryzyka wczesnego kończenia nauki oraz do poradnictwa szkolnego i zawodowego.

Warto zwrócić uwagę na rolę sztucznej inteligencji w edukacji osób niepełnosprawnych. Może ona w szczególności pomóc w zapewnieniu odpowiednich materiałów dla uczniów ze specjalnymi potrzebami edukacyjnymi i zwiększyć dostępność oferowanych im treści. Jako przykład można podać systemy przetwarzające mowę na tekst i odwrotnie, przydatne dla osób niewidzących, niesłyszących bądź mających trudności z opanowaniem czytania lub pisania np. z uwagi na niepełnosprawność intelektualną. Z kolei zapisane wyniki nauczania można wykorzystać do skuteczniejszej diagnozy w kontekście wydawania orzeczeń o potrzebie kształcenia specjalnego. Jednorazowe badania psychologiczno-pedagogiczne dokonywane przez poradnie będą mogły być bowiem wsparte danymi o funkcjonowaniu ucznia zgromadzonymi w dłuższym okresie¹⁹.

Co istotne, sztuczna inteligencja może zostać wykorzystana do automatyzacji powtarzalnych zadań administracyjnych. Pomoże ona usprawnić takie czynności, jak sprawdzanie obecności, zapisy do szkół, weryfikacja wniosków, generowanie dokumentów. Redukcja czasu poświęcanego na wykonywanie rutynowych zadań stanowi szansę na odciążenie nauczycieli i umożliwienie im skoncentrowania się na potrzebach uczniów i pracy merytorycznej.

4. Zagrożenia związane ze stosowaniem narzędzi opartych na sztucznej inteligencji w edukacji

Jak wynika z powyższych rozważań, zastosowanie narzędzi opartych na sztucznej inteligencji może przyczynić się do tego, by nauka stała się bardziej spersonalizowana, łatwiejsza, atrakcyjniejsza i szybsza. Rozwój technologii stwarza wiele szans dla ucz-

¹⁹ W kontekście sytuacji osób niepełnosprawnych motyw 53a AI Act w wersji PE zwraca uwagę, że „jako sygnatariusze Konwencji ONZ o prawach osób niepełnosprawnych Unia i państwa członkowskie są prawnie zobowiązane do ochrony osób z niepełnosprawnościami przed dyskryminacją i do propagowania ich równości, do zapewnienia im dostępu na równych zasadach z innymi osobami do technologii i systemów informacyjno-komunikacyjnych oraz do zapewnienia poszanowania ich prywatności. Z uwagi na rosnące znaczenie i stosowanie systemów sztucznej inteligencji stosowanie zasad projektowania uniwersalnego do wszystkich nowych technologii i usług powinno zapewniać pełny, równy i nieograniczony dostęp dla wszystkich osób, których potencjalnie dotyczą technologie sztucznej inteligencji lub które je stosują, w tym osób z niepełnosprawnościami, w sposób uwzględniający w pełni ich przyrodzoną godność i różnorodność. Istotne jest zatem, aby dostawcy zapewniali pełną zgodność z wymogami dostępności, w tym z dyrektywą (UE) 2016/2102 i dyrektywą (UE) 2019/882. Dostawcy powinni zapewnić zgodność z tymi wymogami już na etapie projektowania”.

niów, nauczycieli i całego systemu kształcenia. Jednocześnie AI Act zwraca uwagę, że „sztuczna inteligencja może być źródłem ryzyka i szkody dla interesu publicznego lub prywatnego i praw podstawowych osób fizycznych, chronionych prawem Unii”²⁰. Należy pamiętać, że do trenowania systemów sztucznej inteligencji wykorzystuje się ogromną ilość danych, algorytmy działają w sposób automatyczny, nierzadko poza kontrolą człowieka, a dodatkowo narzędzia oparte na AI stosowane są na masową skalę. Wiąże się z tym ryzyko naruszeń w odniesieniu do danych osobowych i prywatności, powstają także wątpliwości co do transparentności i możliwości kontroli prowadzonych analiz i ich rezultatów. Sposób działania systemów sztucznej inteligencji, a w szczególności kierunek ich rozwoju i uzyskiwane wyniki, które mogą być oparte na niewłaściwej bądź tendencyjnej selekcji przetwarzanych danych, stwarzają zagrożenie dyskryminacji i wykluczenia w procesie edukacji oraz problem kontroli wartości przekazywanych w zautomatyzowanym procesie nauczania²¹. Jako przykład można tutaj podać powielanie stereotypów i związane z tym ryzyko stronniczości i różnicowania ze względu na płeć. Zauważono w szczególności, że z uwagi na niedostateczną reprezentację kobiet w dziedzinach nauk ścisłych i technicznych²² innowacje opierają się głównie na danych dotyczących mężczyzn i odzwierciedlają ich potrzeby. Jak wskazuje Rezolucja PE, „niekompletne i niedokładne zestawy danych, brak danych z podziałem na płeć oraz nieprawidłowe algorytmy mogą wypaczyć rozumowanie systemu AI”. Następnie „różnice w traktowaniu kobiet i mężczyzn, stereotypy i dyskryminacja mogą [...] być powielane za pomocą języka i obrazów rozpowszechnianych przez media oraz aplikacje opierające się na AI”²³. Niekontrolowane udostępnianie wypracowanych przez sztuczną inteligencję wyników i generowanie na ich podstawie kolejnych treści, naruszających

²⁰ Motyw 4.

²¹ W punkcie 6 Rezolucji PE zwrócono uwagę, że „AI może być źródłem uprzedzeń, a tym samym różnych form dyskryminacji ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne opinie, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną; w związku z powyższym [...] należy zagwarantować prawa wszystkich obywateli i że AI i powiązane technologie nie mogą prowadzić do jakiegokolwiek dyskryminacji”.

²² Według danych Eurostatu w 2018 r. kobiety stanowiły zaledwie 17% studentów z zakresu technologii informacyjno-komunikacyjnych (ICT), por. *The 2018 International Computer and Information Literacy Study (ICILS): Main Findings and Implications for Education Policies in Europe*, <https://education.ec.europa.eu/sites/default/files/document-library-docs/icils-2018-policy-note.pdf> (15.06.2023).

²³ Motyw 44 AI Act w wersji PE tłumaczy, że „tendencyjność może być na przykład nieodłączną cechą podstawowych zbiorów danych, szczególnie jeżeli używa się danych historycznych wprowadzonych przez twórców algorytmów lub wygenerowanych na etapie wdrażania systemów w warunkach rzeczywistych. Na wyniki osiągane przez systemy sztucznej inteligencji wpływa taka nieodłączna tendencyjność, która z zasady stopniowo zwiększa się, a tym samym utrwała i pogłębia

standardy etyczne lub sprzecznych z pożądanymi wartościami czy kierunkami rozwoju, może doprowadzić do powielania złych praktyk pedagogicznych na wielką skalę²⁴.

Innym przykładem istotnego zagrożenia jest możliwość wykorzystywania AI do generowania fałszywych treści, które mogą zakłócić proces kształcenia oraz wychowania. Należą do nich m.in. treści typu *deepfake*²⁵, zawierające zmanipulowane obrazy lub nagrania i przedstawiające rzekomy udział w nich określonych osób poprzez odtworzenie w sposób realistyczny ich wizerunku wraz z charakterystyczną mimiką, głosem czy gestykulacją. Szczególnym zagrożeniem dla dzieci i młodzieży jest wykorzystywanie tej technologii do generowania treści pornograficznych i różnych form cyberprzemocy. Może ona służyć także do tworzenia fałszywych materiałów w celu szantażu, zniesławienia czy manipulowania dużą rzeszą odbiorców²⁶. Jak wskazuje AI Act:

[...] oprócz wielu korzystnych zastosowań sztucznej inteligencji technologia ta może być również niewłaściwie wykorzystywana i może dostarczać nowych i potężnych narzędzi do praktyk manipulacji, wykorzystywania i kontroli społecznej. Takie praktyki są szczególnie szkodliwe oraz stanowią nadużycie i powinny być zakazane, ponieważ są sprzeczne z unijnymi wartościami poszanowania godności ludzkiej, wolności, równości, demokracji i praworządności oraz z prawami podstawowymi Unii, w tym z prawem do niedyskryminacji, ochroną danych i prywatności oraz z prawami dziecka²⁷.

Z uwagi na ryzyka związane ze stosowaniem systemów sztucznej inteligencji zwraca się uwagę na konieczność upowszechniania i pogłębiania wiedzy na ten temat wśród ich potencjalnych nabywców, użytkowników czy podmiotów, na które systemy te mogą oddziaływać²⁸. Dotyczy to także nauczycieli, kadry kierowniczej szkół, organów zarządzających oraz innych uczestników procesu edukacji, w tym uczniów i ich rodziców.

istniejącą dyskryminację, zwłaszcza w odniesieniu do osób należących do niektórych słabszych grup lub grup etnicznych czy społeczności rasowych”.

²⁴ A. Auleytner, M.J. Stępień, *Dostęp do sztucznej inteligencji – równość i inne aspekty prawne dostępu do systemów sztucznej inteligencji*, „Monitor Prawniczy” 2019, nr 21, dodatek, Legalis; A. Auleytner, *Równość dostępu do sztucznej inteligencji*, „Automatyka” 2018, nr 11, s. 28-29.

²⁵ Art. 3 akapit 1 pkt 44d AI Act w wersji PE definiuje *deepfake* jako „zmanipulowane lub syntetyczne treści dźwiękowe, obrazy lub treści wideo, które mylnie wydają się autentyczne lub zgodne z prawdą, i przedstawiają osoby, które wydają się mówić lub robić coś, czego nie powiedziały ani nie zrobiły, wyprodukowane z wykorzystaniem technik sztucznej inteligencji, w tym uczenia maszynowego i uczenia głębokiego”.

²⁶ K. Szpyt, *Sztuczna inteligencja i nowe technologie (nie zawsze) w służbie ludzkości, czyli cywilnoprawna problematyka rozwoju i popularyzacji technologii deepfake*, [w:] *Sztuczna inteligencja, blockchain...*, s. 75.

²⁷ Motyw 16.

²⁸ W tym kontekście Rezolucja PE wskazuje na problemy z rozwojem i upowszechnianiem wiedzy o technologiach cyfrowych. Stwierdza ona, że na cyfrowym rynku pracy Unii Europejskiej brakuje

Komisja Europejska podkreśla, że:

[...] ponieważ systemy sztucznej inteligencji nieustannie się rozwijają, a wykorzystanie danych wzrasta, niezwykle istotne jest wypracowanie lepszego zrozumienia ich wpływu na otaczający nas świat, w szczególności w obszarze kształcenia i szkolenia. Nauczyciele i członkowie kadry kierowniczej szkoły muszą mieć przynajmniej podstawową wiedzę na temat sztucznej inteligencji i wykorzystania danych, aby móc w sposób pozytywny, krytyczny i etyczny pracować z tą technologią i właściwie ją stosować w celu wykorzystania jej pełnego potencjału²⁹.

Wydaje się, że sztuczna inteligencja może być nieocenioną pomocą w codziennej pracy nauczyciela, otwierając przed nim oraz przed uczniami nowe możliwości edukacyjne, jednakże pod warunkiem, że jest właściwie używana i kontrolowana. Aby doprowadzić do utrzymania lub nawet zwiększenia roli nauczyciela w procesie edukacji wobec nowych możliwości stwarzanych przez technologie cyfrowe, konieczne jest zatem świadome, oparte na wiedzy zarządzanie rozwojem i korzystaniem z wprowadzanych narzędzi edukacyjnych, w sposób zmierzający do podtrzymania pozycji nauczyciela i zapobiegający jego marginalizacji.

Warto zaznaczyć, że rozwój umiejętności związanych z zastosowaniem sztucznej inteligencji w edukacji może być odpowiedzią na zgłaszane przez nauczycieli obawy co do możliwości zastąpienia ich w pracy przez narzędzia oparte na technologiach cyfrowych. Należy podkreślić, że AI nie jest zdolna do empatii, a kontakt na poziomie emocjonalnym jest niezbędny w procesie nauczania i wychowania dzieci i młodzieży. Nie wydaje się więc, aby w rzeczywistości rozwój sztucznej inteligencji mógł doprowadzić do wyeliminowania czynnika ludzkiego w procesie kształcenia, a w każdym razie byłoby to niepożądane. Niewątpliwie jednak niewłaściwe zarządzanie sztuczną inteligencją może doprowadzić do osłabienia pozycji nauczyciela lub utraty jego autorytetu, stąd potrzeba odpowiedniego szkolenia w tej dziedzinie i wypracowania właściwych procedur.

Jak wskazuje Parlament Europejski, „edukacja służy osiągnięciu potencjału ludzkiego, kreatywności i autentycznych zmian społecznych, podczas gdy niewłaściwe stoso-

prawie pół miliona ekspertów w dziedzinie dużych zbiorów danych i analizy danych. Zwraca także uwagę na ryzyko powstawania nowych podziałów lub pogłębiania istniejących z uwagi na nierównomierny rozwój wiedzy i infrastruktury w różnych regionach, co zmniejsza dostępność nowych technologii, w tym produktów i usług opartych na AI, zwłaszcza na obszarach słabo zaludnionych i o trudnej sytuacji społeczno-gospodarczej. W związku z tym wskazuje na konieczność podjęcia przez Komisję działań zmierzających do zapewnienia spójności w dzieleniu się korzyściami płynącymi z AI i technologii pokrewnych.

²⁹ *Sztuczna inteligencja w szkole...*

wanie systemów AI opartych na danych może utrudniać rozwój ludzki i społeczny”³⁰. Z tego powodu, mając na uwadze wpływ edukacji na kształtowanie przekonań i wartości ludzi, przed wdrożeniem zautomatyzowanych rozwiązań konieczne jest wprowadzenie w tym obszarze odpowiednich ram etycznych i regulacyjnych.

5. Propozycje unijnych ram prawnych

W związku ze zidentyfikowanymi zagrożeniami na poziomie Unii Europejskiej już od kilku lat podejmowane są działania zmierzające do zapewnienia bezpiecznego stosowania sztucznej inteligencji w edukacji, a także do zapewnienia nauczycielom, członkom kadry kierowniczej szkół i uczniom odpowiedniej wiedzy dotyczącej sztucznej inteligencji i wykorzystania danych³¹. Unia Europejska dąży do stworzenia sprawnie funkcjonującego europejskiego systemu edukacji cyfrowej, mając na uwadze, że wobec dokonującego się w szybkim tempie postępu technologicznego kompetencje i umiejętności cyfrowe są niezbędne, aby zapewnić każdej osobie równe szanse na rozwój życiowy, znalezienie zatrudnienia i udział w społeczeństwie. Znaczenie tychże umiejętności stało się wyraźnie widoczne zwłaszcza w okresie pandemii COVID-19.

We wrześniu 2020 r. Komisja Europejska przedstawiła plan działania w dziedzinie edukacji cyfrowej (na lata 2021-2027)³², w którym wezwała państwa członkowskie do współpracy w celu dostosowania systemów kształcenia i szkolenia do wymagań cyfrowego świata i uczynienia tych systemów powszechnie dostępnymi i sprzyjającymi społecznej spójności. Plan obejmuje dwa strategiczne działania – wspieranie rozwoju efektywnej edukacji cyfrowej oraz rozwijanie kompetencji i umiejętności cyfrowych właściwych w dobie transformacji cyfrowej. Pierwsze z nich zmierza do zapewnienia

³⁰ Motyw Q Rezolucji PE.

³¹ W motywie L Rezolucji PE podkreślono, że „Unia i jej państwa członkowskie są szczególnie odpowiedzialne za wykorzystanie, promowanie i wzmocnienie wartości dodanej płynącej z technologii związanych z AI, a także za dopilnowanie, by technologie te były bezpieczne, przyczyniały się do dobrostanu Europejczyków i działały w ich interesie ogólnym”. Z kolei motyw R wskazuje, że „kształcenie i możliwości edukacyjne są jednym z praw podstawowych”, a „rozwijanie, wprowadzanie i stosowanie technologii związanych z AI w sektorze edukacji należy uznać za działania wysokiego ryzyka i powinny one podlegać bardziej surowym wymaganiom pod względem bezpieczeństwa, przejrzystości, sprawiedliwości i rozliczalności”.

³² Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Plan działania w dziedzinie edukacji cyfrowej na lata 2021-2027. Nowe podejście do kształcenia i szkolenia w epoce cyfrowej*, Bruksela, dnia 30.09.2020 r., COM(2020) 624 final.

infrastruktury cyfrowej³³, nauczycieli posiadających odpowiednie kompetencje w tej dziedzinie i wysokiej jakości treści dydaktycznych, m.in. poprzez szanujące zasady prywatności i etyki narzędzia i platformy. Priorytetami drugiego jest z kolei kształtowanie umiejętności cyfrowych zarówno na poziomie podstawowym – w formie prowadzonej od najmłodszych lat edukacji informatycznej, umożliwiającej odpowiednie poznanie i zrozumienie technologii, w tym sztucznej inteligencji, jak i na poziomie zaawansowanym – w celu zapewnienia większej liczby specjalistów w dziedzinie technologii cyfrowych, z uwzględnieniem równej reprezentacji kobiet na studiach i w zawodach informatycznych.

Plan działania w dziedzinie edukacji cyfrowej w ramach priorytetu 1 i szczegółowego działania 6 obejmował m.in. opracowanie dokumentu zawierającego zasady i wskazówki dla nauczycieli stosujących systemy AI. Zostały one przygotowane w formie wspomnianego już wcześniej dokumentu pt. *Wytyczne etyczne dla nauczycieli dotyczące wykorzystywania sztucznej inteligencji i danych w nauczaniu i uczeniu się* przez nieformalną grupę ekspertów powołanych w tym celu przez Komisję³⁴. Wytyczne są uzupełnieniem działań podejmowanych przez Komisję za pośrednictwem programu Erasmus+, Europejskiego Korpusu Solidarności i eTwinningu. Transformacja cyfrowa stanowi jeden z czterech głównych priorytetów Erasmus+, który ma w szczególności zapewnić finansowanie zadań obejmujących opracowanie i wdrażanie planów transformacji cyfrowej w instytucjach edukacyjnych. Europejski Korpus Solidarności przyczynia się do transformacji cyfrowej, wspierając projekty, które rozwijają umiejętności cyfrowe oraz służą pogłębianiu wiedzy na temat zarówno możliwości, jak i zagrożeń związanych z technologią cyfrową. Z kolei eTwinning oferuje możliwość współpracy między szkołami i przedszkolami z różnych państw UE za pośrednictwem serwisu internetowego oraz szereg form doskonalenia zawodowego dla zarejestrowanych nauczycieli. Ze środków Erasmus+ uruchomiona została także europejska platforma edukacji szkolnej (ESEP), na której zgodnie z zapowiedzią Komisji mają być publiko-

³³ Motyw S Rezolucji PE zwraca uwagę, że „wysokiej jakości, szybka, bezpieczna i powszechnie dostępna łączność, sieci szerokopasmowe o dużej przepustowości, specjalistyczna wiedza informatyczna, umiejętności cyfrowe, sprzęt cyfrowy i infrastruktura cyfrowa, a także akceptacja społeczna oraz ukierunkowane i sprzyjające ramy polityczne to niektóre z warunków koniecznych dla powszechnego i pomyślnego wprowadzenia AI w Unii; [...] ważne jest, by taka infrastruktura i sprzęt zostały wprowadzone równomiernie w całej Unii w celu zlikwidowania utrzymującej się przepaści cyfrowej między jej regionami a obywatelami”.

³⁴ Por. także European Commission, Directorate-General for Education, Youth, Sport and Culture, *Final Report of the Commission Expert Group on Artificial Intelligence and Data in Education and Training – A Executive Summary*, Publications Office of the European Union, 2022.

wane m.in. artykuły oraz internetowy kurs na temat sztucznej inteligencji w edukacji dla nauczycieli.

Ponadto do edukacji odnoszą się uniwersalne ramy prawne przyjmowane przez instytucje Unii Europejskiej, w tym biała księga Komisji z 2020 r. oraz wspomniany już wielokrotnie AI Act. W białej księdze Komisji w sprawie sztucznej inteligencji z 2020 r.³⁵ wskazano warianty strategiczne umożliwiające bezpieczny rozwój godnej zaufania sztucznej inteligencji w Europie³⁶. Podkreślono także kluczowe znaczenie europejskiego podejścia do sztucznej inteligencji, u którego podstaw leży silny nacisk na uzupełnienie niedoborów kompetencji i umiejętności cyfrowych.

W 2021 r. Komisja Europejska przedstawiła wniosek dotyczący kompleksowych ram prawnych w odniesieniu do sztucznej inteligencji (AI Act). Projekt rozporządzenia ustanawia zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w Unii, w tym ich monitorowania po wprowadzeniu do obrotu. W zależności od stopnia ryzyka, jakie wiąże się ze stosowaniem tych systemów, podzielono je na cztery kategorie: nieakceptowalne (zakazane), wysokiego ryzyka (dopuszczalne pod ścisłą kontrolą), ograniczonego ryzyka (podlegające obowiązkowi informacyjnym) i minimalnego ryzyka (brak regulacji)³⁷. Zgodnie z brzmieniem przyjętym przez Parlament Europejski celem rozporządzenia „jest promowanie upowszechniania ukierunkowanej na człowieka i godnej zaufania sztucznej inteligencji oraz zapewnienie wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych, demokracji i praworządności oraz środowiska przed szkodliwymi skutkami systemów sztucznej inteligencji w Unii, przy jednoczesnym wspieraniu innowacji”.

³⁵ Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*, Bruksela, dnia 19.02.2020 r., COM(2020) 65 final.

³⁶ Por. także dokumenty grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji powołanej przez Komisję Europejską w czerwcu 2018 r.: *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, <https://digital-strategy.ec.europa.eu/pl/node/1950> (15.06.2023); *Zalecenia polityczne i inwestycyjne dotyczące godnej zaufania sztucznej inteligencji*, <https://digital-strategy.ec.europa.eu/pl/node/1694> (15.06.2023); *Ostateczna lista oceny godnej zaufania sztucznej inteligencji (ALTAI)*, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> (15.06.2023).

³⁷ Por. M. Susańko, *Podejście oparte na ryzyku w projekcie aktu w sprawie sztucznej inteligencji i RODO*, „Prawo Nowych Technologii” 2023, nr 1, s. 10-18, Legalis; M. Nowakowski, *Ostatnie zmiany w ramach prawnych dla sztucznej inteligencji w Unii Europejskiej – krytyczna analiza*, „Prawo Nowych Technologii” 2021, nr 2, s. 23-30, Legalis.

Do zakazanych systemów sztucznej inteligencji zaliczono m.in. te mające na celu lub skutkujące istotnym zniekształceniem ludzkiego zachowania³⁸, wykorzystywane do oceny społecznej (klasyfikowanie ludzi na podstawie ich zachowań społecznych lub cech osobistych³⁹), identyfikacji i kategoryzacji biometrycznej⁴⁰ (z wyjątkiem identyfikacji dokonywanej *post factum* w związku z poważnymi przestępstwami za zgodą sądu), wyciągania wniosków na podstawie rozpoznawania emocji (w tym w instytucjach edukacyjnych) i do prognozowania kryminologicznego oraz umożliwiające tworzenie baz danych do rozpoznawania twarzy poprzez nieukierunkowane pobieranie (ang. *scraping*) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej⁴¹.

Za systemy wysokiego ryzyka uznano systemy sztucznej inteligencji, które w związku z ich przeznaczeniem stwarzają duże zagrożenie powstania szkody dla zdrowia, bezpieczeństwa, praw podstawowych lub środowiska. Wśród obszarów krytycznych wymieniono m.in. kształcenie i szkolenie⁴². Chodzi tutaj o systemy wykorzystywane

³⁸ Należy przez nie rozumieć rozwiązania wspomagane przez systemy sztucznej inteligencji obejmujące neurotechnologie, „które są wykorzystywane do monitorowania i wykorzystywania danych neuronowych gromadzonych za pośrednictwem interfejsów mózg–komputer lub wpływania na nie, o ile zniekształcają one istotnie zachowanie osoby fizycznej w sposób, który wyrządza lub może wyrządzić tej lub innej osobie poważną szkodę. Takie systemy sztucznej inteligencji wykorzystują mechanizmy podprogowe, których osoby fizyczne nie są w stanie dostrzec, lub wykorzystują słabości osób i konkretnych grup osób ze względu na ich znane lub przewidywane cechy osobowe, takie jak wiek, niepełnosprawność fizyczna lub umysłowa czy sytuacja społeczna lub ekonomiczna” – por. motyw 16 AI Act w wersji PE.

³⁹ W tym ze względu na płeć, tożsamość płciową, rasę, pochodzenie etniczne, status migracyjny lub obywatelstwo, poglądy polityczne, orientację seksualną, wyznanie, niepełnosprawność lub wszelkie inne powody, dla których dyskryminacja jest zakazana na mocy art. 21 Karty praw podstawowych Unii Europejskiej oraz art. 6 Rozporządzenia 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, Dz.Urz. UE 2016, L 119.

⁴⁰ Por. A. Michałowicz, *Przetwarzanie danych biometrycznych a ochrona jednostek – analiza wybranych zagadnień na tle ogólnego rozporządzenia o ochronie danych i projektu aktu w sprawie sztucznej inteligencji*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2021, nr 6(10), s. 78-94, Legalis.

⁴¹ Por. na ten temat M. O’Flaherty, *Facial Recognition Technology and Fundamental Rights*, „European Data Protection Law Review” 2020, vol. 6, no. 2, s. 170-173.

⁴² Zgodnie z motywem 28a przy klasyfikowaniu systemu sztucznej inteligencji jako systemu wysokiego ryzyka zasadnicze znaczenie ma skala szkodliwego wpływu systemu sztucznej inteligencji na prawa podstawowe chronione na mocy Karty. Do praw tych należą m.in. prawo do edukacji oraz prawa osób z niepełnosprawnościami. Podkreślono ponadto, że „dzieciom przysługują szczególne prawa zapisane w art. 24 oraz w Konwencji o prawach dziecka (szerzej rozwinięte w komentarzu ogólnym nr 25 do Konwencji ONZ o prawach dziecka w odniesieniu do środowiska cyfrowego), które wymagają uwzględnienia słabości dzieci oraz zapewnienia im ochrony i opieki koniecznej dla ich dobra”.

w szczególności przy podejmowaniu decyzji o dostępie do instytucji kształcenia i szkolenia zawodowego lub nadawaniu osobom przydziału do tych instytucji lub też do oceniania osób na testach w ramach kształcenia lub jako warunek dopuszczenia do kształcenia. Zostały one sklasyfikowane jako systemy wysokiego ryzyka, ponieważ mogą decydować o przebiegu kształcenia i kariery zawodowej danej osoby, a tym samym wpływać na jej zdolność do zapewnienia sobie źródła utrzymania. Jak wskazano w preambule, „takie systemy, jeżeli są niewłaściwie zaprojektowane i nieodpowiednio stosowane, mogą naruszać prawo do nauki i odbywania szkoleń, a także prawo do niedyskryminacji i mogą utrzymywać historyczne wzorce dyskryminacji”⁴³.

6. Procedury mające na celu zminimalizowanie zagrożeń

Motyw 1 preambuły do AI Act w wersji PE wskazuje, że celem rozporządzenia jest:

[...] promowanie upowszechniania ukierunkowanej na człowieka i godnej zaufania sztucznej inteligencji oraz zapewnienie wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych, demokracji i praworządności oraz środowiska przed szkodliwymi skutkami systemów sztucznej inteligencji w Unii, przy jednoczesnym wspieraniu innowacji i poprawie funkcjonowania rynku wewnętrznego⁴⁴.

Wskazano także, że:

[...] warunkiem wstępnym jest to, by sztuczna inteligencja była technologią ukierunkowaną na człowieka. Nie powinna ona zastępować autonomii człowieka ani zakładać utraty wolności jednostki, a przede wszystkim powinna służyć potrzebom społeczeństwa i dobru wspólnemu. Należy przewidzieć zabezpieczenia, aby zapewnić rozwój i wykorzystywanie sztucznej inteligencji zgodnie z zasadami etycznymi oraz wartościami Unii i Karty⁴⁵.

AI Act kładzie nacisk na to, aby sztuczna inteligencja była nie tylko bezpieczna, ale także wiarygodna. Osiągnięciu tego celu mają służyć wspólne regulacje, ustanawiające w szczególności jednolite obowiązki dla operatorów i zmierzające do zagwarantowania

⁴³ Motyw 35.

⁴⁴ W motywie 13 podkreślono ponadto, że standardy normatywne dla wszystkich systemów sztucznej inteligencji wysokiego ryzyka powinny być zgodne z Kartą praw podstawowych, Europejskim Zielonym Ładem, wspólną deklaracją UE w sprawie praw cyfrowych i wytycznymi w zakresie etyki dotyczącymi godnej zaufania sztucznej inteligencji, które opracowała grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, oraz powinny być niedyskryminacyjne i zgodne z międzynarodowymi zobowiązaniami handlowymi Unii.

⁴⁵ Motyw 4a AI Act w wersji PE.

jednolitej ochrony nadrzędnego interesu publicznego i praw osób na całym rynku wewnętrznym.

W odniesieniu do systemów wysokiego ryzyka stosowanych w kształceniu i szkoleniu sformułowano wymogi, których celem jest zapewnienie, aby instytucje edukacyjne jako użytkownicy systemów sztucznej inteligencji mogły polegać na ich wiarygodności w oparciu o certyfikację uzyskaną przez dostawcę i aby miały możliwość zweryfikowania, czy systemy te są zgodne z ramami regulacyjnymi dotyczącymi AI, zasadami etycznymi i czy zapewniają przestrzeganie obowiązujących przepisów w zakresie ochrony danych.

Systemy sztucznej inteligencji wysokiego ryzyka mają podlegać przede wszystkim wymogom dotyczącym jakości i istotności wykorzystywanych zbiorów danych, dokumentacji technicznej i rejestrowania zdarzeń, przejrzystości i przekazywania informacji operatorom systemów sztucznej inteligencji, nadzoru ze strony człowieka oraz solidności, dokładności i cyberbezpieczeństwa. Zwraca się uwagę, że zbiory danych treningowych powinny być wystarczająco adekwatne, reprezentatywne, odpowiednio zweryfikowane pod kątem błędów oraz jak najbardziej kompletne z punktu widzenia przeznaczenia systemu. Mają one również charakteryzować się odpowiednimi właściwościami statystycznymi w celu zmniejszenia ewentualnej tendencyjności w zbiorach danych i zapobiegania dyskryminacji. Systemy sztucznej inteligencji wysokiego ryzyka powinny działać w sposób spójny w całym cyklu życia i charakteryzować się odpowiednim poziomem dokładności, solidności i cyberbezpieczeństwa. Dostawcy będą musieli ustanowić skuteczny system zarządzania jakością, zapewnić przeprowadzenie wymaganej procedury oceny zgodności, sporządzić odpowiednią dokumentację i ustanowić system monitorowania po wprowadzeniu do obrotu. Systemy sztucznej inteligencji będą podlegały normalizacji i będą musiały posiadać oznakowanie CE świadczące o ich zgodności z rozporządzeniem.

Obowiązki zostały także nałożone na operatorów sztucznej inteligencji, którzy odgrywają kluczową rolę w zapewnieniu praw podstawowych w trakcie korzystania z systemów, znając praktyczne aspekty i okoliczności ich stosowania oraz mając kontakt z osobami, na które AI może wywierać wpływ. Oprócz przestrzegania instrukcji obsługi systemu będą oni musieli określić odpowiednie struktury zarządzania, takie jak ustalenia dotyczące nadzoru ze strony człowieka oraz procedury rozpatrywania skarg i dochodzenia roszczeń. Przed oddaniem systemu do użytku wymagane będzie przeprowadzenie oceny jego wpływu na prawa podstawowe, czemu powinien towarzyszyć szczegółowy plan, opisujący środki lub narzędzia, które pomogą ograniczać

zidentyfikowane ryzyko dla praw podstawowych najpóźniej z chwilą oddania systemu do użytku⁴⁶.

AI Act zobowiązuje dostawców do wdrożenia systemu monitorowania po dokonaniu wprowadzenia do obrotu. Ma to pozwolić na podejmowanie działań naprawczych w krótkim czasie, a także umożliwić innym podmiotom korzystanie z istniejących doświadczeń do ulepszenia swoich systemów oraz procesu projektowania i rozwoju. Dostawcy będą musieli posiadać system zgłaszania właściwym organom wszelkich poważnych incydentów lub wszelkich naruszeń prawa krajowego i prawa Unii, w tym chroniącego prawa podstawowe i prawa konsumenta, zaistniałych w związku ze stosowaniem ich systemów sztucznej inteligencji. Na operatorów został z kolei nałożony obowiązek zgłaszania takich incydentów lub naruszeń wynikających z korzystania z AI.

Systemy sztucznej inteligencji wysokiego ryzyka będą podlegały rejestracji w unijnej bazie danych. Obowiązkiem rejestracji objęto także dostawców modeli generatywnych. Mają oni ponadto wykazywać – poprzez odpowiednie projektowanie, testowanie i analizę – że przed opracowaniem i przez cały okres opracowywania modelu identyfikowano, ograniczano i łagodząco racjonalnie przewidywalne zagrożenia dla zdrowia, bezpieczeństwa, praw podstawowych, środowiska, demokracji i praworządności. Generatywne systemy sztucznej inteligencji oparte na takich modelach będą musiały spełniać wymogi przejrzystości. Powinny one w szczególności ujawniać w odpowiednim czasie, w jasny i zrozumiały sposób, że dane treści (w tym *deepfake*) zostały wygenerowane lub zmanipulowane przez system sztucznej inteligencji, oraz podawać imię i nazwisko osoby fizycznej lub nazwę osoby prawnej odpowiedzialnej za ich wygenerowanie lub zmanipulowanie. Muszą zawierać obowiązki informacyjne i przygotowywać całą niezbędną dokumentację techniczną, aby potencjalni dostawcy niższego szczebla mogli wypełniać nałożone na nich obowiązki. Konieczne ma być także publikowanie szczegółowych podsumowań danych chronionych prawem autorskim, które wykorzystano do szkolenia tych systemów.

Wyjątki od obowiązków wynikających z AI Act wprowadzono dla badań naukowych oraz dla komponentów sztucznej inteligencji dostarczanych na podstawie wolnych i otwartych licencji. Rozporządzenie zachęca do tworzenia tzw. piaskownic regulacyjnych, rozumianych jako ustanowione przez organ publiczny kontrolowane środowisko, które ułatwia bezpieczne opracowywanie, testowanie i walidację innowacyjnych systemów

⁴⁶ Por. także B. Oręziak, *Prawa człowieka jako determinanta sztucznej inteligencji? Propozycja kryteriów i dyrektyw zastosowania sztucznej inteligencji do użytku praktycznego*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, s. 199–210, *Monografie Prawnicze*.

sztucznej inteligencji przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem do użytku zgodnie z określonym planem pod nadzorem regulacyjnym⁴⁷.

Wytyczne KE dla nauczycieli formułują szereg wymogów, które stanowią podstawę etycznego wykorzystania sztucznej inteligencji i danych w nauczaniu, uczeniu się i ocenianiu. Powinny być one spełnione dla każdego systemu sztucznej inteligencji stosowanego w edukacji, w szczególności w celu zminimalizowania ryzyka stronniczości lub błędu wpływającego na wyniki kształcenia. Mają one pomóc dostawcom technologii oraz ich odbiorcom, w tym dyrektorom szkół i nauczycielom, w dokonaniu odpowiedniej oceny wpływu, przeciwdziałaniu potencjalnym zagrożeniom i wykorzystaniu zalet AI oraz stanowić wskazówkę przy opracowywaniu, wdrażaniu i używaniu takiego systemu. Wymogi te obejmują zagwarantowanie: przewodniej i nadzorczej roli człowieka, przejrzystości, różnorodności, niedyskryminacji i sprawiedliwości, dobrostanu społecznego i środowiskowego, ochrony prywatności i właściwego zarządzania danymi, technicznej solidności i bezpieczeństwa oraz odpowiedzialności za działania AI.

W celu zobrazowania, w jaki sposób powyższe wymogi powinny być realizowane w praktyce, można w szczególności wskazać, że aby zapewnić przewodnią i nadzorczą rolę człowieka, należy weryfikować, czy funkcja nauczyciela została wyraźnie określona i czy w trakcie korzystania ze sztucznej inteligencji nauczyciel ma rzeczywisty wpływ na podejmowanie decyzji. Przejrzystość wymaga, aby nauczyciele i członkowie kadry kierowniczej rozumieli, w jaki sposób konkretne algorytmy oceny lub personalizacji funkcjonują w systemie sztucznej inteligencji. Jako warunek dobrostanu społecznego system sztucznej inteligencji powinien wyraźnie wskazywać, że jego interakcje społeczne są symulacją i że nie jest on zdolny do odczuwania ani okazywania empatii. W celu ochrony prywatności i zarządzania danymi konieczne jest monitorowanie, czy dostęp do danych osób uczących się jest chroniony oraz czy dane te są przechowywane w bezpiecznym miejscu i wykorzystywane jedynie do celów, do których zostały zgromadzone⁴⁸. Z kolei dla zapewnienia odpowiedzialności za działania AI szkoła powinna zawrzeć właściwą umowę z dostawcą systemu, która gwarantuje odpowiedni poziom usług, określa zasady wsparcia i rozwiązywania zgłoszonych problemów.

⁴⁷ Należy zwrócić uwagę, że przedstawione obowiązki wynikają z AI Act w wersji PE. Ich zakres może jeszcze ulec zmianie w finalnej wersji rozporządzenia na skutek poprawek wprowadzonych na etapie negocjacji międzyinstytucjonalnych.

⁴⁸ Szerzej na temat ochrony danych przetwarzanych przez systemy sztucznej inteligencji por. D. Lubasz, M. Namysłowska, *Ochrona danych osobowych a sztuczna inteligencja*, [w:] *Ochrona danych osobowych*, D. Lubasz (red.), Warszawa 2020, s. 1009-1030, *Meritum*.

W ślad za sformułowanymi wymogami etycznymi wytyczne wskazują na procedury *compliance*, które będą musiały stosować szkoły już w niedalekiej przyszłości. Zgodnie z nimi:

[...] przed wdrożeniem systemu sztucznej inteligencji należy wprowadzić w całej szkole politykę i zasady, które określą oczekiwania i dostarczą wskazówek co do konsekwentnego postępowania w przypadku wystąpienia problemów. Mogą one obejmować środki dotyczące: zapewnienia zamówień publicznych na godną zaufania i ukierunkowaną na człowieka sztuczną inteligencję od wiarygodnych dostawców posiadających wymagane certyfikaty; wdrożenia nadzorczej roli człowieka; zapewnienia, aby dane wejściowe odpowiadały zamierzonemu celowi systemu sztucznej inteligencji; zorganizowania odpowiedniego szkolenia dla pracowników; monitorowania funkcjonowania systemu sztucznej inteligencji i podejmowania działań naprawczych oraz przestrzegania odpowiednich zobowiązań wynikających z RODO, w tym przeprowadzenia oceny skutków dla ochrony danych⁴⁹.

Istotne jest przy tym poinformowanie o istniejących procedurach nauczycieli, uczniów i rodziców, aby byli oni świadomi istniejących wymogów i oczekiwań.

AI Act wskazuje ponadto, że osoby fizyczne i prawne oraz grupy osób fizycznych, których prawa i wolności mogą zostać naruszone przez systemy sztucznej inteligencji, powinny mieć dostęp do mechanizmów zgłaszania i dochodzenia roszczeń oraz proporcjonalnych i skutecznych środków ochrony prawnej. Przewiduje się w szczególności możliwość zgłaszania naruszeń rozporządzenia krajowym organom nadzorczym oraz prawo do złożenia skargi przeciwko operatorom systemów sztucznej inteligencji, jak również do sądowych środków odwoławczych od decyzji organów nadzorczych.

Dodatkowo Komisja Europejska przedstawiła projekt tzw. AI Liability Directive⁵⁰. Ustanawia ona jednolite wymogi dotyczące niektórych aspektów pozaumownej odpowiedzialności cywilnej za szkody powstałe w wyniku działania systemów AI. Zwrócono w niej uwagę na niedostosowanie aktualnie obowiązujących krajowych przepisów o odpowiedzialności cywilnej do kwestii roszczeń z tytułu odpowiedzialności za szkody spowodowane przez produkty i usługi wspierane przez sztuczną inteligencję. Problematiczne są zwłaszcza kwestie ustalenia osoby odpowiedzialnej oraz ciężaru dowodowego spoczywającego na powodzie, który musi wykazać bezprawne działanie

⁴⁹ Wytyczne KE dla nauczycieli, s. 26.

⁵⁰ Komisja Europejska, Wniosek. Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), Bruksela, dnia 28.09.2022 r., COM(2022) 496 final.

lub zaniechanie sprawcy szkody⁵¹. W przypadku systemów sztucznej inteligencji jest to znacznie utrudnione z uwagi na ich złożoność, autonomiczność i nieprzejrzystość (wspomniany efekt „czarnej skrzynki”). W związku z tym wystąpienie na drogę sądową może generować znaczne koszty, co przy jednoczesnym wydłużeniu postępowania z uwagi na jego złożoność powoduje ryzyko zniechęcenia i rezygnacji z dochodzenia roszczeń przez poszkodowanego.

W celu ułatwienia korzystania ze środków prawnych w związku z działaniami sztucznej inteligencji projekt AI Liability Directive ustanawia wspólne zasady ujawniania dowodów dotyczących systemów AI wysokiego ryzyka oraz ciężaru dowodu w przypadku pozaumownych cywilnoprawnych roszczeń odszkodowawczych spowodowanych przez system sztucznej inteligencji. Umożliwia on uzyskanie informacji na temat systemów sztucznej inteligencji wysokiego ryzyka, które mają być rejestrowane i dokumentowane zgodnie z wymogami AI Act. Wprowadza także wzruszalne domniemania, obejmujące w szczególności istnienie związku przyczynowego między winą pozwanego a wynikiem uzyskanym przez system sztucznej inteligencji lub faktem nieuzyskania przez taki system wyniku. Postanowienia AI Liability Directive mają ułatwić dochodzenie odszkodowania za szkody spowodowane przez systemy sztucznej inteligencji i tym samym zapewnić większą ochronę podmiotów, których prawa mogą zostać naruszone przez działania AI⁵².

7. Zakończenie

Jak wynika z powyższych rozważań, systemy sztucznej inteligencji mogą odegrać ważną rolę w unowocześnieniu edukacji, prowadząc do poprawy jakości kształcenia i zwiększenia jego dostępności dla odbiorców, zarówno w formie stacjonarnej, jak i online. Edukacja cyfrowa odgrywa także ważną rolę we wspieraniu rozwoju społeczno-gospodarczego. Jeżeli jest ona odpowiednio prowadzona, może sprzyjać włączeniu społecznemu, w szczególności w zakresie kształcenia osób z mniejszych miejscowości, niepełnosprawnych czy z innych względów zagrożonych wykluczeniem.

⁵¹ Por. A. Michalak, *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021, s. 375 i n., *Monografie Prawnicze*.

⁵² Na temat odpowiedzialności prawnej za szkody wyrządzone przez sztuczną inteligencję por. także E. Kurowska-Tober, Ł. Czynienik, M. Koniarska, *Aspekty prawne sztucznej inteligencji – zarys problematyki*, „Monitor Prawniczy” 2019, nr 21, dodatek, Legalis. W kontekście usług cyfrowych por. G. Bar, R. Skibicki, *Wyzwania prawne związane z wykorzystaniem sztucznej inteligencji w usługach cyfrowych*, „Prawo Nowych Technologii” 2021, nr 1, s. 40-45, Legalis.

Jednocześnie, jak podkreślono w uzasadnieniu AI Act, „wykorzystywanie sztucznej inteligencji wraz z jej szczególnymi cechami (np. efekt czarnej skrzynki, złożoność, zależność od danych, autonomiczne zachowanie) może mieć negatywny wpływ na szereg praw podstawowych zapisanych w Karcie praw podstawowych Unii Europejskiej”⁵³. Proponowane na poziomie unijnym regulacje prawne mają na celu uwzględnienie różnych źródeł ryzyka i zagwarantowanie wysokiego poziomu ochrony praw podstawowych wobec systemów AI. Służy temu w szczególności sformułowanie zestawu wymogów dotyczących wiarygodnej sztucznej inteligencji oraz proporcjonalnych obowiązków nałożonych na wszystkich uczestników obrotu. Testowanie przed wprowadzeniem do obrotu, zarządzanie ryzykiem i nadzór ze strony człowieka powinny zmniejszyć niebezpieczeństwo błędnych lub stronniczych decyzji podejmowanych przy wsparciu AI w obszarach krytycznych, do których należy także kształcenie i szkolenie. Jednocześnie zapewnienie przejrzystości i identyfikowalności systemów sztucznej inteligencji⁵⁴ w połączeniu z kontrolami na etapie ich funkcjonowania ma umożliwić skuteczne dochodzenie roszczeń przez osoby poszkodowane, których prawa zostały naruszone mimo wprowadzonych przez prawodawcę środków zapobiegawczych.

Projektowane uregulowania mogą generować obciążenie dla szkół, które będą zmagać się z jednej strony z opanowaniem zastosowania nowych technologii w procesie edukacji, a z drugiej – z wypełnieniem licznych obowiązków prawnych. Będą także w jakimś stopniu ponosiły ryzyko odpowiedzialności za potencjalne skutki działania sztucznej inteligencji.

W odpowiedzi na formułowane obawy o niebezpieczeństwo zastąpienia ludzi przez systemy sztucznej inteligencji w procesie edukacji wydaje się, że na ten moment można zaryzykować tezę, iż z uwagi na konieczność zapewnienia nadzorczej roli człowieka nad zadaniami wykonywanymi przez sztuczną inteligencję oraz procedur *compliance* pracy nie zabraknie ani nauczycielom, ani prawnikom.

⁵³ Pkt 3.5 AI Act.

⁵⁴ Na temat prawa podmiotu danych do informacji w kontekście AI por. K. Morawska, *Zasada transparentności i prawo podmiotu danych do informacji a sztuczna inteligencja*, [w:] *Prawo sztucznej...*, s. 187-198; G. Bar, *Przejrzystość, w tym wyjaśnialność, jako wymóg prawny dla systemów Sztucznej Inteligencji*, „Monitor Prawniczy 2020”, nr 20, dodatek, s. 75-79, Legalis.

Bibliografia

- Auleytner A., *Równość dostępu do sztucznej inteligencji*, „Automatyka” 2018, nr 11, s. 28-29.
- Auleytner A., Stępień M.J., *Dostęp do sztucznej inteligencji – równość i inne aspekty prawne dostępu do systemów sztucznej inteligencji*, „Monitor Prawniczy” 2019, nr 21, dodatek, Legalis.
- Bar G., *Przejrzystość, w tym wyjaśnialność, jako wymóg prawny dla systemów Sztucznej Inteligencji*, „Monitor Prawniczy” 2020, nr 20, dodatek, s. 75-79, Legalis.
- Bar G., Skibicki R., *Wyzwania prawne związane z wykorzystaniem sztucznej inteligencji w usługach cyfrowych*, „Prawo Nowych Technologii 2021”, nr 1, s. 40-45, Legalis.
- Byrski J., *Oprogramowanie zawierające elementy sztucznej inteligencji. Wybrane zagadnienia prawne*, [w:] *Experientia docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Trąpcie*, P. Kostański, P. Podrecki, T. Targosz (red.), Warszawa 2017, s. 1331-1343.
- Chat GPT w szkole. Szanse i zagrożenia*, Zintegrowana Platforma Edukacyjna Ministerstwa Edukacji i Nauki, <https://zpe.gov.pl/chat-gpt>.
- Chen L., Chen P., Lin Z., *Artificial Intelligence in Education: A Review*, „IEEE Access” 2020, nr 8, s. 75264-75278, <https://doi.org/10.1109/ACCESS.2020.2988510>.
- Committee on Artificial Intelligence (CAI), *Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, <https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f>.
- European Commission, Directorate-General for Education, Youth, Sport and Culture, *Final Report of the Commission Expert Group on Artificial Intelligence and Data in Education and Training. A Executive Summary*, Publications Office of the European Union, 2022, <https://data.europa.eu/doi/10.2766/65087>.
- Heaven W.D., *ChatGPT is Going to Change Education, Not Destroy It*, MIT Technology Review, 6.04.2023, <https://www.technologyreview.com/2023/04/06/1071059/chatgpt-change-not-destroy-education-openai/>.
- Juściński P., *Prawo autorskie w obliczu rozwoju sztucznej inteligencji*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” 2019, nr 1, s. 5-44.
- Komisja Europejska, *Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*, Bruksela, dnia 19.02.2020 r., COM(2020) 65 final.
- Komisja Europejska, Dyrekcja Generalna ds. Edukacji, Młodzieży, Sportu i Kultury, *Wytoczne etyczne dla nauczycieli dotyczące wykorzystania sztucznej inteligencji i danych w nauczaniu i uczeniu się*, Luksemburg 2022, <https://data.europa.eu/doi/10.2766/169>.
- Komisja Europejska, Wniosek. Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), Bruksela, dnia 28.09.2022 r., COM(2022) 496 final.
- Komisja Europejska, Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, Bruksela, dnia 21.04.2021 r., COM(2021) 206 final.
- Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Plan działania w dziedzinie edukacji cyfrowej na lata 2021-2027. Nowe podejście do kształcenia i szkolenia w epoce cyfrowej*, Bruksela, dnia 30.09.2020 r., COM(2020) 624 final.

- Komunikat Komisji, *Sztuczna inteligencja dla Europy*, Bruksela, dnia 25.04.2018 r., COM(2018) 237 final.
- Kurowska-Tober E., Czynienik Ł., Koniarska M., *Aspekty prawne sztucznej inteligencji – zarys problematyki*, „Monitor Prawniczy” 2019, nr 21, dodatek, Legalis.
- Lubasz D., Namysłowska M., *Ochrona danych osobowych a sztuczna inteligencja*, [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 1009-1030, Meritum.
- Lubasz D., Szkurlat A., *Relacja aktu o sztucznej inteligencji i ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy” 2022, nr 21, dodatek, Legalis.
- Madiega T., *General-Purpose Artificial Intelligence*, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA\(2023\)745708_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf).
- Michalak A., *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021, *Monografie Prawnicze*.
- Michałowicz A., *Przetwarzanie danych biometrycznych a ochrona jednostek – analiza wybranych zagadnień na tle ogólnego rozporządzenia o ochronie danych i projektu aktu w sprawie sztucznej inteligencji*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2021, nr 6(10), s. 78-94, Legalis.
- Morawska K., *Zasada transparentności i prawo podmiotu danych do informacji a sztuczna inteligencja*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, s. 187-198, *Monografie Prawnicze*.
- Nowakowski M., *O moralnej odpowiedzialności HAL-a 9000, czyli etyka sztucznej inteligencji w praktyce. Czy potrzebujemy definicji sztucznej inteligencji?*, „Prawo Mediów Elektronicznych” 2022, nr 1, s. 4-10, Legalis.
- Nowakowski M., *Ostatnie zmiany w ramach prawnych dla sztucznej inteligencji w Unii Europejskiej – krytyczna analiza*, „Prawo Nowych Technologii” 2021, nr 2, s. 23-30, Legalis.
- OECD, *Recommendation of the Council on Artificial Intelligence*, 22.05.2019, <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#mainText>.
- O’Flaherty M., *Facial Recognition Technology and Fundamental Rights*, „European Data Protection Law Review” 2020, vol. 6, no. 2, s. 170-173, <https://doi.org/10.21552/edpl/2020/2/4>.
- Oreżiak B., *Prawa człowieka jako determinanta sztucznej inteligencji? Propozycja kryteriów i dyrektyw zastosowania sztucznej inteligencji do użytku praktycznego*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, s. 199-210, *Monografie Prawnicze*.
- Ostateczna lista oceny godnej zaufania sztucznej inteligencji (ALTAI)*, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.
- Poprawki przyjęte przez Parlament Europejski w dniu 14 czerwca 2023 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html.
- Rada Unii Europejskiej, *Podjęcie ogólne*, Bruksela, dnia 25.11.2022 r., <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/pl/pdf>.
- Rapcewicz A. et al., *Sztuczna inteligencja w kontekście ochrony danych osobowych. Materiały pokonferencyjne*, <https://uodo.gov.pl>.

- Regorowicz M., Konieczny P., *Konwencja Rady Europy w sprawie sztucznej inteligencji*, <https://www.traple.pl/konwencja-rady-europy-w-sprawie-sztucznej-inteligencji/>.
- Rezolucja Parlamentu Europejskiego z dnia 19 maja 2021 r. w sprawie sztucznej inteligencji w sektorze edukacji i kultury oraz w sektorze audiowizualnym, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0238_PL.html.
- Rzymowski J., *Definicja prawnicza sztucznej inteligencji na podstawie projektu rozporządzenia w sprawie sztucznej inteligencji*, „Prawo Nowych Technologii” 2023, nr 1, s. 19-23, Legalis.
- Rojszczak M., *Prawne aspekty systemów sztucznej inteligencji – zarys problemu*, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2019, s. 1-22.
- Susałko M., *Podejście oparte na ryzyku w projekcie aktu w sprawie sztucznej inteligencji i RODO*, „Prawo Nowych Technologii” 2023, nr 1, s. 10-18, Legalis.
- Szpyt K., *Sztuczna inteligencja i nowe technologie (nie zawsze) w służbie ludzkości, czyli cywilnoprawna problematyka rozwoju i popularyzacji technologii deepfake*, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), Warszawa 2019, s. 75-94.
- „Sztuczna Inteligencja w edukacji”. Wywiad... ze Sztuczną Inteligencją, https://elearning.uj.edu.pl/aktualnosci/-/journal_content/56_INSTANCE_VYFRNkIOU5HR/153579096/153958753.
- Sztuczna inteligencja w szkole*, https://poland.representation.ec.europa.eu/news/sztuczna-inteligencja-w-szkole-2022-10-26_pl.
- The 2018 International Computer and Information Literacy Study (ICILS): Main Findings and Implications for Education Policies in Europe*, <https://education.ec.europa.eu/sites/default/files/document-library-docs/icils-2018-policy-note.pdf>.
- Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, <https://digital-strategy.ec.europa.eu/pl/node/1950>.
- Zalecenia polityczne i inwestycyjne dotyczące godnej zaufania sztucznej inteligencji*, <https://digital-strategy.ec.europa.eu/pl/node/1694>.

Niniejsza monografia powstała jako trzecia w serii Krakow Jean Monnet Research Papers w ramach realizowanego przez Katedrę Prawa Europejskiego Uniwersytetu Jagiellońskiego projektu Jean Monnet Module pt. „E-administracja — europejskie wyzwania dla administracji publicznej w państwach członkowskich UE i krajach partnerskich/eGovEU+”.

Przedstawia ona analizę wdrożenia i funkcjonowania cyfrowych usług publicznych w Polsce i w Europie ze szczególnym uwzględnieniem związanych z tym wyzwań. Dotyczą one m.in. rozwoju infrastruktury teleinformatycznej, zapobiegania wykluczeniu cyfrowemu oraz zapewniania ochrony prywatności i bezpieczeństwa obywatelom.

Książka adresowana jest do badaczy zajmujących się administracją, prawem administracyjnym i europejskim oraz do praktyków w wymienionych dziedzinach. Mamy nadzieję, że publikacja poszerzy wiedzę czytelników na temat cyfryzacji usług publicznych oraz zachęci środowisko naukowe do dalszych badań w tym zakresie.

This monograph is the third in the Krakow series of Jean Monnet Research Papers and was written as part of the Jean Monnet Module project, carried out by the Chair of European Law at the Jagiellonian University, “E-government — European Challenges for Public Administration in EU Member States and Partner Countries/eGovEU+.”

The book presents an analysis of the implementation and functioning of digital public services in Poland and Europe with a particular focus on the challenges involved. These include the development of ICT infrastructure, preventing digital exclusion and ensuring privacy and security of citizens.

The monograph is addressed to researchers in administration, administrative and European law as well as to practitioners in the mentioned fields. We hope the publication will broaden the readers' knowledge of the digitization of public services and encourage the scientific community to further research in this area.



<https://akademicka.pl>

