

I. ARTYKUŁY

Martyna Kaczmarczyk*

O systemach sztucznej inteligencji w kontekście praw człowieka w orzecznictwie Europejskiego Trybunału Praw Człowieka

On artificial intelligence systems in the context of human rights in the case law of the European Court of Human Rights

Abstract. Artificial intelligence (AI) is increasingly entering our lives. Rapid technological progress provides many new solutions, without which we often cannot imagine our everyday lives. Despite a rather heavily electronicised and digitalized reality, the potential of artificial intelligence is yet to be fully exploited. Moreover, due to the wide range of applications of AI systems in various areas of life, the possibilities that technological development creates for us go beyond the human imagination. Artificial intelligence can be a source of invaluable help for humans, support, facilitation, and convenience; on the other hand, it can pose many threats to basic values such as human rights, human dignity, democracy or the rule of law.

The article attempts to answer the question of how Strasbourg case law responds to issues concerning threats that new technologies pose to individuals' fundamental rights and freedoms, including the right to privacy, personal freedom, personal security, and the protection of personal data, including biometric data. The starting point for analysing the case law of the European Court of Human Rights (ECHR) is a discussion of international and national regulations in the field of artificial intelligence and their brief characteristics. Then, selected cases of the ECHR are presented and discussed in the context of individual freedoms and rights most vulnerable to violations in connection with the activity of AI systems. So far, the Court has not issued a judgment dedicated to artificial

* University of Warmia and Mazury in Olsztyn, Poland | Uniwersytet Warmińsko-Mazurski w Olsztynie, Polska, <https://orcid.org/0000-0001-6169-9466>, e-mail: martyna.kaczmarczyk@uwm.edu.pl.

intelligence itself and its negative effects on human rights and freedoms. The research problems addressed by this analysis indicate ECHR judgments related to new technologies and to assessing their significance for the functioning of artificial intelligence and discussing its relevance for the future.

Keywords: artificial intelligence systems – human rights – international law – case law of the European Court of Human Rights

Wprowadzenie

Sztuczna inteligencja (AI) coraz intensywniej wkracza w życie ludzi. Gwałtowny postęp technologiczny dostarcza wielu nowych rozwiązań, bez których obecnie często już nie wyobrażamy sobie naszej codzienności. Mimo dość mocno zelektronizowanej i scyfryzowanej rzeczywistości potencjał sztucznej inteligencji nie został jeszcze w pełni wykorzystany. Co więcej, z uwagi na szeroki zakres zastosowania systemów AI w różnych dziedzinach życia możliwości, jakie stwarza rozwój technologiczny, wykraczają poza ludzką wyobraźnię. Sztuczna inteligencja może z jednej strony stanowić źródło nieocenionej pomocy dla człowieka, wsparcia, ułatwienia, udogodnienia, lecz z drugiej – może stwarzać wiele zagrożeń dla elementarnych wartości, jakimi są prawa człowieka, godność ludzka, demokracja czy praworządność.

1 sierpnia 2024 r. wszedł w życie pierwszy na świecie akt prawny, który w sposób kompleksowy objął materię sztucznej inteligencji. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji¹ wprowadza legalne definicje systemów sztucznej inteligencji i wielu powiązanych pojęć, określa zakazane praktyki, klasyfikuje systemy AI, nakłada obowiązki na dostawców systemów sztucznej inteligencji, określa organy notyfikujące, a ponadto ustanawia system odpowiedzialności za negatywne skutki i szkody spowodowane działalnością AI. Zgodnie z prawem unijnym państwa członkowskie Unii Europejskiej (UE) są zobowiązane do wprowadzenia do swoich porządków prawnych odpowiednich regulacji

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 VI 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), PE/24/2024/REV/1, dalej „Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689”.

implementujących nowe rozporządzenie. Obecnie trwają prace nad polskim projektem ustawy o systemach sztucznej inteligencji.

Niemal jednocześnie z powstawaniem unijnego rozporządzenia o sztucznej inteligencji trwały prace nad międzynarodowym aktem prawnym z ramienia Rady Europy (RE). 5 września 2024 r. Komisja Europejska podpisała Ramową Konwencję Rady Europy w sprawie sztucznej inteligencji oraz praw człowieka, demokracji i praworządności². Podpis wyraża zamiar UE, aby stać się stroną konwencji. Akt ten w swoich założeniach jest zbieżny z postanowieniami unijnego rozporządzenia, chociaż pozostaje znacznie mniej rozbudowany.

Celem artykułu jest próba odpowiedzi na pytanie, jak orzecznictwo strasburskie reaguje na zagadnienia dotyczące zagrożeń, które niesie za sobą rozwój nowych technologii, dla podstawowych praw i wolności jednostki, m.in. prawa do prywatności, wolności osobistej, bezpieczeństwa osobistego, ochrony danych osobowych, w tym danych biometrycznych. Punktem wyjścia dla przeprowadzonych analiz orzecznictwa Europejskiego Trybunału Praw Człowieka (ETPC) stało się omówienie regulacji międzynarodowych i krajowych z zakresu sztucznej inteligencji oraz ich krótka charakterystyka. W dalszej kolejności zaprezentowano i omówiono wybrane orzeczenia ETPC w kontekście wolności i praw jednostki, które są najbardziej narażone na naruszenia w związku z działalnością systemów AI. Dotychczas Trybunał nie wydał orzeczenia poświęconego samej sztucznej inteligencji i jej negatywnym skutkom działania w obszarze praw i wolności człowieka. Problemy badawcze dotyczące przeprowadzonej analizy związane są ze wskazaniem wyroków ETPC powiązanych z działalnością nowych technologii, oceną ich znaczenia dla funkcjonowania sztucznej inteligencji oraz dyskusji nad jej istotą w przyszłości.

1. Pojęcie sztucznej inteligencji

Sztuczna inteligencja (ang. *artificial intelligence*, AI) jest terminem określającym wyspecjalizowany system teleinformatyczny, który pracuje w oparciu o system *software* lub zintegrowany w urządzeniu fizycznym

² Ramowa Konwencja Rady Europy w sprawie sztucznej inteligencji oraz praw człowieka, demokracji i praworządności (Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law), Council of Europe Treaty Series – No. 225, dalej „Ramowa Konwencja Rady Europy”.

hardware. Jego działanie polega na rozwiązywaniu złożonych problemów, a funkcjonowanie ma wymiar zarówno fizyczny, jak i cyfrowy³. Pojęcie AI ma zdecydowanie charakter interdyscyplinarny, funkcjonuje bowiem na pograniczu wielu dziedzin naukowych – informatyki, inżynierii komputerowej, matematyki, fizyki, robotyki, prawa, ekonomii czy psychologii⁴. Sztuczna inteligencja wykorzystuje różne technologie obliczeniowe i informatyczne w celu analizy dostarczanych danych (ang. *data science*). Głównymi celami przeprowadzanych analiz jest m.in. uczenie maszynowe, wnioskowanie automatyczne, rozpoznawanie, moderowanie i generowanie mowy oraz obrazu, przetwarzanie języka naturalnego, przewidywanie, rekomendowanie⁵.

W 1955 r. J. McCarthy, amerykański informatyk i matematyk, zaproponował oraz zdefiniował termin *sztuczna inteligencja*. Od tamtego momentu, ze względu na dynamiczny rozwój technologii oraz rewolucję przemysłową, AI otrzymywała nowe, często coraz to bardziej rozbudowane definicje⁶. Ogólnie ujmując, cechami, z którymi przeważnie sztuczna inteligencja jest łączona, są umiejętność uczenia się, zdolność przystosowywania się do zmiennych warunków, podejmowanie własnych decyzji na podstawie przeprowadzonych analiz (niejednokrotnie bardzo skomplikowanych), rozumowanie abstrakcyjne itp. Procesy te możliwe są dzięki działom informatycznym czy też teleinformatycznym, które zajmują się konstruowaniem maszyn oraz algorytmów, następnie podejmując autonomiczne działania przejawiające cechy inteligencji⁷.

Do niedawna w kwestii definiowania sztucznej inteligencji można było polegać na definicjach proponowanych przez poszczególne dziedziny nauki, takie jak wspomniana informatyka, matematyka czy robotyka. Stworzyły one bowiem zbieżne, aczkolwiek ukształtowane

³ M. Jankowska-Augustyn, *Podmiotowość prawna sztucznej inteligencji?*, w: *O czym mówią prawnicy, mówiąc o podmiotowości*, pod red. A. Bielskiej-Brodziak, Katowice 2015, s. 171; J. Rzymowski, *Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji*, „Przegląd Prawa Publicznego” 2024, nr 11, s. 59.

⁴ A. Berdowska, *Wspomaganie procesu rekrutacji pracowników za pomocą chatbotów – analiza wybranych rozwiązań*, „Zarządzanie Zasobami Ludzkimi” 2018, nr 5, s. 93–112.

⁵ P. Kuszneruk, *Wpływ rozwoju sztucznej inteligencji na proces stanowienia prawa w Polsce*, „Przegląd Prawa Publicznego” 2023, nr 5, s. 8.

⁶ K. Różanowski, *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, „Zeszyty Naukowe WWSI” 2007, nr 2, s. 109; M. Sakowska-Baryła, *Sztuczna inteligencja w sektorze publicznym*, w: *Prawo sztucznej inteligencji i nowych technologii*, pod red. B. Fischera, A. Pązika, M. Świerczyńskiego, Warszawa 2023, s. 33.

⁷ Sakowska-Baryła, op. cit., s. 34.

na własne potrzeby i zgodnie z własną specyfikacją metod badawczych, definicje AI. Na potrzeby innych nauk, w tym prawa, definicje te były oczywiście wykorzystywane. Natomiast w przestrzeni prawnej nie funkcjonowały żadne legalne definicje sztucznej inteligencji. Przełomowy okazał się rok 2024, kiedy po wieloletnich pracach oraz konsultacjach weszło w życie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689. Rozporządzenie ustanawia pierwszą legalną definicję systemu AI, która określa, że jest to „system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne”⁸. Podobną i zbieżną zakresem pojęciowym definicję wprowadza Ramowa Konwencja Rady Europy, która stanowi, że systemem AI jest „system maszynowy, który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne. Poszczególne systemy sztucznej inteligencji różnią się pod względem poziomu autonomii i zdolności adaptacyjnej po wdrożeniu”⁹. Definicja ta w przeciwieństwie do definicji z unijnego rozporządzenia nie jest definicją legalną, gdyż konwencja nie została jeszcze uchwalona, a do momentu jej wejścia w życie minie jeszcze trochę czasu. Natomiast jej sformułowanie pokazuje kierunek, w którym zmierza RE pod względem zapewnienia gwarancji bezpiecznego i godnego zaufania funkcjonowania systemów sztucznej inteligencji. Obie definicje pozostają ze sobą zgodne i spójne.

Sztuczna inteligencja to niezwykle potężny i szeroki wachlarz możliwości zastosowania. Jeśli używana jest zgodnie ze swoim przeznaczeniem, stanowi niezbędny filar rozwoju gospodarczego państwa, przyczynia się do wzrostu konkurencyjności, jest nieocenioną pomocą w medycynie, analizuje algorytmy, które przetwarzają ogromne pliki, tzw. *Big Data*, z którymi ludzki umysł nie jest w stanie sobie poradzić. Należy podkreślić, że sztuczna inteligencja dla swojego istnienia oraz dalszego rozwoju potrzebuje wielkich ilości danych do przetwarzania – jest

⁸ Art. 3 pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689.

⁹ Art. 2 Ramowej Konwencji Rady Europy.

to niezbędne źródło jej bytu. Oprócz tak wielu korzyści, jakie niesie za sobą wykorzystywanie systemów AI, sztuczna inteligencja to również zagrożenia, w tym przede wszystkim potencjalne naruszenia elementarnych praw i wolności człowieka oraz wartości, jakimi kieruje się demokratyczne państwo. Z pojęciem sztucznej inteligencji powiązane są ewentualne negatywne skutki wprowadzania AI w kolejne sfery życia ludzkiego. Przede wszystkim chodzi o cyberprzestępczość wykorzystującą sztuczną inteligencję, a związane z nią są pojęcia kradzieży tożsamości, *deepfake*, *spamming*, *phishing*, *sniffing*, *stalking* czy mowa nienawiści i wiele innych¹⁰. Nowe technologie wymykają się spod ocen moralnych i etycznych. Kluczową kwestią pozostaje natomiast cel i sposób wykorzystywania systemów sztucznej inteligencji¹¹. Nie łączy znaczenie ma również coraz większe wykorzystanie AI w dobie cyfryzacji administracji krajowej, wydawania orzeczeń przez sądy, a także prowadzenia przez organy państwowe elektronicznych postępowań¹². Postępujące wdrażanie systemów sztucznej inteligencji skutkuje również poważnymi konsekwencjami dla gospodarek krajowych, w tym rynków pracy. Ludzka praca już jest zastępowana komputerami, maszynami czy robotami¹³. W konsekwencji będzie to prowadzić do zwiększania się bezrobocia, co zrodzi dalsze negatywne skutki społeczne oraz osobiste. Problematyka prawna systemów AI to także coraz bardziej znaczące wykorzystywanie sztucznej inteligencji w różnych dziedzinach medycyny¹⁴.

¹⁰ M. Rojszczak, *Prawne aspekty systemów sztucznej inteligencji – zarys problemu*, w: *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, pod red. K. Flagi-Gieruszyńskiej, J. Gołaczyńskiego, D. Szostka, Warszawa 2019, s. 3–6.

¹¹ K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, LEX/el. 2015, s. 143.

¹² Zob. A. Zalesińska, *Doręczenie elektroniczne w postępowaniu cywilnym*, w: *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, pod red. J. Gołaczyńskiego, Warszawa 2022; Ł. Goździaszek, *Elektroniczne postępowanie upominawcze – doświadczenia i przyszłość*, w: *Prawo nowych technologii. Księga z okazji jubileuszu...*; J. Studzińska, *Informatyzacja postępowania egzekucyjnego – elektroniczne akta komornicze. Postulat czy rzeczywistość?*, w: *Prawo nowych technologii. Księga z okazji jubileuszu...*; M. Jabłoński, *Nowoczesne technologie sztucznej inteligencji a konstytucyjne prawo do sądu*, w: *Prawo nowych technologii. Księga z okazji jubileuszu...*

¹³ J. Męcina, *Od cyfryzacji i robotyzacji do sztucznej inteligencji. Wyzwania dla gospodarki i rynku pracy*, Warszawa 2023, s. 29.

¹⁴ E. Topol, *Medycyna głęboka. Jak sztuczna inteligencja może przywrócić opiece zdrowotnej ludzką twarz*, tłum. A. Boniszewska, Warszawa 2021, s. 263–264.

2. Stan unormowania systemów sztucznej inteligencji w prawie międzynarodowym

W kwestii międzynarodowego podejścia do zagwarantowania prawnej ochrony wolności i praw człowieka, przejrzystości procedur i zasad wdrażania systemów sztucznej inteligencji oraz ponoszenia odpowiedzialności za negatywne skutki, jakie mogą mieć miejsce w związku z działalnością AI, niemal równolegle w UE i RE podjęto prace nad powołaniem komisji i organów eksperckich, dążąc do ustanowienia kompleksowych opracowań prawnych w materii sztucznej inteligencji¹⁵.

Z ramienia UE już na początku 2018 r. powołano grupę ekspertów ds. sztucznej inteligencji i europejski sojusz na rzecz sztucznej inteligencji¹⁶. Celem tego działania było zebranie opinii ekspertów i zgromadzenie szerokiego sojuszu różnych interesariuszy. Grupa ekspertów zajęła się również przygotowaniem propozycji wytycznych dotyczących etyki AI. Pod koniec 2020 r. Parlament Europejski przyjął pierwsze rezolucje dotyczące systemów sztucznej inteligencji w aspekcie etycznym, ochrony praw autorskich oraz odpowiedzialności cywilnej za AI¹⁷. W kwietniu 2021 r. Komisja Europejska zaproponowała pierwsze w historii ramy prawne dotyczące sztucznej inteligencji, które uwzględniały zagrożenia związane ze sztuczną inteligencją i stawiały Europę w pozycji lidera na arenie międzynarodowej¹⁸. Kolejnym ważnym krokiem było przyjęcie 28 września 2022 r. przez Komisję Europejską projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję¹⁹. Następnie

¹⁵ Zob. J. Mazur, *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, „Europejski Przegląd Sądowy” 2020, nr 9, s. 14 i n.

¹⁶ Zob. https://ec.europa.eu/commission/presscorner/detail/en/ip_18_1381 (dostęp: 26 II 2025).

¹⁷ Rezolucja Parlamentu Europejskiego z dnia 20 X 2020 r. w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012 (INL); Rezolucja Parlamentu Europejskiego z dnia 20 X 2020 r. w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję, 2020/2014 (INL); Rezolucja Parlamentu Europejskiego z dnia 20 X 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji, 2020/2015 (INI).

¹⁸ Wniosek dot. Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (Document 52021PC0206); zob. I. Bałos, *Sztuczna inteligencja i jej wynalazki – studium przypadku*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego” 2020, nr 1, s. 95 i n.

¹⁹ Wniosek dot. Dyrektywy Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej

w czerwcu 2023 r. Komisja przyjęła porozumienie polityczne osiągnięte przez Parlament Europejski i Radę w sprawie rozporządzenia o sztucznej inteligencji, zaproponowanego przez Komisję w kwietniu 2021 r. W maju 2024 r. Komisja Europejska zakończyła procedurę przyjęcia nowych przepisów unijnych, zwieńczoną podpisaniem Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 (tzw. AI Act). Dokument wszedł w życie 1 sierpnia 2024 r., ale będzie w pełni stosowany dopiero po 2 latach od tej daty. Proces ustanowienia nowych unijnych norm dotyczących sztucznej inteligencji był wieloetapowy, dokładnie konsultowany i niestety wieloletni.

Nowa unijna regulacja dotycząca systemów AI została oparta na analizie ryzyka z podziałem na niedopuszczalne ryzyko, wysokie ryzyko i niskie lub minimalne ryzyko. Od oceny ryzyka uzależnione są obowiązki, które nakłada się na dostawców oraz użytkowników AI. Rozporządzenie dokładnie wyszczególnia, jakie praktyki w obrębie działalności systemów sztucznej inteligencji są praktykami niedozwolonymi z uwagi na ich sprzeczność z podstawowymi zasadami i prawami UE. Można wymienić m.in. działania oparte na AI związane z propagandą, wykorzystujące słabość osób fizycznych, analizujące emocje jednostki, wprowadzające kategoryzację danych, w tym danych biometrycznych. Ponadto ustanowiony został słownik ustawowy, który zawiera legalne definicje aż 68 pojęć, m.in. sztucznej inteligencji, ryzyka, dostawcy, poszczególnych rodzajów danych i systemów istotnych z punktu widzenia technologii AI. Rozporządzenie wprowadza zasady przewodnie dotyczące systemów AI. Pierwsza z nich to reguła nadzoru człowieka nad systemami sztucznej inteligencji wysokiego ryzyka. Oznacza to, że każdorazowo jednostka ludzka sprawuje nadzór nad takimi systemami, co zapobiega ryzyku dla zdrowia, bezpieczeństwa i praw podstawowych lub minimalizuje ryzyko wystąpienia. Ponadto istotna w tym przypadku jest kwestia samego zaprojektowania systemu wysokiego ryzyka, gdyż wymaga się zastosowania odpowiednich narzędzi interfejsu człowiek–maszyna. Kolejna zasada przewodnia systemów AI to reguła przejrzystości i udostępniania informacji podmiotom stosującym. Trzecia, równie ważna zasada, wyraża obowiązek dokładności, solidności i cyberbezpieczeństwa przy projektowaniu i rozwijaniu systemów sztucznej inteligencji. Ponadto określone zostały również

inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję) (Document 52022PC0496).

obowiązki dostawców systemów sztucznej inteligencji polegające na monitorowaniu i zgłaszaniu zdarzeń. Monitorowaniu podlegać ma cały cykl AI, od momentu wprowadzenia go na rynek. Na dostawcy ciąży także obowiązek zgłaszania wszelkich incydentów i nieprawidłowości w działaniu. Unijny ustawodawca nałożył na państwa członkowskie obowiązek wyznaczenia krajowych organów notyfikujących i organów nadzoru rynku, o czym będzie mowa poniżej²⁰.

Drugim międzynarodowym systemem prawnym w zakresie systemów AI będzie Konwencja Rady Europy w sprawie sztucznej inteligencji, która jeszcze nie została uchwalona. RE na przestrzeni ostatnich lat również podjęła liczne inicjatywy prawotwórcze w dziedzinie sztucznej inteligencji. W 2020 r. z ramienia Zgromadzenia Parlamentarnego RE przyjęto Rezolucję o potrzebie demokratycznego zarządzania sztuczną inteligencją²¹. Wezwano RE do podjęcia intensywniejszych i szybszych działań w materii regulacji prawnych AI. Kolejnym krokiem było rozpoczęcie prac nad projektem Konwencji w sprawie sztucznej inteligencji, praw człowieka, demokracji i praworządności przez Komitet ds. Sztucznej Inteligencji. Projekt został opublikowany w wersji roboczej w lipcu 2023 r.²² Następnie 5 września 2024 r. Komisja Europejska w imieniu UE podpisała wiążący międzynarodowy traktat o sztucznej inteligencji, czyli Ramową Konwencję Rady Europy. Jej kształt wynegocjowało 57 państw.

Ramowa Konwencja Rady Europy swoje oparcie znalazła w wartościach wyrażonych przez Europejską konwencję praw człowieka²³, a więc w najbardziej fundamentalnych wolnościach i prawach człowieka. Ogólnie ujmując, zaproponowane przepisy dotyczą unormowania regulacji o charakterze fundamentalnym dla systemów sztucznej inteligencji, czyli podstawowych zasad i reguł prawa. Ramowa Konwencja

²⁰ Rozporządzenie Parlamentu Europejskiego i Rady 2024/1689. Zob. J. Kozłowski, *Akt w sprawie sztucznej inteligencji w praktyce – charakterystyka unijnej regulacji opartej na ryzyku*, „Europejski Przegląd Sądowy” 2024, nr 12, s. 21; R. Stefanicki, *Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana*, „Przegląd Prawa Handlowego” 2023, nr 1, s. 10 i n.

²¹ Resolution 2341 (2020) Need for democratic governance of artificial intelligence, <https://pace.coe.int/pdf/0b472b0ef9de710970a8106e0bbaf0d10fe3b0119e48da-83a286ab652d6e66b9?title=Res.%202341.pdf> (dostęp: 3 III 2025).

²² Consolidated working draft of the framework convention on artificial intelligence, human rights, democracy and the rule of law, CAI(2023)18, <https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66> (dostęp: 4 III 2025).

²³ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 XI 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. 1993 Nr 61, poz. 284), dalej „EKPC”.

Rady Europy wprowadza legalną definicję systemów AI oraz innych terminów powiązanych, jednak w ograniczonym stopniu. Za główną regułą prawną dokument uznaje stosowanie postanowień konwencji na każdym etapie cyklu życia systemu sztucznej inteligencji z podkreśleniem poszanowania podstawowych praw człowieka i wartości demokracji oraz praworządności. Ramowa Konwencja Rady Europy, chociaż zbieżna z postanowieniami unijnego rozporządzenia, jest stosunkowo oszczędna, mało szczegółowa, nie porusza wielu kwestii tak dogłębnie, jak regulacja UE. Przykładem uogólnionego postanowienia jest chociażby art. 9, który dość enigmatycznie podaje, że zobowiązuje się państwa do podejmowania niezbędnych środków służących ochronie wolności jednostki, godności ludzkiej oraz autonomii. Nie wiadomo natomiast, o jakie środki chodzi. Sformułowanie jest nieprecyzyjne, co pozwala na bardzo szeroką wykładnię, o jakie działania ze strony państwa chodzi. W podobny sposób bardzo ogólnie ujęte zostały zasady odnoszące się do projektowania, rozwijania i stosowania systemów sztucznej inteligencji – przeciwdziałanie dyskryminacji, równość, bezpieczeństwo nie są wartościami odnoszącymi się do AI. Mają swoje odniesienie do licznych regulacji prawnych, zatem znów mamy do czynienia z uogólnieniem i brakiem precyzji. Istotną kwestią – różnicą pomiędzy Ramową Konwencją Rady Europy a Rozporządzeniem Parlamentu Europejskiego i Rady 2024/1689, oprócz przedstawionych licznych różnic w poziomie szczegółowości poszczególnych zagadnień prawnych, jest ukształtowanie systemu odpowiedzialności za naruszenia wolności i praw człowieka. W ramach rozporządzenia UE nałożone zostały szczególne obowiązki związane z odpowiedzialnością za działalność AI na osoby fizyczne i prawne w roli dostawców. Natomiast w ramowej konwencji odpowiedzialność i obowiązek odszkodowawczy spoczywa na państwie²⁴.

3. Sztuczna inteligencja a regulacje krajowe

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 w sierpniu 2024 r. niemal od razu rozpoczęły się prace nad polskim projektem ustawy o systemach sztucznej

²⁴ Ramowa Konwencja Rady Europy; zob. A. Michalak, *Projekt rozporządzenia Parlamentu UE o odpowiedzialności cywilnej za działania systemów sztucznej inteligencji – krok w dobrym kierunku czy niepotrzebne odstępstwo od zasad ogólnych?*, w: *Prawo sztucznej inteligencji i nowych technologii*, pod red. B. Fischera, A. Pázika, M. Świerczyńskiego, Warszawa 2021, s. 47.

inteligencji²⁵. Ustanowienie norm wewnętrznych poświęconych AI przez państwa członkowskie UE jest bowiem warunkiem koniecznym dla realizacji prawa unijnego. Projekt ustawy z ramienia Ministerstwa Cyfryzacji otrzymał numer UC71 i od 16 października 2024 r. trwają nad nim prace w Rządowym Centrum Legislacji²⁶. Zgodnie z założeniami autorów projektu Rada Ministrów powinna przyjąć nowe przepisy w I kwartale 2025 r.

Projektowana ustawa o systemach sztucznej inteligencji będzie stanowić *novum* w polskim systemie prawnym. Jest to szczególnie istotne z perspektywy odpowiedzialności za szkody wyrządzone przez działalność systemów sztucznej inteligencji. Chodzi przede wszystkim o naruszenia praw i wolności osobistych osób fizycznych i prawnych. Dotychczas kwestie prawnej odpowiedzialności za wspomniane naruszenia przez AI nie miały swojej szczególnej formy umocowanej w przepisach wewnętrznych. Zastosowanie w tych przypadkach miały wybrane, istniejące już regulacje prawne z zakresu prawa krajowego oraz międzynarodowego – przede wszystkim przepisy ogólne z zakresu ochrony praw człowieka, w tym dóbr osobistych, prawa ochrony konsumentów, przepisy z zakresu ochrony własności intelektualnej, regulacje dotyczące ochrony danych osobowych oraz przepisy o odpowiedzialności cywilnej i z zakresu prawa konkurencji. Zatem odpowiedzialność za szkody wyrządzone przez działanie sztucznej inteligencji nie była wystarczająco uregulowana, ponieważ z uwagi na specyficzny charakter materii AI, przepisy te nie były do niej dostosowane, a jedynie poprzez odpowiednią wykładnię mogły mieć zastosowanie do indywidualnych spraw z zakresu łamania praw przez działalność sztucznej inteligencji. W związku z tym brakowało ze strony ustawodawcy odpowiedniej ochrony wolności i praw, ponadto o odpowiedniej randze prawnej oraz właściwej rekompensaty za naruszenia. Postępująca czwarta rewolucja przemysłowa i w związku z tym pojawiająca się potrzeba dostosowania właściwych krajowych norm oraz unifikacji prawa UE w szerokiej materii AI doprowadziły do podjęcia prac nad projektem ustawy o systemach sztucznej inteligencji.

²⁵ Projekt ustawy o systemach sztucznej inteligencji (UC71) w wykazie prac legislacyjnych i programowych Rady Ministrów, <https://www.gov.pl/web/premier/projekt-ustawy-o-systemach-sztucznej-inteligencji> (dostęp: 5 III 2025).

²⁶ Projekt ustawy o systemach sztucznej inteligencji (UC71) w Rządowym Procesie Legislacyjnym, <https://legislacja.rcl.gov.pl/projekt/12390551/katalog/13087901> (dostęp: 5 III 2025).

Projekt ustawy o systemach sztucznej inteligencji ma na celu wprowadzenie do krajowego porządku prawnego regulacji służących stosowaniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689. Głównym celem projektowanych przepisów jest poprawa funkcjonowania rynku krajowego, co będzie stanowiło skutek ustanowienia jednolitych ram prawnych. Szczególnie chodzi o zakres rozwoju, możliwość wprowadzenia do obrotu, a następnie oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji AI w UE. Jest to działanie ukierunkowane na zgodność z wartościami unijnymi. Systemy sztucznej inteligencji powinny być zorientowane na jednostkę ludzką i godne zaufania. Jednocześnie wprowadzenie odpowiednich regulacji zapewni właściwy i wysoki poziom ochrony praw i wolności podstawowych, bezpieczeństwa, a także wartości takich jak demokracja, praworządność i ochrona środowiska. Bardzo istotną kwestią jest również wspieranie innowacji na polskim rynku, czemu nowe ustawodawstwo zdecydowanie będzie sprzyjać.

Pozytywnie należy oceniać działania podjęte w celu ustanowienia reżimu prawnego poświęconego sztucznej inteligencji. Po pierwsze, materia ta wymaga ustanowienia norm na poziomie ustawowym ze względu na swoją specyfikę. Posłużenie się aktem prawnym niższego rzędu, np. rozporządzeniem, nie byłoby adekwatne i nie czyniłoby zadość niezbędnym gwarancjom ochrony praw i wolności człowieka. Po drugie, proponowany akt jest w pełni zgodny z rozporządzeniem unijnym, wyraża te same wartości, definicje, zasady oraz reguły odpowiedzialności za działalność związaną z wykorzystywaniem sztucznej inteligencji. Ustawodawca jest jednak zobowiązany do wprowadzenia pewnych zmian w wewnętrznym porządku prawnym, aby w pełni odpowiadał unijnym normom. Przede wszystkim konieczne jest powołanie organu notyfikującego, którym będzie minister właściwy do spraw informatyzacji, oraz nowego organu nadzoru rynku, wyspecjalizowanego w zagadnieniach dotyczących AI. Zgodnie z projektowanymi przepisami powstanie Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (Rozdział II, art. 5)²⁷. Kolejną kwestią jest potrzeba sprecyzowania przepisów, które będą umożliwiały nakładanie administracyjnych kar finansowych za naruszenia przepisów dotyczących sztucznej inteligencji. Najbardziej odpowiednie wydaje się zastosowanie trybu przepisów o postępowaniu egzekucyjnym w administracji z enumeratywnym,

²⁷ Ibidem.

ustawowym określeniem przypadków, w których organ mógłby nałożyć w drodze decyzji karę pieniężną. Warto podkreślić, że na arenie międzynarodowej Polska staje się prekursorem w kwestii nowych rozwiązań prawnych dotyczących zaawansowanych technologii. Do tej pory tylko dwa państwa członkowskie UE ustanowiły wewnętrzne normy prawne poświęcone działalności systemów AI. W Hiszpanii w 2023 r. powstał pierwszy europejski organ nadzorujący wykorzystywanie systemów sztucznej inteligencji – Agencja Nadzoru Sztucznej Inteligencji (Agencia Española de Supervisión de Inteligencia Artificial, AESIA)²⁸. Natomiast w Austrii na początku 2024 r. uchwalono Telekommunikationsgesetz i ustanowiono punkt kontaktowy ds. sztucznej inteligencji, a następnie Radę Doradczą ds. sztucznej inteligencji²⁹. Zatem polski projekt ustawy jest jak dotąd jedynym w UE tak kompleksowym aktem normatywnym w zakresie systemów sztucznej inteligencji, ponieważ ustawodawcy hiszpańscy i austriaccy skupili się jedynie na dostosowaniu krajowych regulacji do wymogu utworzenia organów czy też instytucji nadzorujących wdrażanie i wykorzystywanie AI.

4. Europejski Trybunał Praw Człowieka o sztucznej inteligencji

Orzecznictwo strasburskie dotyczące systemów sztucznej inteligencji oraz naruszeń praw i wolności jednostki w kontekście działalności tych systemów związane jest ze specyfiką wydawania orzeczeń przez ETPC. Wyroki ETPC nie są bowiem wydawane z urzędu. W znacznej większości przypadków postępowanie zostaje zainicjowane przez złożenie skargi indywidualnej na naruszenie określonych praw chronionych przez EKPC. Nadmienić należy, że wymogiem prawnym dla złożenia skargi jest wyczerpanie krajowej drogi sądowej i środków odwoławczych. Powoduje to, że względu na czasochłonny proces przejścia przez krajową drogę sądową, że Trybunał wydaje niejako z opóźnieniem swoje opinie na temat niedostatecznych gwarancji ochrony wolności i praw lub ich naruszeń. Tak dzieje się również w przypadku materii systemów sztucznej inteligencji.

²⁸ Zob. <https://www.hacienda.gob.es/GabineteMinistro/notas%20prensa/2023/consejo-de-ministros/22-08-23-np-cm-estatutos-agencia-inteligencia-artificial.pdf> (dostęp: 8 III 2025).

²⁹ Zob. <https://dejure.org/gesetze/TKG> (dostęp: 8 III 2025).

Jedną z najstarszych decyzji ETPC, która pośrednio odwołuje się do systemów sztucznej inteligencji, jest sprawa *Van der Velden przeciwko Holandii* dotycząca pobierania oraz przechowywania materiału genetycznego przez organy państwowe³⁰. Trybunał stwierdził, że „[p]otencjalne wykorzystanie materiału komórkowego w przyszłości, systematyczne pobieranie takiego materiału wykracza poza zakres neutralnych cech identyfikacyjnych, takich jak odciski palców, i ma wystarczająco intryzujący charakter, by stanowić ingerencję w prawo do poszanowania życia prywatnego”³¹. Dodatkowo Trybunał zwrócił uwagę, że ze względu na wyjątkowo wrażliwy charakter materiału genetycznego, w związku z możliwością wykorzystania go w przyszłości, jego przechowywanie jest niebezpieczne w czasach dynamicznie rozwijających się nowych technologii. Podobnie wypowiedział się Trybunał w wyroku z 2008 r. w sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu* w kwestii przechowywania danych biometrycznych w postaci odcisków palców przez organy krajowe³². Nie sposób nie zgodzić się ze stwierdzeniem, że „[n]iepokój jednostki dotyczący ewentualnego przyszłego wykorzystywania prywatnych informacji pozyskanych przez organy władzy jest uzasadniony prawnie i ma znaczenie dla rozstrzygnięcia tego, czy ingerencja miała miejsce. W rzeczy samej, mając na względzie gwałtowne tempo zachodzenia zmian w dziedzinie genetyki i technologii przetwarzania informacji, nie można nie wziąć pod uwagę ewentualności, iż w przyszłości na interesy z zakresu życia prywatnego związane z informacją genetyczną może być wywierany negatywny wpływ na nowe sposoby lub w sposób, który nie może zostać precyzyjnie przewidziany w dniu dzisiejszym”³³. Dodatkowo Trybunał wskazał, że profile DNA zawierają znaczną ilość danych o unikalnym charakterze. Podobne stanowisko zajął Trybunał w wyroku z 2020 r. w sprawie *Gaughran przeciwko Zjednoczonemu Królestwu*³⁴ dotyczącej przechowywania profilu DNA przez organy państwowe. ETPC stwierdził, że niezróżnicowany charakter uprawnień do zatrzymywania profilu DNA, odcisków palców i fotografii skarżącego jako osoby skazanej za przestępstwo, nawet

³⁰ Decyzja ETPC z 7 XII 2006 r. w sprawie *Van der Velden przeciwko Holandii*, skarga nr 29514/05.

³¹ Ibidem.

³² Wyrok ETPC z 4 XII 2008 r. w sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu*, skargi nr 30562/04 i 30566/04.

³³ Ibidem.

³⁴ Wyrok ETPC z 13 II 2020 r. w sprawie *Gaughran przeciwko Zjednoczonemu Królestwu*, skarga nr 45245/15.

jeśli zostały one wykorzystane, bez odniesienia do wagi przestępstwa lub potrzeby przechowywania na czas nieokreślony oraz przy braku jakiegokolwiek rzeczywistej możliwości kontroli, nie udało się osiągnąć właściwej równowagi między konkurującymi ze sobą interesami publicznymi i prywatnymi. Ten rozszerzony zakres uznania nie jest jednak wystarczający, aby stwierdzić, że zatrzymywanie takich danych może być proporcjonalne w okolicznościach, do których zalicza się brak odpowiednich zabezpieczeń, w tym brak jakiegokolwiek rzeczywistej kontroli nad przechowywanymi danymi³⁵.

Zbliżone stanowisko zaprezentował ETPC w orzeczeniu z 2015 r. dotyczącym gromadzenia i przechowywania danych teleinformatycznych przez organy państwowe w sprawie *Zakharov przeciwko Rosji*. Trybunał, chociaż nie użył wprost terminu *sztuczna inteligencja*, to wskazał bardzo istotne wytyczne dla organów państwowych przeprowadzających czynności operacyjne służące inwigilacji³⁶. Trybunał zaznaczył, że „[p]rzez widywalność w szczególnym kontekście niejawnych środków kontroli, takich jak przechwytywanie komunikacji, nie może oznaczać, iż osoba powinna mieć możliwość przewidzenia tego, kiedy organy władzy będą prawdopodobnie przechwytywać jej komunikację, tak aby osoba ta mogła dostosować odpowiednio do tego faktu swoje zachowanie. Ryzyko arbitralności jest jednakże oczywiste, zwłaszcza w przypadku wykonywania niejawnego uprawnienia powierzonego władzy wykonawczej. Konieczne zatem jest przyjęcie jasnych, szczegółowych przepisów w przedmiocie podsłuchiwanie rozmów telefonicznych, szczególnie w świetle tego, że dostępna technologia z każdym dniem staje się coraz bardziej wyrafinowana. Prawo krajowe musi być wystarczająco wyraźne, aby dać osobom odpowiednie wskazówki co do okoliczności i warunków, w jakich organy władzy publicznej są uprawnione do zastosowania któregośkolwiek z takich środków”³⁷. Podobnie wypowiedział się Trybunał w 2016 r. w sprawie *Szabó i Vissy przeciwko Węgrom*³⁸ oraz w sprawie z 2020 r. *Breyer przeciwko Niemcom*³⁹. Oba postępowania dotyczyły działań operacyjnych prowadzonych przez organy państwowe w ramach inwigilacji. W pierwszym orzeczeniu ETPC zaznaczył, że

³⁵ Ibidem.

³⁶ Wyrok ETPC z 4 XII 2015 r. w sprawie *Zakharov przeciwko Rosji*, skarga nr 47143/06.

³⁷ Ibidem.

³⁸ Wyrok ETPC z 12 I 2016 r. w sprawie *Szabó i Vissy przeciwko Węgrom*, skarga nr 37138/14.

³⁹ Wyrok ETPC z 30 I 2020 r. w sprawie *Breyer przeciwko Niemcom*, skarga nr 50001/12.

„[n]aturalną konsekwencją form przybieranych przez terroryzm dnia dzisiejszego jest wykorzystywanie przez rząd najnowszych technologii dla wyprzedzenia takich ataków, łącznie z masowym monitorowaniem komunikacji, mogących zawierać wskazówki dotyczące zbliżających się incydentów. Techniki stosowane przy takich operacjach monitorujących wskazują na znaczny postęp w ostatnich latach. Osiągnęły taki stopień wyrafinowania, jaki przeciętny obywatel z trudem może sobie wyobrazić, zwłaszcza wraz z technologicznym umożliwieniem i rozpowszechnieniem zautomatyzowanego i systemowego gromadzenia danych. Wobec tego postępu Trybunał musi zbadać kwestię, czy rozwojowi metod kontroli skutkujących ogromem zgromadzonych danych towarzyszy jednoczesny rozwój zabezpieczeń prawnych chroniących poszanowanie praw obywateli wynikających z EKPC. Dane te często zawierają dalsze informacje o warunkach, w jakich powstały elementy podstawowe przechwycone przez organy władzy, elementy takie jak czas i miejsce oraz sprzęt użyty dla stworzenia plików komputerowych, fotografii cyfrowych, wiadomości elektronicznych i tekstowych. W rzeczy samej, cel wysiłków rządu, który dąży do ograniczenia terroryzmu i przywrócenia tym samym zaufania obywateli w zdolność rządu do utrzymania bezpieczeństwa publicznego, zostałby zniweczony, gdyby zagrożenie terrorystyczne zostało paradoksalnie zastąpione przez dostrzegalne zagrożenie wywołane nieograniczonymi uprawnieniami władzy wykonawczej do ingerencji w sfery życia prywatnego obywateli za pomocą niekontrolowanych, a jednocześnie daleko idących technik i prerogatyw kontrolnych”⁴⁰. We wspomnianym orzeczeniu *Breyer przeciwko Niemcom* Trybunał zwrócił uwagę, że wartości społeczeństwa demokratycznego muszą być jak najwierniej przestrzegane w procedurach nadzorczych. Chociaż Trybunał nie dopatrzył się naruszeń praw skarżącego, to podkreślił, że jedną z fundamentalnych zasad społeczeństwa demokratycznego jest praworządność. Praworządność oznacza między innymi, że ingerencja władzy wykonawczej w prawa jednostki powinna podlegać skutecznej kontroli, którą normalnie powinna zapewnić władza sądownicza, przynajmniej w ostateczności, przy czym kontrola sądowa daje najlepsze gwarancje niezawisłości, bezstronności i właściwej procedury⁴¹. Interesujące zdanie odrębne do wyroku przedstawił sędzia Ranzoli, który podkreślił, że ingerencja w prawa skarżącego

⁴⁰ Wyrok ETPC w sprawie *Szabó i Vissy przeciwko Węgrom*, op. cit.

⁴¹ Wyrok ETPC w sprawie *Breyer przeciwko Niemcom*, op. cit.

nie była proporcjonalna do zamierzonych zgodnych z prawem celów, w szczególności dlatego, że ustawodawstwo krajowe nie ograniczało się do środków wymierzonych przeciwko terroryzmowi lub innym poważnym przestępstwom lub do kwestii bezpieczeństwa narodowego, lecz w rzeczywistości wykaczało daleko poza to. Ingerencja ta nie odpowiadała „pilnej potrzebie społecznej” i w związku z tym nie była konieczna w społeczeństwie demokratycznym⁴².

Przykładem orzeczenia, w którym Trybunał wypowiadał się pośrednio w sprawie sztucznej inteligencji, jest również polska skarga *Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce*⁴³. Wyrok został wydany w 2024 r. i dotyczył oceny legalności stosowania środków niejawnego nadzoru przez polskie służby oraz skuteczności środków prawnych służących ich zakwestionowaniu. Teza wyroku stanowi, że „[w] niniejszej sprawie skarżący zarzucili ingerencję w wykonywanie swego prawa [...], która to ingerencja nie miała wynikać z zastosowania konkretnych środków kontroli operacyjnej w stosunku do skarżących, lecz z samego istnienia przepisów prawa pozwalających na niejawną kontrolę ich komunikacji, jak i z ryzyka zastosowania takich środków wobec skarżących. [...] Skarżący zakwestionowali odnośne przepisy prawne dotyczące kontroli niejawnej, w formie, w jakiej są one stosowane przez różne krajowe służby mundurowe i wywiadowcze. Trzeba wskazać, z jednej strony, iż system prawny kontroli niejawnej składa się z wielu przepisów prawnych regulujących funkcjonowanie odnośnych służb państwowych, a z drugiej strony, całość odnośnych przepisów realizuje jeden analogiczny model stosowania takiej kontroli”⁴⁴. Trybunał podkreślił, że w kwestii systemów sztucznej inteligencji „[w]obec postępu technologicznego, który miał miejsce w ciągu dwóch ostatnich dekad w sferze komunikacji elektronicznej, taka komunikacja może obecnie ujawniać duże ilości danych osobowych. Nadto, każda ingerencja spowodowana przez pozyskanie odnośnych danych telekomunikacyjnych jest zwielokrotniona przez jej masowy charakter, jako że dane takie

⁴² Ibidem.

⁴³ Wyrok ETPC z 28 V 2024 r. w sprawie *Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce*, skarga nr 72038/17; zob. M. Rojszczak, *Polskie przepisy inwigilacyjne na tle standardów europejskich – glosa do wyroku Europejskiego Trybunału Praw Człowieka z 28.05.2024 r., skargi nr 72038/17 i 25237/18, Pietrzak i Bychawska-Siniarska i in. Przeciwko Polsce*, „Europejski Przegląd Sądowy” 2025, nr 1.

⁴⁴ M. Rojszczak, *Polskie przepisy inwigilacyjne...*; zob. B. Opaliński, *Pozyskiwanie danych telekomunikacyjnych przez Agencję Bezpieczeństwa Wewnętrznego po wyroku Trybunału Konstytucyjnego z 30 lipca 2014 roku*, „Ius Novum” 2017, nr 3, s. 143–162.

mogą stanowić przedmiot analiz i badań pozwalających na stworzenie intymnego portretu danej osoby poprzez monitorowanie jej działań w sieciach społecznościowych, jej przemieszczania się, surfowania po Internecie, jak i nawyków komunikacyjnych, oraz przez poznanie jej kontaktów. Pozyskiwanie odnośnych danych telekomunikacyjnych w toku masowego gromadzenia danych może być tak samo inwazyjne, jak pozyskiwanie treści komunikacji, a tym samym pozyskiwanie i retencja danych tego rodzaju, jak i badania prowadzone na tychże danych, muszą być analizowane w kontekście takich samych gwarancji, jakie mają zastosowanie do treści komunikacji, przy czym nie ma konieczności, by przepisy prawne regulujące przetwarzanie takich danych były w każdym aspekcie identyczne z przepisami regulującymi przetwarzanie treści komunikacji⁴⁵.

Natomiast w orzeczeniu z 2019 r. w sprawie *Einarsson przeciwko Islandii*⁴⁶ wprost pojawia się termin *sztuczna inteligencja*. Skarga dotyczyła zarzutu braku bezstronności jednego z sędziów składu orzekającego sądu krajowego oraz odmowy dostępu do dokumentacji. Jest to orzeczenie wyjątkowe na tle pozostałego przedstawionego orzecznictwa ETPC, które nie odnosiło się wprost do systemów AI. Jeden z sędziów ze składu orzekającego, sędzia Pavli, w częściowo rozbieżnej opinii zwrócił uwagę, że „[s]ądy w co najmniej dwóch jurysdykcjach (Zjednoczone Królestwo i Irlandia) zatwierdziły w ostatnich latach wykorzystanie analizy wspomaganej technologicznie, wykorzystującej formę sztucznej inteligencji znaną jako kodowanie predykcyjne, dla celów ujawniania dowodów elektronicznych w postępowaniach cywilnych o dużym znaczeniu. Logika ta znajdowałaby takie samo zastosowanie w sprawach karnych o porównywalnym stopniu złożoności. Warunkiem leżącym u podstaw wykorzystania tego rodzaju zaawansowanej technologii jest oczywiście to, by obydwie strony od początku miały zapewniony możliwie szeroki dostęp do danych. Po drugie, ramy postępowania karnego i praktyki dochodzeniowo-śledcze muszą być zorganizowane w taki sposób, aby umożliwić obronie odpowiedni dostęp na odpowiednim (tj. wczesnym) etapie postępowania⁴⁷.

⁴⁵ Wyrok ETPC z 28 V 2024 r. w sprawie *Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce*, op. cit.

⁴⁶ Wyrok ETPC z 4 IX 2019 r. w sprawie *Einarsson i inni przeciwko Islandii*, skarga nr 39757/15.

⁴⁷ Ibidem.

Podsumowując powyższe, dotychczasowe orzecznictwo strasburskie w kontekście AI można podzielić zasadniczo na trzy rodzaje: (1) dotyczące negatywnych skutków pozyskiwania i przechowywania danych osobowych, (2) skargi na krajowe procedury związane z szeroko pojętą inwigilacją stosowaną przez organy krajowe oraz (3) jeden przykład wyroku, w którym Trybunał odwołał się bezpośrednio do systemów sztucznej inteligencji. Analiza orzecznictwa ETPC dotyczącego naruszeń wolności i praw człowieka przez systemy sztucznej inteligencji wskazuje, że w znakomitej większości przypadków podstawę skargi stanowi naruszenie art. 8 EKPC (prawa do prywatności): „[k]ażdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji; niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób”⁴⁸. Tylko w jednym przypadku, wyrok *Einarsson przeciwko Islandii*, skarga opierała się na art. 6 EKPC (prawie do rzetelnego procesu sądowego), który stanowi, że „[k]ażdy ma prawo do sprawiedliwego i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony ustawą przy rozstrzyganiu o jego prawach i obowiązkach o charakterze cywilnym albo o zasadności każdego oskarżenia w wytoczonej przeciwko niemu sprawie karnej”⁴⁹. Szeroko pojęte prawo do prywatności, ochrona informacji o osobie, w tym ochrona danych biometrycznych, stanowią jak dotąd najczęstszą podstawę złożenia skarg do ETPC.

Podsumowanie

Problematyka systemów sztucznej inteligencji w kontekście naruszeń wolności i praw człowieka jest obecnie bardzo istotna. Przede wszystkim nowe technologie coraz mocniej osadzają się w ludzkiej rzeczywistości. Niezwykle intensywny rozwój technologiczny sprawia, że wykorzystanie AI w kolejnych sferach życia człowieka staje się powszechne.

⁴⁸ Art. 8 EKPC.

⁴⁹ Art. 6 EKPC.

Wymaga to od ustawodawcy krajowego i międzynarodowego reakcji, czujności oraz wyczucia.

Wprowadzenie międzynarodowych przepisów poświęconych sztucznej inteligencji zasługuje na najwyższą aprobatę. Systemy AI nie są czymś nowym, funkcjonują w przestrzeni ludzkiej na coraz to wyższym poziomie zaawansowania od kilkudziesięciu lat. W związku z tym czas oczekiwania na sprecyzowany system prawny, odpowiadający specyfice sztucznej inteligencji, był stosunkowo długi. Nadmienić należy, że nie zawsze inne przepisy prawa, z których czerpała AI, były wystarczające.

Dotychczasowe orzecznictwo ETPC w zakresie sztucznej inteligencji jest nieliczne. Dotąd Trybunał nie orzekał jeszcze w żadnej sprawie opartej na skardze o naruszenie wolności i praw jednostki w związku ze stosowaniem systemów sztucznej inteligencji, chociaż z pełnym przekonaniem można stwierdzić, że takie wyroki w niedalekiej przyszłości zaczną się pojawiać. Warto nadmienić, że sama specyfika skargi do ETPC, w tym przede wszystkim wymóg wyczerpania prawnej drogi krajowej, sprawia, że upłynie jeszcze trochę czasu, zanim pojawi się pierwsze orzecznictwo strasburskie mające za podstawę *stricte* kwestie łamania praw człowieka w związku z działalnością AI. Nie zmienia to jednak faktu, że w orzecznictwie ETPC istnieją wyroki, w których Trybunał dostrzegł zagrożenia spowodowane rozwojem i postępem technologicznym. Sprawy te dotyczą głównie pozyskiwania, przetwarzania i przechowywania wrażliwych danych obywateli przez organy państwowe. Zatem przede wszystkim chodzi o art. 8 EKPC, który dotyczy szeroko rozumianej ochrony prawa do prywatności. Jest ono bowiem główną wartością narażoną na zagrożenia ze strony wykorzystywania sztucznej inteligencji. Zgodnie z zaprezentowanym orzecznictwem ETPC potrzebny jest rozwój prawnych gwarancji chroniących przed ewentualnymi ingerencjami ze strony AI. Z całą pewnością należy stwierdzić, że rozwojowi nowych technologii, w tym systemów sztucznej inteligencji, towarzyszyć powinien stały rozwój wspomnianych gwarancji.

Chociaż, jak wspomniano wyżej, aktualnie brakuje orzecznictwa strasburskiego opartego *stricte* na przypadkach naruszeń praw jednostki przez zastosowanie systemów sztucznej inteligencji, to omówione wyroki można ocenić jako zdecydowanie cenne wskazówki dla ustanowienia przez systemy krajowe gwarancji i ochrony podstawowych praw człowieka w kontekście rozwoju AI. W swoich uzasadnieniach ETPC wskazał uwagi mające znaczenie dla wykorzystania sztucznej inteligencji, lecz wprost nie stanowią one podstawy orzekania. Można

wyróżnić przede wszystkim wymóg określenia przejrzystych i konkretnych zasad wykorzystywania systemów sztucznej inteligencji w działaniach podejmowanych przez organy państwowe w ramach prowadzonych działań operacyjnych, w tym podsłuchu rozmów, odczytu wiadomości oraz innych działań z zakresu inwigilacji. Z tych wskazówek powinien korzystać przede wszystkim ustawodawca krajowy w pierwszym kroku, jakim będzie wprowadzenie do wewnętrznego porządku prawnego ustawy poświęconej systemom sztucznej inteligencji. Ma to bowiem podwójnie istotne znaczenie. Z jednej strony stwarza gwarancje ochrony praw człowieka oraz określa ramy dla działań władzy publicznej. Natomiast z drugiej – umożliwia obywatelowi rozeznanie, co innym podmiotom oraz organom władzy publicznej wolno w zakresie jego wolności i praw oraz jakimi środkami mogą się one posługiwać.

BIBLIOGRAFIA

- Bałos I., *Sztuczna inteligencja i jej wynalazki – studium przypadku*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego” 2020, nr 1, s. 95–115.
- Berdowska A., *Wspomaganie procesu rekrutacji pracowników za pomocą chatbotów – analiza wybranych rozwiązań*, „Zarządzanie Zasobami Ludzkimi” 2018, nr 5, s. 93–112.
- Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, LEX/el. 2015.
- Goździaszek Ł., *Elektroniczne postępowanie upominawcze – doświadczenia i przyszłość*, w: *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, pod red. J. Gołaczyńskiego, Warszawa 2022, s. 190–200.
- Jabłoński M., *Nowoczesne technologie sztucznej inteligencji a konstytucyjne prawo do sądu*, w: *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, pod red. J. Gołaczyńskiego, Warszawa 2022, s. 229–244.
- Jankowska-Augustyn M., *Podmiotowość prawna sztucznej inteligencji?*, w: *O czym mówią prawnicy, mówiąc o podmiotowości*, pod red. A. Bielskiej-Brodziak, Katowice 2015, s. 171–196.
- Kozłowski J., *Akt w sprawie sztucznej inteligencji w praktyce – charakterystyka unijnej regulacji opartej na ryzyku*, „Europejski Przegląd Sądowy” 2024, nr 12, s. 20–25.
- Kusznieruk P., *Wpływ rozwoju sztucznej inteligencji na proces stanowienia prawa w Polsce*, „Przegląd Prawa Publicznego” 2023, nr 5, s. 7–18.
- Mazur J., *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, „Europejski Przegląd Sądowy” 2020, nr 9, s. 13–18.

- Męcina J., *Od cyfryzacji i robotyzacji do sztucznej inteligencji. Wyzwania dla gospodarki i rynku pracy*, Warszawa 2023.
- Michalak A., *Projekt rozporządzenia Parlamentu UE o odpowiedzialności cywilnej za działania systemów sztucznej inteligencji – krok w dobrym kierunku czy niepotrzebne odstępstwo od zasad ogólnych?*, w: *Prawo sztucznej inteligencji i nowych technologii*, pod red. B. Fischera, A. Pązika, M. Świerczyńskiego, Warszawa 2021, s. 41–50.
- Opaliński B., *Pozyskiwanie danych telekomunikacyjnych przez Agencję Bezpieczeństwa Wewnętrznego po wyroku Trybunału Konstytucyjnego z 30 lipca 2014 roku*, „Ius Novum” 2017, nr 3, s. 143–162.
- Rojszczak M., *Polskie przepisy inwigilacyjne na tle standardów europejskich – glosa do wyroku Europejskiego Trybunału Praw Człowieka z 28.05.2024 r., skargi nr 72038/17 i 25237/18, Pietrzak i Bychawska-Siniarska i in. Przeciwko Polsce*, „Europejski Przegląd Sądowy” 2025, nr 1, s. 31–43.
- Rojszczak M., *Prawne aspekty systemów sztucznej inteligencji – zarys problemu*, w: *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, pod red. K. Flagi-Gieruszyńskiej, J. Gołaczyńskiego, D. Szostka, Warszawa 2019, s. 1–21.
- Różanowski K., *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, „Zeszyty Naukowe WWSI” 2007, nr 2, s. 109–135.
- Rzymowski J., *Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji*, „Przegląd Prawa Publicznego” 2024, nr 11, s. 56–63.
- Sakowska-Baryła M., *Sztuczna inteligencja w sektorze publicznym*, w: *Prawo sztucznej inteligencji i nowych technologii*, t. 3, pod red. B. Fischera, A. Pązika, M. Świerczyńskiego, Warszawa 2023, s. 31–51.
- Stefanicki R., *Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana*, „Przegląd Prawa Handlowego” 2023, nr 1, s. 4–15.
- Studzińska J., *Informatyzacja postępowania egzekucyjnego – elektroniczne akta komornicze. Postulat czy rzeczywistość?*, w: *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, pod red. J. Gołaczyńskiego, Warszawa 2022, s. 245–256.
- Topol E., *Medycyna głęboka. Jak sztuczna inteligencja może przywrócić opiece zdrowotnej ludzką twarz*, tłum. A. Boniszewska, Warszawa 2021.
- Zalesińska A., *Doręczenie elektroniczne w postępowaniu cywilnym*, w: *Prawo nowych technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, pod red. J. Gołaczyńskiego, Warszawa 2022, s. 136–147.