https://doi.org/10.21784/ZC.2023.015

Jarosław Bugajski
Uczelnia Nauk Społecznych

Sztuczna inteligencja – zagrożenie czy bezpieczeństwo?

Artificial intelligence –threat or security?

Abstrakt. Postęp technologiczny na przestrzeni ostatnich lat doprowadził do wysokiego rozwoju sztucznej inteligencji (SI), która niesie ze sobą wiele pozytywnych aspektów, ale jednocześnie może doprowadzić do naruszenia praw podstawowych jednostek i tym samym zagrozić bezpieczeństwu społecznemu. Wychodząc zatem od zagadnień związanych z rozwojem i zagrożeniami ze strony SI, podjęta została analiza prawna polityki regulacyjnej w odniesieniu do praw człowieka.

Słowa kluczowe: sztuczna inteligencja, system SI, AI, nowoczesne technologie, zagrożenia, bezpieczeństwo

Abstract. Technological progress in recent years has led to the high development of artificial intelligence (AI), which brings many positive aspects, but at the same time can lead to the violation of the fundamental rights of individuals and thus threaten social security. Therefore, starting from the issues related to the development and threats from AI, a legal analysis of the regulatory policy in relation to human rights was undertaken.

Keywords: artificial intelligence, SI system, AI, modern technologies, threats, security

Wstęp

W procesie rozwoju i wpływu nowoczesnych technologii, a szczególnie sztucznej inteligencji (SI) (*artificial intelligence*, AI), na życie i funkcjonowanie społeczeństwa istotną staje się kwestia dotycząca granic rozwoju i ich oddziaływania społecznego. Zjawisko to bowiem staje

się przyczyną zagrożenia dla poczucia bezpieczeństwa społeczeństwa między innymi na płaszczyźnie etycznej jak i prawnej, dlatego też dużą wagę przykłada się do problemów związanych z ochroną praw człowieka. Istotnymi zagrożeniami stają się zatem potencjalne dyskryminujące działania tej technologii dotyczące naruszenia prywatności, wykluczenia cyfrowego, rosnącej nierówności oraz bezrobocia. W związku z tym należy zauważyć, iż rozwój nowoczesnych technologii SI niesie ze sobą nowe wyzwania w zakresie prawodawstwa normującego wspomniane kwestie. Wychodząc zatem od rozwijającego się dość szybko systemu sztucznej inteligencji w kontekście rozwoju gospodarczego, podjęto próbę określenia sytuacji prawnej polityki regulacyjnej w zakresie SI, mającej przełożenie na bezpieczeństwo społeczne.

Rozwój i zagrożenia SI

Sztuczna inteligencja jest systemem informatycznym stworzonym przez człowieka rozwijającym się jako multidyscyplinarny obszar badawczy. Dlatego też przyjąć należy, iż powstał on na przecięciu nauk filozoficznych, matematycznych, ekonomicznych, psychologicznych, neuronauki, teorii kontroli, robotyki oraz inżynierii komputerowej.[1] W ramach wspomnianego obszaru rozwijanych jest szereg technologii obliczeniowych i informatycznych, a do głównych ich funkcji należy zaliczyć uczenie maszynowe, przetwarzanie języka naturalnego, automatyczne wnioskowanie, przewidywanie, optymalizowanie, nawigowanie i rekomendowanie, rozpoznawanie oraz generowanie mowy i obrazu. Sztuczna inteligencja poprzez swe zastosowania jest technologią dynamicznie transformującą dotychczasowe modele gospodarcze, relacje społeczne, organizację państwa oraz stosunki międzynarodowe. Niewątpliwie kompetencją podstawową, na której opiera się stosowanie sztucznej inteligencji jest nauka o danych (*data science*). Dlatego też

[1] Zob. A. Berdowska, *Wspomaganie procesu rekrutacji pracowników za pomocą chatbotów – analiza wybranych rozwiązań*, Zarządzanie Zasobami Ludzkimi 2018, Nr 5, s. 93–112; M. Jankowska-Augustyn, *Podmiotowość prawna sztucznej inteligencji?* [w:] A. Bielska-Brodziak (red.), *O czym mówią prawnicy, mówiąc o podmiotowości*, Katowice 2015, s. 171.

mowa jest zatem o nowej gospodarce opartej na niewidzialnych aktywach, gdzie dzięki sztucznej inteligencji całkowicie zmienia się sposób poznania, przetwarzania oraz organizacji rzeczywistości. Sztuczna inteligencja wykraczając poza ograniczenia umysłowe człowieka może przewidywać zjawiska i zachowania, autonomizować maszyny i procesy, czy wreszcie rozumieć sytuacje tak złożone, że nie byłby tego w stanie, w tak szybkim czasie, dokonać ludzki umysł. Nowoczesne technologie powiązane ze zjawiskiem cyfrowej transformacji (*digital transformation*) społeczeństwa mają zatem niewątpliwie wpływ na każdy obszar ludzkiej egzystencji.[2]

Obok szans związanych z ekspansją technologiczną istnieją także liczne zagrożenia, gdzie do najczęstszych można zaliczyć ryzyko nadmiernej inwigilacji społeczeństwa.[3] Istotnymi są również wielopłaszczyznowe zagrożenia prawa do prywatności oraz zagrożenia wynikające z istnienia zdematerializowanej cyberprzestrzeni (m.in. *phishing*, s*pamming*, kradzież tożsamości, *sniffing*, mowa nienawiści „hejt", *deep fakes*). Do zagrożeń natomiast o charakterze ogólnospołecznym można zaliczyć wykluczenie cyfrowe, lukę cyfrową lub podział cyfrowy, *digital divide* oraz przestępczość komputerową. Należy przy tym podkreślić, iż technologia sama w sobie wymyka się spod ocen etycznych, a kluczowym w tej mierze staje się przede wszystkim sposób jej wykorzystania.[4]

Rozwój technologiczny jest uwarunkowany dostępem do możliwie największej ilości danych, ponieważ to dane są podstawowym motorem napędowym wszelkich zjawisk technologicznych. Istnienie i możliwość dalszego rozwoju AI uzależnione jest od olbrzymich zaso-

[2] K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii*, cz. I, rozdz. I, 2015, LEX, s. 191.

[3] Zob. T.F. Chan, *System oceny obywateli w Chinach powstrzymał już ludzi od 11 mln lotów i 4 mln podróży pociągiem*, https://businessinsider.com.pl/lifestyle/podroze/system-oceny-obywateli-w-chinach-efekty-dzialania/7yl1phz (dostęp: 30.03.2023).

[4] M. Bellon, *Szef technologicznego giganta: AI podzieli świat. Społeczeństwa bez niej będą biedniejsze i słabsze*, https://businessinsider.com.pl/technologie/marc-benioff-ceo-salesforce-o-sztucznej-inteligencji/zx4tq1m (dostęp: 26.03.2023).

bów danych, a stopniowe upowszechnienie AI należy wiązać również z możliwością analiz olbrzymich, złożonych nawet z miliardowych ilości rekordów, baz danych (*Big Data*).[5] Dlatego też najistotniejszym zagadnieniem wiążącym rozwój technologiczny z bezpieczeństwem dla społeczeństwa jest pytanie o prawny status danych.

Prawna polityka regulacyjna w zakresiesztucznej inteligencji

Wraz z rozwojem „nowoczesnych technologii" zawsze pojawiają się problemy dotyczące zarówno etycznych, jak i prawnych regulacji związanych z zasadami funkcjonowania komputerów oraz robotów. Najczęściej stawiane pytania w tym zakresie odnoszą się do kwestii stanowienia prawa i paradoksalnie dotyczą one odpowiedzialności człowieka za podejmowane działania przy wykorzystaniu komputerów, jak również odpowiedzialności komputerów za działania w stosunku do człowieka.[6] W szerokich obszarach działalności komputerów zdolnych do analizy oraz rozwiązywania problemów rodzi się wiele dylematów odnośnie pojawiających się nowych zagadnień i niejasności, a szczególnie w zakresie etyki. Dylematy te stają się fundamentalnym elementem określającym stopień odpowiedzialności, który stanowi jednocześnie jeden z większych problemów prawnych w kontekście nowoczesnych technologii. Powstaje zatem słuszny podstawowy dylemat dotyczący procesu stanowienia prawa w kontekście działań SI, dotyczący tego czy komputery mogą być odpowiedzialne za swoje działania oraz czy odpowiedzialność za komputer ponosi twórca lub właściciel oprogramowania czy posiadacz rzeczy. Należy stwierdzić, iż podstawową odpowiedzią na ten dylemat jest kwestia ustalenia posiadania osobowości prawnej. Natomiast w różnych stanowiskach teoretyków prawa dowo-

[5] M. Rojszczak, *Prawne aspekty systemów sztucznej inteligencji – zarys problemu* [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019, s. 3-6.

[6] S. Braman, *Change of State: Information, Policy, and Power*, Cambridge: MIT Press, 2006, s. 278.

dzi się, iż powinno się rozróżniać zachowanie robotów jako narzędzi interakcji międzyludzkich z zachowaniem robotów jako podmiotów w sferze prawnej.[7] W obecnym rozwoju nowoczesnych technologii omawiana kwestia staje się kluczowym priorytetem dla zadań ustawodawcy, tym bardziej, iż prawna doktryna cyberodpowiedzialności jest szczególnie istotna w obliczu zmian życia w warunkach rozwoju sztucznej inteligencji.[8]

Obecnie zasady odpowiedzialności określa ukształtowane w sferze prawa rozróżnienie między *hardware* i *software*, dlatego też potencjalne niebezpieczeństwo stwarzane przez sztucznie inteligentne maszyny zwiększa się z momentem powstania, a szczególnie gdy stają się one mobilne. Dynamika rozwoju cyberprzestrzeni oraz sztucznej inteligencji i robotyki znacznie przewyższają możliwości prawodawców. Sztuczna inteligencja nie doczekała się jeszcze definicji legalnej, choć w oparciu o działania SI funkcjonują m.in. programy do automatycznego tworzenia informacji, programy asystentów głosowych (*Google Assistant*), programy diagnostyczne stosowane w medycynie, rozpoznawania twarzy.[9] Technologia SI może być również wykorzystywana w świadczeniu usług prawnych, gdzie znane są już zastosowania SI w informatyce prawniczej, w procesie tworzenia prawa i rozstrzygania sporów on-line. [10] Stosowanie technologii SI zatem coraz częściej porusza kwestie natury prawnej. Polityka regulacyjna dotycząca SI znajduje również swoje odzwierciedlenie w strategiach, które kształtują tym samym obraz przyszłych regulacji i są podstawowym elementem w procesie stanowienia prawa.[11] Dlatego też zagadnienie SI wraz

[7] U. Pagallo, *The Laws of Robots Crimes, Contracts, and Torts*, Dordrecht Heidelberg New York: Springer, 2013, s. 79.

[8] K. Chałubińska–Jentkiewicz, *Cyberodpowiedzialność*, Toruń: Wydawnictwo Adam Marszałek, 2019, s. 110.

[9] G. Hallevy, *Liability for Crimes Involving Artificial Intelligence Systems*, Switzerland: Springer, 2015, s. 3.

[10] Ł. Goździaszek, *Perspektywy wykorzystania sztucznej inteligencji w postępowaniu sądowym*, „Przegląd Sądowy" 2015, nr 10.

[11] D. Dervanović, "Inhuman Lawyer: Developing Artificial Intelligence in the Legal Profession." *In Robotics, AI and the Future of Law*, ed. Marcelo Corrales, Mark Fenwick, and Nikolaus Forgo, 209–34. Singapore: Springer, s. 209.

z strategiami regulacyjnymi najlepiej odzwierciedlają obecne tendencje ustawodawcze związane z rozwojem nowoczesnych technologii. Polityka regulacyjna dotycząca SI zakłada ewidentnie potrzebę zmian regulacyjnych podyktowanych względami etyki SI wynikającymi z konieczności powiązania jej z wartościami o charakterze powszechnym. Chodzi tu zatem przede wszystkim o ochronę danych, prawo do prywatności, ochronę własności intelektualnej, ustalenie zasad odpowiedzialności karnej i cywilnej. W związku z tym cele przyszłej regulacji wydają się być oczywiste i standardowe, jednak w kontekście samego stanowienia prawa we wskazanym obszarze, polityka poszczególnych państw zasadniczo się różni, gdyż państwa członkowskie Unii Europejskiej (UE) minimalizują swoje zaangażowanie w stanowieniu nowego prawa odnośnie SI oczekując regulacji na poziomie Parlamentu Europejskiego.[12]

Sztuczna inteligencja jest zagadnieniem interdyscyplinarnym, dlatego też w tych okolicznościach wymagana jest strategia wypracowana w oparciu o złożoną analizę uwzględniającą wiele aspektów zjawiska SI.[13] Polska stoi na stanowisku popierającym kraje odmawiające nadania systemom SI statusu obywatelstwa, czy też osobowości prawnej. Opowiada się zatem za koncepcją supremacji człowieka nad systemami SI, a przez to odpowiedzialnością ludzką, osobistą, czy też osób prawnych, których człowiek jest założycielem i zarządcą. Reżim prawa prywatnego międzynarodowego również nie dopuszcza czynnego udziału typu sztucznej inteligentnej osoby prawnej w obrocie prawnym.

W niedalekiej przyszłości życie społeczne toczyć się będzie w środowisku wszechobecnych systemów autonomicznych realizujących własne, a nie ludzkie procesy decyzyjne. Stanowisko państwa oraz prawa

[12] Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, 2015/2103(INL); Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy", Bruksela (25.04.2018), COM (2018) 237 final.

[13] M. Hildebrandt, „From Galatea 2.2 to Watson- and back?" *In Human Law and Computer Law: Comparative Perspectives*, ed. Mireille Hildebrandt, and Jeanne Gaakeer, 23–45. Dordrecht: Springer, 2013, s. 42.

jest jednak dosyć jasne w tym zakresie, gdyż z punktu widzenia konstytucji to człowiek decyduje o funkcjonowaniu państwa, czy to w sposób bezpośredni czy też pośredni. Przesunięcie natomiast punktu ciężkości na systemy autonomiczne spowoduje, iż takie sytuacje przestaną w większości mieć miejsce. Póki co każdy przejaw działalności człowieka jest wobec niezmiennych podstaw konstytucyjnych kreowany przez wolę współobywateli. W pracach nad odpowiednim usankcjonowaniem SI, kluczowa jest decyzja odnośnie przyjęcia założenia konstytucyjnego, iż wszelkie systemy autonomiczne muszą podlegać kontroli człowieka z niezbywalnym prawem do ingerencji oraz zmiany decyzji SI, aż po jej wyłączenie, co powinno stanowić punkt wyjścia do dalszych prac oraz dyskusji. Określenie zatem tej sytuacji na poziomie konstytucyjnym przekładać się powinno na regulacje prawne na płaszczyźnie ustawowej. W związku z tym zapotrzebowanie na wprowadzenie normy generalnej w omawianym zakresie wydaje się być oczywiste, tym bardziej w świetle standardów konstytucyjnych oraz konwencyjnych. Należy przy tym podkreślić, iż wszystkie normy konstytucyjne czynią człowieka centralnym punktem systemu prawa, co wynika z Konstytucji Rzeczpospolitej Polskiej (art. 1 Konstytucji RP)[14]. Podobne założenia wynikają również z europejskiej konwencji praw człowieka (EKPC)[15] oraz Karty praw podstawowych Unii Europejskiej (KPP).[16]

Na podstawie powyższych regulacji prawnych nieakceptowalne jest aktualnie, aby maszyny miałaby w jakimkolwiek stopniu stać wyżej niż prawa i wolności człowieka, ponieważ to właśnie człowiek pozostaje jedynym centrum i celem tych praw, natomiast system technologiczny SI powinien zawsze odgrywać rolę służebną wobec człowieka. Dlatego też konstruowanie norm niższego rzędu odnośnie funkcjonowania SI musi niewątpliwie pozostawać w zgodzie z prawami człowieka

[14] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 r. nr 78, poz. 483.

[15] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 r. nr 61, poz. 284.

[16] Karta Praw Podstawowych Unii Europejskiej, Dz.Urz. UE C 326, s. 391.

i nie może tych praw w żaden sposób naruszać.[17] Chodzi zatem przede wszystkim o prawa człowieka do poszanowania jego życia prywatnego i rodzinnego, domu i korespondencji, komunikowania się oraz ochrony czci i dobrego imienia oraz decydowania o swoim życiu osobistym (art. 47 Konstytucji RP, art. 7 KPP UE oraz w art. 8 EKPC). Dotyczy to również jego danych osobowych (art. 8 KPP i RODO[18]), wolności wypowiedzi (w art. 54 Konstytucji RP, art. 11 KPP UE oraz w art. 10 EKPC) oraz nie może także działać w sposób dyskryminujący (art. 32 Konstytucji RP, art. 21 KPP UE oraz art. 14 EKPC).

Zabezpieczeniem przed wszelkim zagrożeniem odnośnie nadmiernego rozwoju systemów SI ograniczającego prawa człowieka jest niewątpliwie RODO, gdyż dostęp do danych ma fundamentalne znaczenie. Dlatego też osiągnięcie określonych założonych celów SI możliwe jest wyłącznie przy uzyskaniu ogromnej liczby spersonalizowanych, wrażliwych informacji. Istnieje zatem niebezpieczeństwo, iż ze względu na wymogi technologii potrzeba wyrażenia zgody na przetwarzanie danych osobowych stanie się jedynie pustą formalnością. Natomiast bez udzielenia takiej zgody w zasadzie nie da się właściwie żyć w nowoczesnym społeczeństwie, a idąc dalej, potrzeba zwiększenia funkcjonalności systemu technologicznego jako całości wymusi w praktyce rezygnację albo z przepisów RODO, albo z ich rzeczywiście proobywatelskiej interpretacji.[19]

W świetle praw człowieka, istnienie normy podstawowej, która zawsze uznawałaby wolę człowieka za ważniejszą od woli maszyny (SI), wydaje się być czymś oczywistym, którą to normę można zarówno

[17] B. Oręziak, *Prawa człowieka jako determinanta sztucznej inteligencji? Propozycja kryteriów i dyrektyw zastosowania sztucznej inteligencji do użytku praktycznego*, [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, C.H.Beck, Warszawa 2020, s. 245.

[18] Rozporządzenie PE 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.L.2016.119.1.

[19] D. Ćwiklak, *Mój brat robot. Kiedy zastąpią nas maszyny?* 2017, https://www.newsweek.pl/biznes/roboty-i-ludzie-maszyny-i-technologia-zastapia-nas-w-pracy/c537m19 (dostęp: 30.03.2023).

wpisać do konstytucji, jak również zrekonstruować na podstawie istniejących już przepisów konstytucyjnych czy konwencyjnych. Rekonstrukcja jednak takiej normy rodzi pytania o odpowiedzialność za działanie SI podległej człowiekowi. Jak również o rzeczywiste możliwości faktyczne i prawne realizacji takiej nadrzędności. Można zatem stwierdzić, iż rozwój prawa zmierza w omawianym zakresie do swoistej hipokryzji normatywnej polegającej na deklaratywnym przyjmowaniu wskazanej nadrzędności z równoczesnym faktycznym powierzeniem decyzji maszynom świata.

Sztuczna inteligencja w regulacjach Unii Europejskiej – Biała Księga

Komisja Europejska opublikowała Białą Księgę w sprawie sztucznej inteligencji, którą można uznać, jako Europejskie podejście do doskonałości i zaufania.[20] Opublikowanie i przedstawienie opracowań z tego zakresu miało na celu przede wszystkim znalezienie odpowiedniego kierunku działań organów Unii Europejskiej oraz ustalenie wymagań jakie powinny spełniać ramy prawne dla rozwoju sztucznej inteligencji. Zwrócono również uwagę na korzyści związane z rozwojem technologii, która ma być dostosowana do interesów państw członkowskich Unii Europejskiej i przede wszystkim do jej obywateli[21]. Kwestie te zostały ujęte również w opracowaniach Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji powołanej przez Komisję Europejską. Istotnym aktem przywołanej Komisji jest dokument: „Wytyczne z zakresie etyki dotyczące godnej zaufania sztucznej inteligencji" z dnia 10 kwietnia 2019 roku[22]. Celem przywołanego dokumentu jest promowanie godnej zaufania sztucznej inteligencji, która powinna posiadać

[20] Biała Księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania z dnia 19 lutego 2020 r., COM (2020) 65 final.

[21] D. Lubasz, *Konstruowanie humanocentrycznej SI z wykorzystaniem instru-mentów prawnych ochrony danych osobowych* w: Sztuczna inteligencja w kontekście ochrony danych osobowych, 2020, s. 20.

[22] Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji,* 2019.

trzy cechy mające charakteryzować wyposażony w nią system, przez cały jego cykl życia. Powinna zatem być zgodna z prawem, tj. przestrzegać wszystkich obowiązujących przepisów ustawowych i wykonawczych oraz powinna być etyczna – zapewniając zgodność z zasadami i wartościami etycznymi i w końcu solidna zarówno z technicznego, jak i ze społecznego punktu widzenia, czyli nie przynosząca żadnych niezamierzonych szkód.[23] Należy przy tym podkreślić, iż wspomniane wytyczne stanowią tylko istotne wskazówki do bezpiecznego korzystania ze sztucznej inteligencji, natomiast nie posiadają mocy wiążącej dla organów Unii Europejskiej. W związku z tym warto przywołać kilka istotnych wymogów, na które ten dokument stawia. Systemy sztucznej inteligencji powinny zatem wskazywać na przewodnią i nadzorczą rolę człowieka i zapewniać odpowiednią ochronę prywatności oraz zarządzanie danymi. Kolejny istotny wymóg dotyczy dążenia do poprawy identyfikowalności i możliwości kontrolowania systemów. SI powinna również w sposób przejrzysty i proaktywny przekazywać zainteresowanym stronom informacje na temat możliwości i ograniczeń systemu, co powinno stać się istotną wskazówką dotyczącą odpowiedniej działalność edukacyjnej polepszającej świadomość społeczeństwa w tym zakresie.[24]

Powyższa analiza wskazuje ewidentnie istotną potrzebę udziału człowieka w kontekście tworzenia systemów SI i ich nadzorowania. Celem zatem wszystkich regulacji Unii Europejskiej w kontekście rozwoju SI jest i zawsze powinna być maksymalizacja korzyści, jakie przynosi sztuczna inteligencja, przy jednoczesnym ograniczeniu ryzyka niosącego ze sobą, gdyż wdrożenie sztucznej inteligencji powinno służyć dobru ogólnemu. W związku z tym opracowania organów Unii Europejskiej skupiają się między innymi na kwestii ochrony danych osobowych, gdzie można zauważyć wiele podstawowych problemów. Należy do nich zaliczyć sprzeczność między innowacjami w obszarze *big data* a ochroną danych, wdrażanie *big data* zgodnie z wymogami społecznymi i etycznymi, zapewnienie bezpieczeństwa przepływu danych osobowych, ograniczenia techniczne, przede wszystkim w kontekście

[23] Ibidem, s. 2.
[24] Ibidem, s. 3.

anonimizacji i pseudonimizacji, pochodzenie danych z innego rodzaju źródeł, w tym także ze źródeł niezweryfikowanych bądź niezaufanych, konieczność zapewnienia bezpieczeństwa danych osobowych na szczeblu globalnym i uregulowanie w odpowiedni sposób obowiązków administratorów danych.[25]

Sztuczna inteligencjaa prawa człowieka

W związku z tym, że sztuczna inteligencja jest rozwiązaniem innowacyjnym i niesie ze sobą spore ryzyko, zarówno Unia Europejska jak i jej państwa członkowskie dostrzegają konieczność wprowadzenia regulacji nowych technologii z poszanowaniem dla ludzkiej godności i praw człowieka. Podstawowym aktem Prawa Unii Europejskiej regulującym podstawowe prawa człowieka jest Karta Praw Podstawowych (KPP).[26] Dlatego też według art. 1 ww. aktu godność człowieka jest nienaruszalna, musi być szanowana oraz chroniona i każdy ma prawo do ochrony danych osobowych (art. 8 KPP). Ponadto dane te powinny być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, jak również każdy ma prawo do dostępu do zebranych danych, które go dotyczą i prawo do dokonania ich sprostowania. Tworzenie i regulowanie sztucznej inteligencji w ścisłym związku z prawami człowieka jest jednak na skalę światową rzadkim zjawiskiem, jak np. w Azji (szczególnie w Chinach), gdzie przy tworzeniu systemów AI, takie wartości jak godność i inne podstawowe prawa człowieka nie odgrywają bowiem istotnej roli.[27] Zgodnie z zaleceniami organów Unii Europejskiej, rozwijanie algorytmów sztucznej inteligencji w UE powinno odbywać się nie tylko z poszanowaniem godności człowieka, ale także z jednoczesną ochroną danych osobowych obywateli UE. W tym kontekście warto wskazać, że od 2018 roku na terenie całej Unii Europejskiej obowiązują przepi-

[25] D. Lubasz, *Konstruowanie humanocentrycznej SI…*, op.cit, s. 21.

[26] Karta Praw Podstawowych Unii Europejskiej (2016/C 202/02).

[27] Deloitte, Europejskie regulacje dot. sztucznej inteligencji, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/europejskie-regulacje-sztuczna-inteligencja-COVID-19.html (dostęp: 30.03.2023).

sy 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[28] i jest to ogólne rozporządzenie o ochronie danych (RODO). Wprowadzanie sztucznej inteligencji powinno odbywać się zatem zgodnie z ww. regulacją, która obowiązuje jedynie na terenie państw członkowskich Unii Europejskiej. W tym miejscu warto przywołać treść art. 22 ust. 1 RODO który wskazuje na zapewnienie interwencji człowieka w przypadku podejmowania decyzji w sposób zautomatyzowany. Zgodnie z ww. regulacją, osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Analizując przepisy prawa Unii Europejskiej, które mają charakter powszechnie obowiązujący (rozporządzenia, dyrektywy), można zauważyć, że wszelkich regulacji prawnych odnoszących się do postępującego rozwoju sztucznej inteligencji jest stosunkowo niewiele. W przywoływanej już Białej Księdze wskazano, że obecnie Europa znajduje się jeszcze na słabej pozycji w dziedzinie zastosowań konsumenckich i platform internetowych.[29] Warte podkreślenia jest również, iż według zapisów Białej Księgi wykorzystywanie sztucznej inteligencji może mieć wpływ także na wartości na których zbudowana jest Unia i nieodpowiednie unormowanie tego faktu może prowadzić do naruszenia praw podstawowych.[30] Istnieje bowiem niebezpieczeństwo, iż systemy AI mogą ograniczać podstawowe prawa, takie jak między innymi prawo do wolności wypowiedzi i zgromadzeń oraz prawo do dochodzenia

[28] 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. .UE.L 2016 Nr 119).

[29] Biała Księga w sprawie…op.cit., s. 5.

[30] Z badań Rady Europy wynika, że korzystanie ze sztucznej inteligencji może mieć wpływ na wiele praw podstawowych: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (dostęp: 29.03.2023).

odszkodowania na drodze sądowej i rzetelnego procesu. Mogą wpływać również na dyskryminację ze względu na płeć, rasę, pochodzenie etniczne, religię lub wierzenia, niepełnosprawność, wiek oraz orientację seksualną i ochronę danych osobowych i życia prywatnego, czy też ochronę konsumentów. Dlatego też sztuczna inteligencja jeśli będzie wprowadzana w sposób nieprawidłowy, stanowić będzie potencjalne ryzyko do naruszenia praw podstawowych obywateli Unii Europejskiej.

Zagrożenia, prewencja i bezpieczeństwo

Odnośnie zagrożeń dotyczących praw człowieka związanych ze stosowaniem sztucznej inteligencji warto odnieść się między innymi do Raportu FRA[31] (Agencja Praw Podstawowych Unii Europejskiej – FRA)[32]. Wskazano w nim wykorzystanie systemu kategoryzacji osób bezrobotnych działającego w 2014 r. w Polsce, gdzie tworzenie profilu kandydata na podstawie wprowadzonych informacji stało się jedną z metod przetwarzania tych danych. Skutkowało to zakwalifikowaniem człowieka do jednej z określonych kategorii mający przy tym doniosły wpływ na jego przyszłość. System ten kierowany przez AI ukazał problemy związane z wykorzystaniem algorytmów stworzonych poza bezpośrednią kontrolą człowieka w administracji publicznej. Dlatego też działanie systemu spotkało się z dużą krytyką ze strony społeczeństwa w związku z brakiem możliwości zakwestionowania przyporządkowania bezrobotnego do konkretnego profilu. Pomimo konstytucyjnego prawa do zaskarżania orzeczeń i decyzji zawartego w art. 78 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., finalnie w odpowiedzi na te działania Rzecznik Praw Oby-

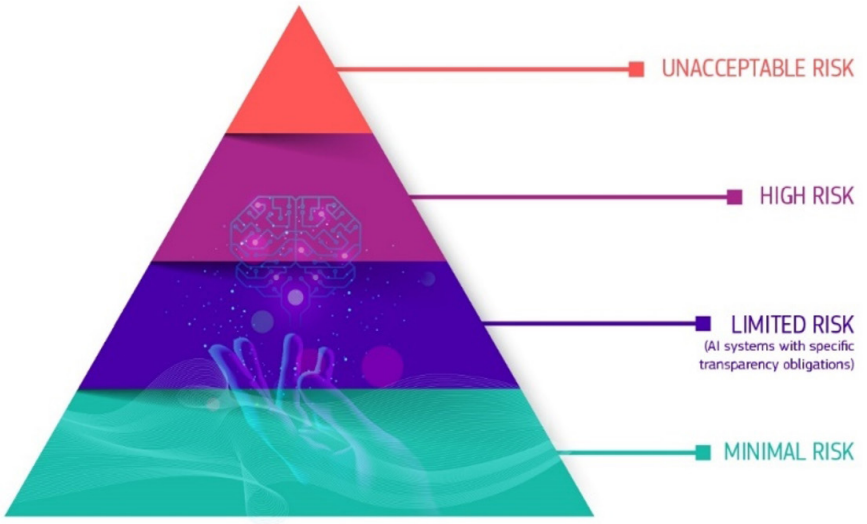
[31] *Naprawić przyszłość. Sztuczna inteligencja a prawa podstawowe. Podsumowanie*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_pl.pdf (dostęp: 26.03.2023).

[32] Niezależny ośrodek odniesienia i doskonałości w zakresie promowania i ochrony praw człowieka w UE. Pomaga bronić praw podstawowych wszystkich ludzi żyjących w UE. *European Union Agency For Fundamental Rights,* https://fra.europa.eu/en (dostęp: 27.03.2023).

watelskich złożył skargę do Trybunału Konstytucyjnego. W Raporcie wyraźnie wykazano, że stosowanie systemów sztucznej inteligencji może naruszać szereg praw podstawowych gwarantowanych przez Kartę praw podstawowych, jak i pozostałe akty prawne obowiązujące w państwach członkowskich UE.

Wiele przedsiębiorstw i organów administracji publicznej już korzysta lub planuje korzystać z SI i powiązanych technologii. Prace nad SI są jednak wciąż na różnym etapie zaawansowania. Natomiast w związku z nieuniknionym i niepohamowanym rozwojem technologii, FRA sugeruje, iż tworząc przyszłe akty normatywne w zakresie sztucznej inteligencji należy zapewnić, aby SI przestrzegało wszystkich praw podstawowych zawartych szczególnie w KPP. FRA proponuje również zagwarantowanie obywatelom możliwości zaskarżenia decyzji podjętych przez SI. Tym samym istotna jest weryfikacja działania systemów SI pod względem naruszania praw podstawowych oraz stworzenie przez UE wspólnego systemu kontroli nad podmiotami korzystającymi z SI. Pomimo wielu obaw, należy jednak stwierdzić, że obecny rozwój technologiczny i zwiększona dostępność danych stwarzają również wyjątkową możliwość lepszego zrozumienia struktur społecznych. Można to zatem wykorzystać do wspierania przestrzegania praw podstawowych jak również rozwiązania, które umożliwia zastosowanie sztucznej inteligencji. Może to doprowadzić do lepszego zrozumienia przyczyn, a w konsekwencji do złagodzenia skutków naruszeń praw podstawowych i do zagwarantowania bezpieczeństwa.

Proponowane ramy prawne dla sztucznej inteligencji bazują na wyodrębnieniu czterech kategorii systemów SI. Uzależnione są one od poziomu ryzyka jakie stwarza ich zastosowanie, a mianowicie ryzyka niedopuszczalnego, wysokiego, ograniczonego i minimalnego, co przedstawia poniższa grafika:



Źródło: *Budowanie zaufania przez pierwsze w historii ramy prawne dotyczące sztucznej inteligencji*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_pl (dostęp: 28.03.2023).

Odnośnie ryzyka niedopuszczalnego *(unacceptable*)[33] zalicza się tutaj systemy sztucznej inteligencji sprzeczne z unijnymi wartościami poszanowania godności ludzkiej, wolności, równości, demokracji i praworządności oraz z prawami podstawowymi Unii, a w tym z Kartą Praw Podstawowych. Również z prawem do niedyskryminacji, ochrony danych i prywatności oraz z prawami dziecka, stwarzające wyraźne zagrożenie dla bezpieczeństwa, źródeł utrzymania i praw obywateli. Wszystkie uznane zostały za niedopuszczalne. Katalog zakazanych praktyk w dziedzinie sztucznej inteligencji obejmuje wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie systemów SI. Chodzi tu zatem o systemy służące do manipulowania ludźmi, czyli takie, w których stosuje się techniki podprogowe działające na podświadomość lub wykorzystuje słabości pewnych grup osób, takich jak dzieci, osoby z niepełnosprawnościami czy zaburzeniami psychicznymi.

[33] *Budowanie zaufania przez pierwsze w historii ramy prawne dotyczące sztucznej inteligencji*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_pl (dostęp: 28.03.2023).

Celem takiego systemu jest zniekształcenie zachowania danej osoby w sposób powodujący lub mogący spowodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną. Zalicza się do nich również systemy używane przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych, prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości (tzw. *social scoring*). Występują one w kontekście zagrożenia wówczas kiedy punktowa ocena społeczna prowadzi do krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych grup w kontekstach społecznych. Oczywiście grup nie związanych z kontekstami, w których pierwotnie wygenerowano lub zgromadzono dane lub w przypadku, gdy takie traktowanie jest nieuzasadnione lub nieproporcjonalne do zachowania społecznego lub jego wagi.

Ponadto zakazane będzie wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa. Chodzi tutaj o systemy służące do identyfikacji osób fizycznych na odległość poprzez porównanie ich danych biometrycznych (np. wizerunku twarzy, chodu, zarysu sylwetki) z danymi biometrycznymi zawartymi w referencyjnej bazie danych. Natomiast chodzi o wspomnianą bazę, gdzie zbieranie danych, ich porównywanie i identyfikacja odbywają się bez znacznego opóźnienia. W celu zatem uniknięcia obchodzenia przepisów, za taki system identyfikacji biometrycznej „w czasie rzeczywistym", uznawany będzie system, w którym identyfikacja następuje zarówno natychmiast, jak i z niewielkim opóźnieniem**.** Od tego zakazu projekt rozporządzenia przewiduje ograniczone wyjątki**,** obejmujące ukierunkowane poszukiwanie ofiar przestępstw, w tym zaginionych dzieci oraz zapobieganie konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa osób fizycznych lub atakowi terrorystycznemu. Wyjątki takie jak, wykrywanie, lokalizowanie, identyfikowanie lub ściganie sprawców lub podejrzanych o popełnienie najcięższych przestępstw, takich jak np. udział w organizacji przestępczej, terroryzm, handel ludźmi, zabójstwo, gwałt czy porno-

grafia dziecięca.[34] Chodzi przy tym o przestępstwa, które w danym państwie członkowskim podlegają karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata. Natomiast każde pojedyncze wykorzystanie systemu zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa, wymagać będzie, co do zasady, uzyskania uprzedniego zezwolenia udzielonego przez sąd lub niezależny organ administracyjny państwa członkowskiego. Decyzja co do wykorzystywania tego typu systemów, należeć będzie do państw członkowskich. Będą one mogły w ogóle nie przewidzieć takiej możliwości albo przewidzieć ją jedynie w odniesieniu do niektórych spośród wskazanych wyżej dozwolonych celów. W przypadku podjęcia decyzji o dopuszczeniu możliwości wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa, dane państwo zobowiązane będzie do przyjęcia niezbędnych szczegółowych przepisów krajowych, regulujących wydawanie i wykonywanie zezwoleń na wykorzystanie systemów oraz ich nadzorowanie.[35]

Systemy sztucznej inteligencji wysokiego ryzyka (*high risk*) stanowią znaczne zagrożenie dla zdrowia i bezpieczeństwa lub praw podstawowych osób w Unii Europejskiej, szczególnie w kontekście Karty Praw Podstawowych. Jest to kluczowa kategoria, na której przede wszystkim skupia się projekt rozporządzenia. Określa on przy tym zasady klasyfikacji systemów SI jako systemów wysokiego ryzyka, wymogi dotyczące wiarygodnej sztucznej inteligencji, jakie systemy wysokiego ryzyka muszą spełniać oraz obowiązki spoczywające na dostawcach i użytkownikach takich systemów. Przyjęta w rozporządzeniu klasyfikacja systemów wysokiego ryzyka, wyróżnia dwie grupy. Pierwsza – gdy projektowane ramy regulacyjne dla sztucznej inteligencji wysokiego

[34] Przestępstwa wskazane w art. 2 ust. 2 decyzji ramowej Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (2002/584/WSiSW), Dz.U. UE L 190, 18.7.2002, s. 34, z późn. zm.

[35] Wniosek w sprawie rozporządzenia Parlamentu Europejskiego…, op. cit.

ryzyka wpisują się w system unijnego prawodawstwa harmonizacyjnego w obszarze warunków wprowadzania produktów do obrotu. System SI wysokiego ryzyka to system przeznaczony do użycia związanego z bezpieczeństwem elementu produktu (*safety component*) lub sam jest produktem objętym unijnymi przepisami harmonizacyjnymi. Są to w szczególności dyrektywy i rozporządzenia oparte na nowych ramach prawnych, dotyczące produktów takich jak maszyny, zabawki, wyroby medyczne, windy czy środki ochrony indywidualnej). Jednocześnie również produkt, którego związanym z bezpieczeństwem elementem jest system SI lub sam system SI jako produkt, podlega na podstawie wyżej wskazanych przepisów harmonizacyjnych ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.[36]

Druga grupa obejmuje zastosowania SI obecnie uznane za obarczone wysokim ryzykiem. Chodzi zatem o systemy wykorzystywane w obszarach dotyczących identyfikacji i kategoryzacji biometrycznej osób fizycznych**,** zarządzające infrastrukturą krytyczną i jej eksploatacją, systemy dotyczące kształcenia i szkolenia zawodowego**.** Następnie systemy odnośnie zatrudnienia, zarządzania pracownikami i dostęp do samozatrudnienia, dostęp do podstawowych usług prywatnych oraz usług i świadczeń publicznych, a także korzystanie z nich. Jak również ściganie przestępstw, czyli m.in. systemy przeznaczone do wykorzystania przez organy ścigania. Zalicza się również zarządzanie migracją, azylem i kontrolą graniczną oraz sprawowanie wymiaru sprawiedliwości i procesy demokratyczne**.**

Projekt rozporządzenia przewiduje możliwość dodawania, w drodze aktów delegowanych przyjmowanych przez Komisję, kolejnych systemów wysokiego ryzyka przeznaczonych do wykorzystania w wyżej wskazanych obszarach i określa szczegółowe kryteria, którymi Komisja ma się kierować w tym zakresie. W odniesieniu do niektórych systemów sztucznej inteligencji, biorąc pod uwagę specyficzne ryzyko manipulacji – ograniczone ryzyko *(limited risk*) – jakie stwarzają, projekt rozporządzenia przewiduje wyłącznie minimalne obowiązki dotyczące przejrzystości. Mają one zastosowanie do trzech grup systemów SI.

[36] *Budowanie zaufania*…, op.cit.

Pierwsza, to systemy wchodzące w interakcję z ludźmi, czyli wszelkiego rodzaju *chatboty*. Chodzi o obowiązek informowania osoby fizycznej o tym, że wchodzi ona w interakcję z systemem SI, chyba że będzie to jednoznacznie wynikać z okoliczności i kontekstu korzystania z systemu. Druga grupa to systemy wykorzystywane do wykrywania emocji lub określania powiązań z kategoriami (społecznymi) na podstawie danych biometrycznych. Chodzi tutaj o obowiązek informowania osób fizycznych o fakcie stosowania wobec nich tego typu systemów. Trzecia grupa – to systemy, które generują obrazy, treści dźwiękowe lub treści wideo, które łudząco przypominają istniejące osoby, miejsca, obiekty czy zdarzenia, które manipulują obrazami lub treściami, przez co osobie będącej ich odbiorcą mogą się one fałszywie wydać autentyczne lub prawdziwe (technologia *deepfake*). Należy do nich obowiązek ujawniania, że treści zostały wygenerowane lub zmanipulowane przez system SI. Powyższe obowiązki nie będą jednak dotyczyć systemów, które zostały zatwierdzone na mocy przepisów prawa do celów związanych z egzekwowaniem prawa. Chodzi zatem o przeciwdziałanie i ściganie przestępstw oraz sytuacji, gdy zastosowanie technologii *deepfake* będzie konieczne do wykonywania prawa do wolności wypowiedzi i prawa do wolności sztuki i nauki zagwarantowanych w Karcie praw podstawowych Unii Europejskiej z zastrzeżeniem odpowiednich gwarancji zabezpieczających prawa i wolności osób trzecich.[37]

Systemy z zakresu minimalne ryzyko (*minimal risk*), to wszystkie pozostałe systemy SI. Stanowią one większość spośród obecnie używanych na terenie UE, np. systemy stosowane w grach wideo lub filtrach spamu, jako nie stwarzające zagrożenia dla praw lub bezpieczeństwa obywateli lub stwarzające zagrożenie minimalne, nie będą podlegać żadnym szczególnym wymaganiom i obowiązkom. W odniesieniu do takich systemów projektowane rozporządzenie obliguje Komisję Europejska i państwa członkowskie do zachęcania i ułatwiania tworzenia przez branżę SI kodeksów postępowania. Na podstawie wspomnianych kodeksów, dostawcy dobrowolnie stosowaliby wymogi obligatoryjne przewidziane w rozporządzeniu dla systemów sztucznej inteligencji wysokiego ryzyka. Projektowana regulacja skupia się na systemach

[37] Wniosek w sprawie rozporządzenia Parlamentu Europejskiego…, op. cit.

wysokiego ryzyka, ustanawiając przy tym szereg rygorystycznych wymagań, których spełnienie warunkuje dopuszczalność wykorzystywania takich systemów w Unii Europejskiej. Obejmują one wdrożenie i utrzymywanie systemu zarządzania ryzykiem, zapewnienie wysokiej jakości zbiorów danych treningowych, walidacyjnych i testowych, aby system działał zgodnie z przeznaczeniem i bezpiecznie oraz aby nie stał się źródłem dyskryminacji, jak również sporządzanie i aktualizowanie dokumentacji technicznej systemu, automatyczne rejestrowanie zdarzeń. Następnie obejmują również przejrzystość i udostępnianie informacji użytkownikom, aby zapobiec tzw. efektowi czarnej skrzynki (*black box*) powodującemu, że niektóre systemy sztucznej inteligencji mogą stać się niezrozumiałe lub zbyt skomplikowane dla osób fizycznych oraz nadzór ze strony człowieka. Systemy SI bowiem wysokiego ryzyka muszą być skonstruowane tak, aby zapewniony był skuteczny nadzór nad nimi ze strony ludzi. W końcu systemy te obejmują również dokładność, solidność i cyberbezpieczeństwo. Systemy bowiem sztucznej inteligencji wysokiego ryzyka muszą, w kontekście ich przeznaczenia, osiągać odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz działać z zachowaniem tego poziomu przez cały cykl życia. Muszą być odporne na błędy, usterki lub niespójności mogące wystąpić zarówno w samym systemie, jak i w środowisku w którym działa.[38]

Projekt rozporządzenia obliguje państwa członkowskie do przyjęcia krajowych przepisów ustanawiających kary pieniężne za ich naruszenie. Wysokość kar ma być uzależniona od rodzaju naruszenia. W celu zapewnienia wdrożenia i stosowania przepisów rozporządzenia, państwa członkowskie zobowiązane będą do ustanowienia lub wyznaczenia właściwych organów krajowych. Pełnić one będą funkcje między innymi krajowego organu nadzorczego, odpowiedzialnego za wdrożenie i stosowanie Aktu w sprawie sztucznej inteligencji. Organy te pełnić będą funkcje punktu kontaktowego w relacjach z Komisją oraz reprezentującego państwo członkowskie w Europejskiej Radzie ds. Sztucznej Inteligencji. Ustanowione organy krajowe pełnić będą również funkcje organu nadzoru rynku – czyli organu prowadzącego działania

[38] Ibidem.

i stosującego środki nadzoru rynku zgodnie z rozporządzeniem (UE) 2019/1020.[39] Organy krajowe pełnić będą także funkcje organu notyfikującego, czyli organu odpowiadającego za opracowanie i stosowanie procedur koniecznych do oceny, wyznaczania i notyfikowania jednostek oceniających zgodność (jednostek notyfikowanych) oraz ich monitorowanie. Co do zasady wszystkie trzy wyżej wymienione funkcje realizować ma w każdym państwie jeden organ krajowy. Dopuszczalne będzie jednak ich rozdzielenie pomiędzy różne organy, jeżeli przemawiać będą za tym względy organizacyjne i administracyjne. Na szczeblu unijnym utworzona zostanie nowa instytucja – Europejska Rada ds. Sztucznej Inteligencji, w skład której wejdą osoby kierujące krajowymi organami nadzorczymi. W skład Rady wejdzie również Europejski Inspektor Ochrony Danych, będący organem doradczym i wspierającym Komisję Europejską w obszarze SI, poprzez gromadzenie fachowej wiedzy i najlepszych praktyk i ich udostępnianie państwom członkowskim oraz poprzez wkład w wypracowywanie jednolitych praktyk administracyjnych, jak również poprzez wydawanie opinii i zaleceń w kwestiach związanych z wdrażaniem rozporządzenia, w tym w kwestii specyfikacji technicznych lub norm czy kwestii sporządzania wytycznych.

W opublikowanym przez Wysokiego Komisarza Praw Człowieka Organizacji Narodów Zjednoczonych (OHCHR)[40] raporcie „Prawo do prywatności w erze cyfrowej" przeanalizowano w jaki sposób sztuczna inteligencja wpływa na prawo ludzi do prywatności, zdrowia, edukacji, swobody przemieszczania się, wolność zgromadzeń i zrzeszania się czy wolności wypowiedzi. Dokument zawiera negatywną ocenę profilowania, automatycznego podejmowania decyzji i innych technologii uczenia maszynowego. Zdaniem autorów dokumentu, państwa i koncerny technologiczne często pospiesznie włączają aplikacje SI, nie dochowując przy tym należytej staranności. Raport wskazuje wiele przy-

[39] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. L 169 z 25.6.2019, s. 1), stanowiące jeden z elementów nowych ram prawnych.

[40] Wysoki Komisarz Praw Człowieka ONZ, https://www.ohchr.org/en/ohchr_homepage (dostęp: 29.03.2023).

padków niesprawiedliwego traktowania osób z powodu niewłaściwego wykorzystania sztucznej inteligencji, takich jak odmowa świadczeń socjalnych z powodu zastosowania wadliwych algorytmów lub aresztowanie z powodu wadliwego oprogramowania do rozpoznawania twarzy. W raporcie Wysokiego Komisarza Narodów Zjednoczonych ds. praw człowieka przedstawione zostały istotne cechy systemów sztucznej inteligencji mogące bezpośrednio wpływać na kwestię bezpieczeństwa danych oraz praw człowieka. Systemy te zazwyczaj opierają się na dużych zbiorach danych, często zawierających dane osobowe. Zdaniem autorów raportu sprzyja to szerokiemu gromadzeniu, przechowywaniu i przetwarzaniu danych. Wiele firm z sektora prywatnego optymalizuje usługi, aby zebrać jak najwięcej danych. Na przykład serwisy społecznościowe polegają głownie na gromadzeniu i komercjalizacji ogromnych ilości danych o użytkownikach Internetu. Z kolei tak zwany „Internet rzeczy" staje się szybko rosnącym źródłem danych wykorzystywanych zarówno przez przedsiębiorstwa, jak i państwa. Zbieranie informacji odbywa się w przestrzeniach intymnych, prywatnych i publicznych. Korzystający z nich brokerzy danych pozyskują, łączą, analizują i udostępniają dane osobowe niezliczonym odbiorcom. Brakuje jednak kontroli publicznej nad tymi procesami oraz pozostaje kwestia, w jakim celu te dane są pozyskiwane. Raport wskazuje również, iż decyzje oparte na sztucznej inteligencji nie są wolne od błędów, a efekty mogą powodować ograniczenia dostępu do praw człowieka, a przy tym również dokładność wykorzystywanych danych jest często wątpliwa. Szczególnie wyraziście okazało się to podczas wielu badań w czasie pandemii koronawirusa, gdzie raport ukazuje, iż analiza setek medycznych narzędzi działających z wykorzystaniem sztucznej inteligencji do diagnozowania i przewidywania ryzyka COVID-19, opracowanych z dużymi nadziejami, wykazała, że żadne z nich nie nadawało się do użytku klinicznego. Jakość danych, na których pracują algorytmy sztucznej inteligencji, to ogromny problem, ponieważ zarówno mogą być one wadliwe i dyskryminujące, jak i nieaktualne lub nieistotne. Zbiory danych określanych jako stronnicze są często podstawą do podejmowania i wprowadzania w życie decyzji dyskryminujących i stanowią przy tym poważne zagrożenie dla mniejszości.[41]

[41] Ibidem.

Organizacja Narodów Zjednoczonych zauważa zatem niezaprzeczalny i stale rosnący wpływ technologii sztucznej inteligencji na korzystanie z prawa do prywatności i innych praw człowieka. Wskazuje jednak na niepokojące zmiany, w tym na rozległy ekosystem w dużej mierze nieprzejrzystego gromadzenia i wymiany danych osobowych stanowiący podstawę części powszechnie stosowanych systemów sztucznej inteligencji.

Rozporządzenie w sprawie sztucznej inteligencji

Wszystkie dotychczasowe rozważania prawne Unii Europejskiej doprowadziły do przedstawienia przez Parlament Europejski i Radę, Rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (Rozporządzenie).[42] Rozwiązania bazujące na sztucznej inteligencji umożliwiają lepsze prognozowanie, optymalizację operacji i przydzielania zasobów oraz personalizację świadczonych usług, dzięki czemu osiągane wyniki są korzystne z punktu widzenia kwestii społecznych i ochrony środowiska, a przedsiębiorstwa i europejska gospodarka zyskują kluczową przewagę konkurencyjną.[43] Art. 1 Rozporządzenia ustanawia między innymi zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w Unii, jak również zakazy dotyczące określonych praktyk w zakresie sztucznej inteligencji. W przypadku systemów sztucznej inteligencji przeznaczonych do wchodzenia w interakcję z osobami fizycznymi ustanawia zasady rozpoznawania emocji oraz systemów kategoryzacji biometrycznej, a także systemów sztucznej inteligencji wykorzystywanych do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi. Katalog kwestii uregulowa-

[42] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii) z dnia 21 kwietnia 2021 r., 2021/0106.

[43] Ibidem.

nych w omawianym Rozporządzeniu jest szeroki, a w szczególności warto zwrócić uwagę na wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka.

Istotny jest również zakres podmiotowy ww. Rozporządzenia, ponieważ nie ma ono zastosowania do wszystkich podmiotów UE. Art. 2 ust. 1 Rozporządzenia posiada natomiast zastosowanie między innymi do dostawców wprowadzających do obrotu lub oddających do użytku systemu sztucznej inteligencji w Unii, jak również do użytkowników systemów sztucznej inteligencji, którzy znajdują się w Unii. Zapisy w art. 5 ww. Rozporządzenia zakazują stosowania technik podprogowych będących poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną. Zakazują również wprowadzania do obrotu systemu sztucznej inteligencji, który wykorzystuje dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób. Zakazują wykorzystywania systemów sztucznej inteligencji przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, kiedy to punktowa ocena społeczna prowadzi do jednego lub obu z następujących skutków krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub całych ich grup w kontekstach społecznych. Zapisy Rozporządzenia zakazują wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów: ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci; zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu; wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa.

Należy zauważyć, że powyższy katalog ma charakter zamknięty, co

oznacza, że jedynie wymienione zachowania będą uznane za zakazane zgodnie z Rozporządzeniem. Pomimo jednak wystąpienia katalogu zamkniętego, praktyki zakazane zostały wyszczególnione w sposób dosyć ogólny, co sprawia, że należy każdorazowo dokonać analizy, czy dana czynność nie będzie stać w sprzeczności z omawianym aktem prawnym. Katalog nie ma charakteru absolutnego, nieograniczonego, bowiem prawodawca zdecydował się na odstępstwa od reguły. Dotyczy to przede wszystkim wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do egzekwowania prawa. W tym wypadku dopuszczono możliwość naruszenia powyższej zasady, jednakże tylko w określonych sytuacjach, tj. gdy jest to niezbędne do poszukiwania ofiar przestępstw (w tym zaginionych dzieci) oraz zapobiegnięciu poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa osób, wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy lub podejrzanego o przestępstwa, o których mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW[44]. W tym m.in. udział w organizacjach przestępczych, terroryzm, handel ludźmi, seksualne wykorzystanie dzieci i pornografia dziecięca, nielegalny handel środkami odurzającymi i substancjami psychotropowymi, nielegalny handel bronią, amunicją i materiałami wybuchowymi, korupcja, nadużycia finansowe, w tym mające negatywny wpływ na interesy finansowe Wspólnot Europejskich, pranie wpływów pieniężnych z przestępczości, przestępczość komputerowa, zabójstwo, ciężkie uszkodzenie ciała, nielegalny handel organami i tkankami ludzkimi, porwanie, bezprawne przetrzymywanie i branie zakładników i rasizm oraz ksenofobia.

Podsumowanie

Sztuczna inteligencja jest zjawiskiem rozwijającym się w ostatnich latach w sposób bardzo dynamiczny co powoduje, iż regulacje krajowe i unijne nie odpowiadają aktualnej sytuacji. W związku z tym, konieczne

[44] Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002, s. 1).

jest wprowadzenie określonych regulacji, które usystematyzują kwestie związane z systemami SI i bezpieczeństwem ludności. Sztuczna inteligencja bowiem niesie ze sobą wiele pozytywnych aspektów, natomiast niewłaściwe zastosowanie technologii może jednak doprowadzić do ryzyka naruszenia podstawowych praw człowieka. Korzystanie z technologii sztucznej inteligencji staje się już światowym standardem, co ma przełożenie na fundamenty kształtowania się kierunków poszukiwania rozwiązań dotyczących ryzyka związanego z tworzeniem i wykorzystywaniem systemów SI, szczególnie w omawianym obszarze dotyczącym praw człowieka. Dlatego też istotne jest wypracowanie i usankcjonowanie odpowiedniej prawnej polityki regulującej funkcjonowanie takich systemów sztucznej inteligencji. Istotna zatem była analiza aktualnych zagrożeń społecznych ze strony sztucznej inteligencji w kontekście bezpieczeństwa społecznego. Omawiane wymiary stanowią zatem dynamiczne ramy ekosystemu SI pełniąc, z jednej strony rolę stabilizatora, z drugiej natomiast uwzględniając potrzebę ciągłego kształtowania procesu stanowienia prawa odnośnie wpływu nowoczesnych technologii na świecie.

Bibliografia

Akty prawne

Biała Księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania z dnia 19 lutego 2020 r., COM (2020) 65 final.

Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi (Dz.U. L 190 z 18.7.2002).

Karta Praw Podstawowych Unii Europejskiej (2016/C 202/02).

Karta Praw Podstawowych Unii Europejskiej, Dz.Urz. UE C 326.

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy", Bruksela (25.04.2018), COM (2018) 237 final.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 r. nr 78, poz. 483.

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 r. nr 61, poz. 284.

Przestępstwa wskazane w art. 2 ust. 2 decyzji ramowej Rady z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (2002/584/WSiSW), Dz.U. UE L 190, 18.7.2002, s. 34, z późn. zm.

Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, 2015/2103(INL).

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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. .UE.L 2016 Nr 119).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.U. L 169 z 25.6.2019, s. 1), stanowiące jeden z elementów nowych ram prawnych.

Rozporządzenie PE 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.L.2016.119.1.

Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii) z dnia 21 kwietnia 2021 r., 2021/0106.

Literatura

Berdowska A., *Wspomaganie procesu rekrutacji pracowników za pomocą chatbotów* – analiza wybranych rozwiązań, Zarządzanie Zasobami Ludzkimi 2018, Nr 5.

Braman S., *Change of State: Information, Policy, and Power*, Cambridge: MIT Press, 2006.

Chałubińska–Jentkiewicz K., *Cyberodpowiedzialność*, Wyd. Adam Marszałek, Toruń 2019.

Chałubińska-Jentkiewicz K., Karpiuk K., *Prawo nowych technologii*, cz. I, rozdz. I, 2015, LEX.

Dervanović D., „Inhuman Lawyer:Developing Artificial Intelligence in the Legal Profession." *In Robotics, AI and the Future of Law*, ed. Marcelo Corrales, Mark Fenwick, and Nikolaus Forgo, 209–34. Singapore: Springer.

Goździaszek Ł., *Perspektywy wykorzystania sztucznej inteligencji w postępowaniu sądowym*, „Przegląd Sądowy" 2015, nr 10.

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji,* 2019.

Hallevy G., *Liability for Crimes Involving Artificial Intelligence Systems*, Switzerland: Springer, 2015.

Hildebrandt M., "From Galatea 2.2 to Watson- and back?" *In Human Law and Computer Law: Comparative Perspectives*, ed. Mireille Hildebrandt, and Jeanne Gaakeer, 23–45. Dordrecht: Springer, 2013.

Jankowska-Augustyn M., *Podmiotowość prawna sztucznej inteligencji?* [w:] Bielska-Brodziak A. (red.), *O czym mówią prawnicy, mówiąc o podmiotowości*, Katowice 2015.

Lubasz D., *Konstruowanie humanocentrycznej SI z wykorzystaniem instrumentów prawnych ochrony danych osobowych* w: Sztuczna inteligencja w kontekście ochrony danych osobowych, 2020.

Oręziak B., *Prawa człowieka jako determinanta sztucznej inteligencji? Propozycja kryteriów i dyrektyw zastosowania sztucznej inteligencji do użytku praktycznego*, [w:] *Prawo sztucznej inteligencji*, red. Lai L., Świerczyński M., C.H.Beck, Warszawa 2020.

Pagallo U., *The Laws of Robots Crimes, Contracts, and Torts*, Dordrecht Heidelberg New York: Springer, 2013.

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

Źródła internetowe:

Bellon M., *Szef technologicznego giganta: AI podzieli świat. Społeczeństwa bez niej będą biedniejsze i słabsze*, https://businessinsider.com.pl/technologie/marc-benioff-ceo-salesforce-o-sztucznej-inteligencji/zx4tq1m (dostęp: 26.03.2023).

Budowanie zaufania przez pierwsze w historii ramy prawne dotyczące sztucznej inteligencji, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_pl (dostęp: 28.03.2023).

Deloitte, Europejskie regulacje dot. sztucznej inteligencji, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/europejskie-regulacje-sztuczna-inteligencja-COVID-19.html (dostęp: 30.03.2023).

Naprawić przyszłość. Sztuczna inteligencja a prawa podstawowe. Podsumowanie, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_pl.pdf (dostęp: 26.03.2023).

Niezależny ośrodek odniesienia i doskonałości w zakresie promowania i ochrony praw człowieka w UE. Pomaga bronić praw podstawowych wszystkich ludzi żyjących w UE. *European Union Agency For Fundamental Rights,* https://fra.europa.eu/en (dostęp: 27.03.2023).

Wysoki Komisarz Praw Człowieka ONZ, https://www.ohchr.org/en/ohchr_homepage (dostęp: 29.03.2023).

Z badań Rady Europy wynika, że korzystanie ze sztucznej inteligencji może mieć wpływ na wiele praw podstawowych: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 (dostęp: 29.03.2023).