ADAM WIŚNIEWSKI

Sztuczna inteligencja i prawa człowieka w kontekście prawa międzynarodowego

Artificial Intelligence and Human Rights in the Context of International Law

This paper aims to provide answers to questions about how the most advanced regulations at the international or supranational level in the EU and the CoE, as well as the jurisprudence of the European Court of Human Rights (ECtHR), address the problems of threats to human rights resulting from the development of AI technologies. After characterizing these regulations, an analysis was made of selected ECtHR judgments. Research problems in the analysis carried out in this study are connected, in particular, with the differences and similarities between the compared standards in the context of threats associated with AI technologies and their significance in the future.

ADAM WIŚNIEWSKI, doktor habilitowany nauk prawnych,
profesor Uniwersytetu Gdańskiego
ORCID – 0000-0002-4921-0215, e-mail: praaw@wp.pl

SŁOWA KLUCZOWE: Sztuczna inteligencja, prawa człowieka, Unia Europejska, Rada Europy, Europejski Trybunał Praw Człowieka

KEYWORDS: Artificial intelligence, human rights, European Union, Council of Europe, European Court of Human Rights

HTTPS://DOI.ORG/10.36128/PRIW.VI47.785

1 Uwagi ogólne

Rozwój technologii opartych na sztucznej inteligencji (dalej: SI), który bez wątpienia uległ w ostatnich latach znaczącemu przyspieszeniu, zmusza do postawienia szeregu pytań o zagrożenia wynikające z tego zjawiska. Rozwój ten jest bowiem nieunikniony i może być oceniany pozytywnie umożliwiając, m.in. zwiększanie efektywności. Z drugiej jednak strony rozwojowi sztucznej inteligencji towarzyszą nieodłącznie także aspekty negatywne związane w szczególności z zagrożeniem dla ochrony praw człowieka. Trudno obecnie wyobrazić sobie w jakim kierunku dokładnie podążą szybkie zmiany w tym zakresie, widać jednak, iż zjawisko SI w coraz większym stopniu przenika do codziennego życia. Zagrożeniom tym starają się wychodzić naprzeciw różne inicjatywy prawodawcze, podejmowane obecnie zarówno na poziomie krajowym, jak i międzynarodowym. Rozwój i wdrażanie systemów opartych na sztucznej inteligencji prowadzi do stosowania technologii, które cechuje różny stopień złożoności i automatyzacji. Pośród praw, które są szczególnie zagrożone w związku z rozwojem zjawiska sztucznej inteligencji wymienia się nie tylko prawo do prywatności oraz ochronę danych osobowych, zasadę równości i zakaz dyskryminacji, ale także prawa związane z prawem do rzetelnego procesu, prawo do wolności zgromadzeń czy wolność wypowiedzi oraz wolność religii[1]. W raporcie Agencji Praw Podstawowych na ten temat zwraca się uwagę, iż „potencjalnie stronnicza decyzja podjęta przy zastosowaniu algorytmu może wiązać się z prawem do niedyskryminacji, ochrony danych osobowych oraz prawem do skutecznego środka odwoławczego. Podobnie na daną kwestię można spojrzeć z perspektywy różnych praw. Na przykład dobre wyjaśnienie decyzji podjętej przez algorytm jest wymagane na podstawie prawa do ochrony danych osobowych, prawa do dobrej administracji oraz prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu”.[2] Wynika to m.in. z różnic dotyczących przypisywania priorytetowego znaczenia prawom człowieka, które mogą być zagrożone rozwojem zjawiska AI, dotyczy to zwłaszcza takich praw, jak prawo do prywatności[3].

1 Zob. Getting The Future Right Artificial Intelligence and Fundamental Rights, raport Agencji Praw Podstawowych, European Union Agency for Fundamental Rights, 2020, ss. 57–82, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf. [dostęp: 12.06.2023].

2 Ibidem, 57.

3 Ibidem, 22.

W opracowaniach poświęconych zagadnieniu SI w kontekście prawa międzynarodowego zwraca się uwagę, iż największe doświadczenie w zakresie tworzenia regulacji międzynarodowych lub ponadnarodowych w zakresie sztucznej inteligencji posiadają takie organizacje jak Organizacja Współpracy Gospodarczej i Rozwoju, Organizacja Współpracy Gospodarczej i Rozwoju, Unia Europejska (EU) oraz Rada Europy (RE) [4]. Znamienne jest przy tym, iż najbardziej zaawansowane prace, jeśli chodzi o tworzenie norm dotyczących sztucznej inteligencji, prowadzone są w ramach takich organizacji regionalnych, jak UE[5] oraz RE. W ramach UE zwrócić należy zwłaszcza uwagę na przyjęty 14 czerwca 2023 r. przez Parlament Europejski projekt Rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Rozporządzenie w sprawie SI) i zmieniające niektóre akty ustawodawcze Unii. Szereg działań podjęto także pod auspicjami Rady Europy, w ramach której funkcjonuje, przypomnijmy, najbardziej skuteczny regionalny system ochrony praw człowieka oparty na Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności z 1950 roku (EKPC). Konwencja ta, aczkolwiek określana jest mianem „klejnotu w koronie" Rady Europy, przyjęta siedemdziesiąt lat temu, zawiera ogólnie sformułowane prawa, które nabierają uszczegółowioną postać dzięki bogatemu orzecznictwu Europejskiego Trybunału Praw Człowieka. Trybunał wydaje znakomitą większość orzeczeń na skutek skarg indywidulanych zarzucających naruszenie EKPC przez jedno z państw-stron Konwencji. W lutym 2023 r. Komitet Rady Europy do spraw Sztucznej Inteligencji opublikował „zerowy" projekt Konwencji w sprawie sztucznej inteligencji, praw człowieka, demokracji i praworządności. Datowany na 6 stycznia 2023 r. dokument zawiera wstępną propozycję Rady Europy dotyczącą przyszłych ram regulacyjnych sztucznej inteligencji[6].

4 Świerczyński Marek, Więckowski Zbigniew, „Sztuczna inteligencja w prawie międzynarodowym. Rekomendacje wybranych rozwiązań", Warszawa: Wydawnictwo Difin, 2021 r., s. 19.

5 Zob. m.in. Brattnerg Erik, Csernatoni Raculuca, Rugova Venesa, „Europe and AI: Leading, Lagging Behind, or Carving its Own Way", Carnegi Endowment for International Peace, July 2020, s. 3.

6 W lipcu 2023 r. opublikowano ujednolicony projekt roboczy Konwencji Ramowej o sztucznej inteligencji, prawach człowieka, demokracji i praworządności: „Consolidated Working Draft of The Framework Convention on Artificial Intelligence, Human Rights, Democracy and The Rule Of Law, https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66 [dostęp: 18.10.2023].

Bez wątpienia zarówno wspomniane unijne Rozporządzenie, będące pierwszą próbą regulacji zagadnienia sztucznej inteligencji, jak i Konwencja Rady Europy w sprawie sztucznej inteligencji po ich wejściu w życie będą oddziaływać na orzecznictwo ETPC, stanowiąc wyraz kształtującego się konsensusu państw-stron EKPC w tej dziedzinie.

Celem niniejszego opracowania jest podjęcie próby odpowiedzi na pytania o to, jak wspomniane regulacje oraz orzecznictwo strasburskie podchodzą do zagadnienia zagrożeń dla praw jednostki stwarzanych przez rozwój technologii opartych na sztucznej inteligencji. Po dokonaniu charakterystyki najważniejszych regulacji dotyczących SI tworzonych obecnie w ramach UE oraz RE, które jednocześnie można uznać za stosunkowo najbardziej zaawansowane w sferze międzynarodowej, przedstawione zostaną wybrane orzeczenia ETPC związane są ze zjawiskiem SI. Idzie tu zwłaszcza o orzecznictwo w kontekście praw najbardziej narażonych na naruszenie w związku z rozwojem i zastosowaniem systemów opartych na sztucznej inteligencji. Problemy badawcze związane z prowadzoną w tym opracowaniu analizą wiążą się w szczególności ze wskazaniem różnic oraz podobieństw pomiędzy ocenianymi standardami dotyczącymi technologii wykorzystujących SI w kontekście zagrożeń jakie stwarzają dla praw jednostki oraz ich znaczenia w przyszłości.

2 Unia Europejska

W ramach UE podejmowanych jest wiele przedsięwzięć o charakterze legislacyjnym związanych ze zjawiskiem sztucznej inteligencji. Przykładowo w październiku 2020 r. Parlament Europejski przyjął szereg rezolucji związanych ze sztuczną inteligencją, w tym w sprawie aspektów etycznych[7], odpowiedzialności[8] i praw autorskich[9]. Wspomnieć też warto o przyjętej

7 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).

8 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję, 2020/2014(INL).

9 Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji, 2020/2015(INI).

28 września 2022 r. przez Komisję Europejską projekcie dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję (SI Liability Directive, AILD). Uzupełnia ona unijne ramy odpowiedzialności cywilnej, wprowadzając regulacje dotyczące szkód wyrządzonych przez systemy SI. Celem tej dyrektywy jest wprowadzenie większej ochrony ofiar systemów SI za sprawą ułatwienia dochodzenia roszczeń o odszkodowanie, jak również także wspieranie sektora sztucznej inteligencji.

Wspomniany na wstępie projekt Rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniające niektóre akty ustawodawcze przyjęty 14 czerwca 2023 r. przez Parlament Europejski, aczkolwiek stanowi regulację znajdującą się nadal na jednym z etapów w stosunkowo długotrwałym procesie legislacyjnym prowadzącym do wejścia tego Rozporządzenia w życie, już obecnie może zostać uznany za posiadający charakter wiodący a zarazem pionierski[10]. Główny cel inicjatywy związanej z przyjęciem Rozporządzenia UE w sprawie SI wiąże się z potrzebą zapewnienia należytego funkcjonowania rynku wewnętrznego poprzez określenie zharmonizowanych przepisów dotyczących wykorzystywania technologii SI[11]. Zwraca się przy tym uwagę na zagrożenia związane z podejmowaniem nieskoordynowanych działań w tym zakresie na poziomie krajowym, łączący się przede wszystkim z możliwością fragmentacji rynku wewnętrznego oraz spadku pewności prawa „co do tego, w jaki sposób dotychczasowe i nowe przepisy będą miały zastosowanie do takich systemów w Unii"[12].

Dla potrzeb niniejszego opracowania istotne jest przede wszystkim znaczenie proponowanego Rozporządzenia dla ochrony praw podstawowych w kontekście wykorzystywania technologii SI. We wniosku dotyczącym Rozporządzenia stwierdzono, iż proponowany akt wzmocni i będzie promował ochronę praw chronionych Kartą „dzięki zestawowi wymogów dotyczących wiarygodnej sztucznej inteligencji oraz proporcjonalnym obowiązkom nałożonym na wszystkich uczestników łańcucha wartości"[13]. Do praw chronionych w tym przypadku zaliczono: prawo do godności

10 Zob. m.in. Brattnerg, Csernatoni, Rugova, „Europe and AI", 3.

11 Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii. SEC (2021) 167 final, SWD (2021) 84 final, SWD (2021) 85 final. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206, 7 [dostęp: 20.10.2023].

12 Ibidem.

13 Ibidem, 13.

człowieka (art. 1), poszanowanie życia prywatnego i ochrona danych osobowych (art. 7 i 8), niedyskryminację (art. 21) oraz równość kobiet i mężczyzn (art. 23). Celem ma być również zapobieganie ograniczaniu prawa do wolności wypowiedzi (art. 11) i wolności zgromadzania się (art. 12), zapewnienie ochrony prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu, prawa do obrony i domniemania niewinności (art. 47 i 48), jak również ogólnej zasady dobrej administracji. Wspomniano też, iż w określonych dziedzinach Rozporządzenie będzie miało pozytywny wpływ na prawa wielu szczególnych grup, takie jak prawa pracowników do należytych i sprawiedliwych warunków pracy (art. 31), wysoki poziom ochrony konsumentów (art. 28), prawa dziecka (art. 24) oraz integracja osób niepełnosprawnych (art. 26)[14].

Z punktu widzenia analizy prowadzonej w tym opracowaniu istotne jest to, iż Rozporządzenie UE w sprawie SI poddaje regulacji rozwój systemów opartych na sztucznej inteligencji z punktu widzenia zagrożeń jakie stwarzają one dla zdrowia, bezpieczeństwa lub praw podstawowych. W Rozporządzeniu tym zastosowano podejście oparte na analizie ryzyka, wprowadzając rozróżnienie między zastosowaniami AI, które stwarzają (i) niedopuszczalne ryzyko, (ii) wysokie ryzyko oraz (iii) niskie lub minimalne ryzyko[15]. W zależności od poziomu ryzyka Roporządzenie wprowadza różne obowiązki dla dostawców i użytkowników.

W tytule II pojawił się wykaz zakazanych praktyk, który obejmuje wszystkie systemy sztucznej inteligencji, których wykorzystywanie uznaje się za niedopuszczalne ze względu na ich sprzeczność z wartościami Unii, a zatem np. prawami podstawowymi. Zakaz obejmuje o systemy, które:

1. opierają się na manipulacji poznawczo-behawioralnej: na przykład zabawki aktywowane głosem, które zachęcają dzieci do niebezpiecznych zachowań;
2. zakładają stosowanie klasyfikacji społecznej osób na podstawie zachowania, statusu społeczno-ekonomicznego lub cech osobistych;
3. działające w czasie rzeczywistym i zdalne systemy identyfikacji biometrycznej, takie jak systemy rozpoznawanie twarzy[16].

14 Ibidem.
15 Ibidem, 15.
16 Ibidem.

Z kolei w tytule III Rozporządzenia zawarto przepisy szczegółowe dotyczące systemów sztucznej inteligencji, które stwarzają wysokie ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych osób fizycznych. Systemy takie mogą zostać dopuszczone do obrotu na rynku europejskim pod warunkiem spełnienia określonych wymogów obowiązkowych i przeprowadzenia oceny zgodności *ex ante*. Klasyfikacja systemu sztucznej inteligencji jako systemu wysokiego ryzyka opiera się na przeznaczeniu systemu AI zgodnie z obowiązującymi przepisami dotyczącymi bezpieczeństwa produktów. Z tego powodu zaklasyfikowanie danego systemu jako systemu SI wysokiego ryzyka zależy nie tylko od funkcji pełnionej przez system sztucznej inteligencji, ale także od konkretnego celu i trybu jego wykorzystania.

Wyróżniono dwie główne kategorie systemów sztucznej inteligencji wysokiego ryzyka:

1. systemy sztucznej inteligencji przeznaczone do wykorzystywania jako związane z bezpieczeństwem elementy produktów podlegających ocenie zgodności *ex ante* przeprowadzanej przez osoby trzecie;
2. inne samodzielne systemy sztucznej inteligencji mające wpływ głównie na prawa podstawowe, które wyraźnie wymieniono w załączniku III do Rozporządzenia. Zawarty tam wykaz systemów sztucznej inteligencji wysokiego ryzyka zawiera ograniczoną liczbę systemów sztucznej inteligencji, w przypadku których ryzyko już się urzeczywistniło lub może się urzeczywistnić w najbliższej przyszłości. Aby zapewnić możliwość dostosowania rozporządzenia do pojawiających się sposobów wykorzystania i zastosowań AI, Komisja może rozszerzyć wykaz systemów sztucznej inteligencji wysokiego ryzyka wykorzystywanych w pewnych z góry określonych obszarach, stosując zestaw kryteriów i metodykę oceny ryzyka.

W Rozporządzeniu istotną rolę przypisano nadzorowi nad systemami wysokiego ryzyka, który ma pełnić człowiek. Warto zwrócić uwagę, że w art. 14 Rozporządzenia postanowiono, iż systemy sztucznej inteligencji wysokiego ryzyka projektuje się i opracowuje się w taki sposób, w tym poprzez uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie wykorzystywania systemu sztucznej inteligencji wysokiego ryzyka mogły je skutecznie nadzorować osoby fizyczne.

Przewidziano wymóg, iż systemy sztucznej inteligencji wysokiego ryzyka należy projektować i opracowywać się w taki sposób, aby osiągały, z uwagi na ich przeznaczenie, odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz działały konsekwentnie pod tymi względami w całym cyklu życia (art. 15).

Systemy sztucznej inteligencji o ograniczonym ryzyku powinny natomiast spełniać minimalne wymogi w zakresie przejrzystości, które będą umożliwiać użytkownikom podejmowanie świadomych decyzji. Po interakcji z aplikacjami użytkownik będzie mógł zdecydować, czy chce dalej z nich korzystać. Użytkownicy powinni być świadomi interakcji z sztuczną inteligencją. Obejmuje to systemy sztucznej inteligencji, które generują obrazy, treści audio lub wideo lub manipulują nimi, na przykład *deepfakes*[17].

Z kolei tzw. generatywna sztuczna inteligencja, a zatem np. ChatGPT, będzie musiała spełniać wymogi związane z zapewnieniem przejrzystości. Obowiązki w zakresie przejrzystości będą miały zastosowanie do systemów, które (i) wchodzą w interakcję z człowiekiem, (ii) są wykorzystywane do wykrywania emocji lub określania powiązań z kategoriami (społecznymi) na podstawie danych biometrycznych lub (iii) generują treści lub manipulują nimi (technologia deepfake). Minimalne ryzyko związane z technologiami SI obejmuje aplikacje takie jak filtry spamu lub gry wideo oparte na sztucznej inteligencji. Proponuje się, aby w tych obszarach regulacja polegała głównie na dobrowolnych kodeksach postępowania[18].

W Rozporządzeniu w sprawie SI przewidziano, iż konieczne jest poinformowanie o zastosowaniu SI osób fizycznych wchodzących w interakcję się z systemem sztucznej inteligencji lub gdy ich emocje lub cechy charakterystyczne są rozpoznawane za pomocą środków zautomatyzowanych. Natomiast jeżeli system sztucznej inteligencji jest wykorzystywany do

17 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. [dostęp: 12.10.2023]. Zob. także The European Union's Artificial Intelligence Act, https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/. [dostęp: 14.10.2023]. SI Act: Different Rules for Different Risk Levels. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. [dostęp: 21.10.2023].

18 *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, 2021. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206, Article 69. [dostęp: 24.10.2023].

generowania obrazów, dźwięków lub treści wideo, które w znacznym stopniu przypominają autentyczne treści, lub do manipulowania takimi obrazami, dźwiękami lub treściami wideo, obowiązkowe ma być ujawnianie, że określone treści wygenerowano za pomocą środków zautomatyzowanych, z zastrzeżeniem sytuacji wyjątkowych dotyczących zgodnych z prawem celów (egzekwowanie prawa, wolność wypowiedzi). Ma to pozwolić tym osobom na dokonywanie świadomych wyborów lub na wycofanie się z danej sytuacji[19].

Warto zwrócić uwagę, iż w tytule VIII określono obowiązki dostawców systemów sztucznej inteligencji w zakresie monitorowania i zgłaszania zdarzeń. Obowiązki te mają dotyczyć monitorowania systemu po jego wprowadzeniu do obrotu oraz zgłaszania incydentów i przypadków nieprawidłowego działania związanych ze sztuczną inteligencją i prowadzenia dochodzeń w tych sprawach. Z kolei organy nadzoru rynku będą również kontrolować rynek i sprawdzać zgodność z obowiązkami i wymogami dotyczącymi wszystkich systemów sztucznej inteligencji wysokiego ryzyka już wprowadzonych do obrotu. Przewidziane egzekwowanie prawa *ex post* powinno zapewnić, aby po wprowadzeniu systemu sztucznej inteligencji do obrotu organy publiczne dysponowały uprawnieniami i zasobami umożliwiającymi interwencję w przypadku, gdy systemy sztucznej inteligencji generują nieoczekiwane ryzyko, które wymaga szybkiego działania. Będą one również monitorować spełnianie przez podmioty gospodarcze ich odpowiednich obowiązków wynikających z rozporządzenia[20].

Znaczenie Rozporządzenia UE w sprawie SI polega na tym, iż określa ono zharmonizowane zasady rozwoju, wprowadzania do obrotu i wykorzystania sztucznej inteligencji na terenie Unii Europejskiej zapobiegając rozwijaniu nieskoordynowanych regulacji w tym zakresie na poziomie krajowym[21]. Rozporządzenie powinno być postrzegane w kontekście innych głównych pakietów ogłoszonych przez UE, takich jak rozporządzenie o usługach cyfrowych (DSA), rozporządzenie o rynkach cyfrowych (DMA) czy o zarządzaniu cyfrowym (DGA). Pierwsze dwa akty regulują przede wszystkim bardzo duże komercyjne platformy internetowe, takie jak Google, Amazon, Facebook i Apple. Dodać należy, iż Rozporządzenie

19 Ibidem, 17.

20 Ibidem.

21 Liliane Edwards, *The EU AI Act: A Summary of its Significance and Scope* (London: Ada Lovelace Institute, 2022), 4. Expert-explainer-The-EU-AI-Act-11-April-2022.pdf. [dostęp: 29.10.2023].

nie zastępuje, ale będzie pokrywać się z ochroną, jaką zapewnia Ogólne Rozporządzenie o Ochronie Danych (RODO), chociaż zakres Rozporządzenia UE w sprawie SI jest szerszy i nie ogranicza się do danych osobowych[22].

Rozporządzenie UE w sprawie SI jest natomiast krytykowane m.in. z powodu zbyt szerokiego zakresu zastosowania, obejmuje ono bowiem systemy opracowane przy użyciu dowolnego podejścia wymienionego w załączniku I (uczenie się maszynowe, podejście logiczne i oparte na wiedzy czy podejście statystyczne), które mogą generować wyniki, takie jak treść, prognozy, rekomendacje, lub decyzje mające wpływ na „środowisko, z którym wchodzą w interakcje" (art. 3 ust. 1 i załącznik I). Wywołuje to obawy, że regulacja ta okaże się zbyt szeroka, obejmując większość współcześnie stosowanego i tworzonego oprogramowania. Sugeruje się też, iż ograniczenia wprowadzane w związku ze stosowaniem SI mogą doprowadzić do eliminacji istotnych rodzajów oprogramowania. Jak stwierdza Lilian Edwards, w rzeczywistości spory tego typu mają charakter akademicki, tymczasem operacyjne skutki rozporządzenia dotyczą przede wszystkim technologii opartych na SI zakwalifikowanych jako technologie SI wysokiego ryzyka, który zdefiniowane zostały stosunkowo precyzyjnie[23].

3 Rada Europy

Szereg inicjatyw prawotwórczych w dziedzinie SI podjęto również w ramach Rady Europy, która przoduje jak idzie o tworzenie międzynarodowych instrumentów prawnych w dziedzinie praw człowieka. Przypomnijmy, iż wszystkie 46 państw członkowskich RE ratyfikowało Europejską Konwencję Praw Człowieka będącą podstawowym i najważniejszym traktatem prawa człowieka w Europie. W 2020 roku Zgromadzenie Parlamentarne RE przyjęło rezolucję o Potrzebie Demokratycznego Zarządzania Sztuczną Inteligencją[24] i wezwało Radę Europy do „mocnego i szybkiego działania". Jednocześnie członkowie Zgromadzenia zwrócili uwagę, iż „instrumenty soft-law okazały się niewystarczające, jeśli chodzi o wychodzenie

22 Ibidem.
23 Ibidem, 7.
24 Need for democratic governance of artificial intelligence. Recommendation 2181 (2020). https://pace.coe.int/en/files/28804/html. [dostęp: 28.10.2023].

naprzeciw wyzwaniu oraz ochronie praw człowieka, demokracji i rządów prawa"[25]. Naprzeciw tym oczekiwaniom wychodzi wspomniany już projekt Konwencji w sprawie sztucznej inteligencji, praw człowieka, demokracji i praworządności opracowany przez stworzony w ramach Rady Europy przez Komitet do spraw Sztucznej Inteligencji. Komitet ten został powołany w 2021 roku z zadaniem „opracowania instrumentu prawnego dotyczącego rozwoju, projektowania i stosowania systemów sztucznej inteligencji w oparciu o standardy Rady Europy w zakresie praw człowieka, demokracji i praworządności oraz sprzyjającego innowacjom"[26].

W lipcu 2023 r. opublikowano ujednolicony projekt roboczy Konwencji Ramowej o sztucznej inteligencji, prawach człowieka, demokracji i praworządności. Wersja ta jest następstwem pierwszego czytania poprawionego projektu zerowego i została przygotowana przez przewodniczącego CSI przy pomocy Sekretariatu. Projekt ten ma służyć za podstawę do dalszych negocjacji. Zawiera on postanowienia, które wstępnie uzgodniono podczas pierwszego czytania poprawionego Projektu Zero, a także propozycje opracowane przez przewodniczącego przy pomocy Sekretariatu[27].

Projekt Konwencji opiera się na standardach Rady Europy w zakresie praw człowieka, demokracji i praworządności. W Preambule podkreślono „potrzebę zapewnienia poszanowania praw człowieka zapisanych w Konwencji Rady Europy o ochronie praw człowieka i podstawowych wolności z 1950 r. i Praw Politycznych oraz innych mających zastosowanie międzynarodowych traktatów dotyczących praw człowieka". Odwołano się także do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 r. i protokołów zmieniających. W ten sposób nowa Konwencja zostaje niejako osadzona w ramach istniejących już zobowiązań w zakresie ochrony praw człowieka.

Zgodnie z art. 1 ust. 1 Konwencji Ramowej ustanawia ona „pewne fundamtentalne zasady, reguły i prawa, których celem jest zapewnienie, iż

25 COE Parliamentarians Call for Democratic Governance of Artificial Intelligence. 31.10.2020. https://dukakis.org/center-for-ai-and-digital-policy/coe-parliamentarians-call-for-democratic-governance-of-artificial-intelligence/. [dostęp: 28.10.2023].

26 CSI – Committee on Artificial Intelligence. https://www.coe.int/en/web/artificial-intelligence/cai. [dostęp: 12.11.2023].

27 Ibidem. Oczekuje się, że ukończenie prac nad tekstem Konwencji nastąpi we wrześniu 2023 r., a ostateczna wersja zostanie przedłożona Komitetowi Ministrów Rady Europy w listopadzie 2023 r. W tej chwili nie jest jasne, czy nastąpi to zgodnie z harmonogramem i kiedy ostateczna wersja zostanie przyjęte brzmienie Konwencji

projektowanie, rozwój oraz stosowanie systemów opartych na sztucznej inteligencji jest w pełni zgodne z poszanowaniem praw człowieka, funkcjonowaniem demokracji oraz przestrzeganiem rządów prawa". Warto zaważyć, iż w ust. 1 tego mowa jest o ustanowieniu mechanizmu monitorowania w celu zapewnienia implementacji postanowień Konwencji Ramowej.

W art. 2 projektu Konwencji Ramowej zaproponowano prawną definicję systemów SI oraz terminów związanych z SI. Zaproponowanie definicji legalnych związanych ze stosowaniem SI należy ocenić pozytywnie. Kwestia braku odpowiedniej definicji stanowi sporą przeszkodę w dyskusjach na temat przyjęcia odpowiednich regulacji m.in. na poziomie Unii Europejskiej.

Zakres zastosowania Konwencji Ramowej określony został w jej artykule 4 ust. 1 oraz 3, gdzie w ust. 1 mowa jest o tym, iż ma ona „zastosowanie projektowania, rozwoju i stosowania systemów sztucznej inteligencji wykorzystywanych w kontekście obejmującym kwestie związane z poszanowaniem praw człowieka, funkcjonowaniem demokracji i przestrzeganiem praworządności [...]. Co więcej, Konwencja ma zastosowanie do takich systemów przez cały cykl ich życia, niezależnie od tego, czy działania te są podejmowane przez podmioty publiczne czy prywatne. Konwencja. Natomiast w ust. 3 tego artykułu znalazło się wyłączenie związane z dziedziną militarną, bowiem stwierdzono, iż „konwencja nie ma zastosowania do projektowania, rozwoju i stosowania systemów sztucznej inteligencji wykorzystywanych do celów związanych z obroną narodową".

Postanowienia Konwencji Ramowej sformułowane są na stosunkowo wysokim stopniu ogólności, formułują raczej zasady ogólne aniżeli szczegółowe regulacje, jak w przypadku unijnego Rozporządzenia UE w sprawie SI. Przykładem tego typu ogólnego postanowienia może być art. 6 Ramowej Konwencji określający wymogi dotyczące poszanowania praw człowieka. Zgodnie z jego treści, każde Państwo-Strona ma obowiązek podjęcia środków mających na celu „zminimalizowanie i, w miarę możliwości, zapobieganie wszelkim bezprawnym szkodom lub naruszeniom praw człowieka i podstawowych wolności, które mogłyby wyniknąć z niewłaściwego stosowania systemów sztucznej inteligencji przez władze publiczne".

Podobnie na wysokim stopniu ogólności sformułowany został wymóg zachowania wolności jednostki, godności ludzkiej i autonomii określony w art. 9 Ramowej Konwencji. W myśl tego postanowienia państwa zobowiązane zostały do podjęcia niezbędnych środków „w celu ochrony wolności jednostki, godności ludzkiej i autonomii, a w szczególności zdolności do podejmowania świadomych decyzji, wolnych od nadmiernych wpływów,

manipulacji lub szkodliwych skutków, które mogą niekorzystnie wpłynąć na prawo do wolności wypowiedzi i zgromadzeń, uczestnictwa w demokracji i korzystanie z innych odpowiednich praw człowieka i podstawowych wolności w wyniku niewłaściwego zastosowania systemu sztucznej inteligencji".

W rozdziale III zatytułowanym „Zastosowanie systemów sztucznej inteligencji w dostarczaniu towarów, obiektów i usług" przewidziano w istocie również szereg zasad dotyczących Ochrony wolności jednostki, godności ludzkiej i autonomii (art. 9), dostępu do debaty publicznej i włączających procesów demokratycznych (art. 10) oraz ochrony zdrowia publicznego i środowiska (art. 11).

W świetle wspomnianego art. 9 zobowiązanie po stronie państwa-strony zostało sformułowane, podobnie jak w innych postanowieniach, jako obowiązek „podjęcia niezbędnych środków". Środki te mają zostać podjęte „w celu ochrony wolności jednostki, godności ludzkiej i autonomii, a w szczególności zdolności do podejmowania świadomych decyzji, wolnych od nadmiernych wpływów, manipulacji lub szkodliwych skutków, które mogą niekorzystnie wpłynąć na prawo do wolności wypowiedzi i zgromadzeń, uczestnictwa w demokracji i korzystanie z innych odpowiednich praw człowieka i podstawowych wolności w wyniku niewłaściwego zastosowania systemu sztucznej inteligencji". Z kolei np. obowiązek ochrony zdrowia publicznego i środowiska polegać ma na obowiązku podjęcia przez poszczególne państwa niezbędnych środków „w celu ochrony zdrowia publicznego i środowiska w kontekście stosowania systemu sztucznej inteligencji".

W rozdziale IV określone zostały podstawowe zasady projektowania, rozwoju i stosowania systemów sztucznej inteligencji obejmujące zasady: równości i przeciwdziałania dyskryminacji, ochrony prywatności i danych osobowych, odpowiedzialności prawnej, przejrzystości i nadzoru, bezpieczeństwa bezpiecznej innowacji oraz Konsultacje społeczne zawierają dodatkowe informacje.

W Konwencji przewidziano odrębny rozdział (V) dotyczący środków i zabezpieczeń zapewniających odpowiedzialności i możliwość dochodzenia zadośćuczynienia. Wprowadzono tu obowiązek każdego z państw-stron podjęcia środków zapewniających „możliwość zadośćuczynienia za jakąkolwiek bezprawną krzywdę lub naruszenie praw człowieka i podstawowych wolności wynikających ze stosowania systemów sztucznej inteligencji poprzez" zapewnienie rejestracji oraz archiwizacji użycia SI, która będzie komunikowana użytkownikom tych systemów oraz zapewnienia,

że taka komunikacja będzie zawierała wystarczające informacje, tak, aby istniała skuteczna możliwość zakwestionowania zastosowania systemu SI lub zaskarżenia decyzji wpływającej na prawa i wolności osoby będącej ofiarą SI. Obowiązkiem państwa jest też zapewnienie skutecznych mechanizmów dochodzenia roszczeń w takich przypadkach.

Wspomniany wcześniej mechanizm implementacji uregulowany w Rozdziale VII przewiduje m.in. obowiązek po stronie państw stron ustanowienia lub wyznaczenia krajowych organów nadzorczych, których zadaniem będzie w szczególności nadzorowanie i nadzorowanie przestrzegania wymogów dotyczących oceny ryzyka i skutków systemów sztucznej inteligencji.

Oceniając projekt Konwencji Ramowej zwrócić należy przede wszystkim uwagę na stosunkowo ogólne sformułowanie obowiązków państw-stron, co wiąże się z ramowym charakterem zasad zawartych w Konwencji Ramowej w porównaniu ze znaczenie bardziej szczegółowymi postanowieniami Rozporządzenia UE w sprawie SI. Ten ramowy charakter postanowień Konwencji Ramowej może stwarzać problemy na etapie kontrolowania implementacji jej postanowień na poziomie krajowym. W projekcie przyjęto wprawdzie ogólną definicję „systemu sztucznej inteligencji", brak jest jednak zniuansowania zastosowania postanowień Konwencji do różnych systemów SI w zależności od zagrożeń, które stwarzają. Pod tym względem podejście przyjęte w projekcie Rozporządzenia UE w sprawie SI opartego na analizie ryzyka oraz wprowadzającego rozróżnienie między zastosowaniami AI, które stwarzają różne, odmiennie poziomy tego ryzyka wydaje się znacznie trafniejsze.

Na krytykę zasługuje też z pewnością wyłączenie z zakresu zastosowania Konwencji Ramowej spraw z zakresu obrony narodowej (*national defence*) przewidziane w art. 4 ust. 3. Słusznie w związku z tym organizacje pozarządowe ostrzegają, że proponowane w projekcie Konwencji Ramowej wyjątki dotyczące bezpieczeństwa narodowego mogą pomóc rządom autorytarnym. Zalecają one w związku z tym, aby w ogóle nie wspominać o bezpieczeństwie narodowym, albo też odnosić się do niego jedynie jako uzasadnionej podstawy ograniczeń praw, która musi być jasno określona przez prawo oraz konieczna i proporcjonalna w społeczeństwie demokratycznym[28].

28 Limitations Related To National Security In CoE Framework Convention on SI CINGO's Position, file:///C:/Users/User/Downloads/CINGO%20CoE%20Nat%20Sec%20Position%20(1).pdf. [dostęp: 10.10.2023].

Oba akty, tj. zarówno Konwencja Ramowa jak i Rozporządzenie UE w sprawie SI, zostały opracowane, aby zapewnić należyte przestrzeganie standardów praw człowieka w dobie szybkiego rozwoju systemów AI. Warto jednak zwrócić uwagę, iż podczas gdy Konwencja nakłada obowiązki na państwa, Rozporządzenie UE w sprawie SI nakłada szczególne obowiązki na osoby fizyczne i prawne. Zwrócić też warto uwagę, iż Konwencja Ramowa wprowadza wymogi dotyczące zagwarantowania prawa do kontroli decyzji podejmowanych przez system sztucznej inteligencji przez człowieka oraz wymóg zapewnienia każdej osobie możliwość interakcji z człowiekiem oprócz systemu sztucznej inteligencji lub zamiast niego. Jest to do pewnego stopnia zbieżne z wymogami dotyczącymi zastosowania SI, które można odnaleźć w orzecznictwie Europejskiego Trybunału Praw Człowieka, o którym mowa jest w dalszej części tego opracowania.

4 Orzecznictwo ETPC związane ze sztuczną inteligencją

Specyfika analizy orzecznictwa strasburskiego związanego z zagrożeniami wynikającymi z rozwoju systemów opartych na sztucznej inteligencji wiąże się przede wszystkim z tym, iż ETPC nie działa z urzędu. Jego proces orzeczniczy inicjowany jest w znakomitej większości wypadków przez skargi indywidualne zarzucające naruszenie praw chronionych w Konwencji. Dodać należy, iż jednym z warunków dopuszczalności skargi indywidulanej do ETPC jest wyczerpanie krajowych środków odwoławczych w związku z zarzutem naruszenia praw chronionych przez EKPC. Po pierwsze zatem, siłą rzeczy orzecznictwo ETPC dotyczące różnych aspektów sztucznej inteligencji pojawia się z pewnym opóźnieniem, co należy wiązać z koniecznością wyczerpania procedury odwoławczej na poziomie krajowym. Po drugie, orzecznictwo to dotyczy poszczególnych skarg zarzucających naruszeniem i nie przedstawia systematycznej analizy naruszeń związanych ze sztuczną inteligencją. Wiąże się to również z tym, iż pomimo znanych potencjalnych zagrożeń, jakie dla poszczególnych praw chronionych Konwencją stwarza zjawisko sztucznej inteligencji, stosunkowo niewiele jest na razie orzeczeń, w których pojawia się wyraźnie wątek naruszenia tych praw w kontekście działania systemów opartych na

sztucznej inteligencji. Poniżej przedstawione zostały wybrane orzeczenia ETPC związane ze zjawiskiem sztucznej inteligencji.

Wśród jednego z najstarszych orzeczeń, które można wiązać z problematyką sztucznej inteligencji wymienić można sprawę S. and Marper v. The United Kingdom, w której chodziło o zarzut postawionych przez dwóch skarżących, iż ich odciski palców praz materiału biologicznego do badań DNA i profili DNA były przetrzymywane przez czas nieokreślony po zakończeniu postępowania karnego[29]. W wyroku ETPC wydanym w tej sprawie stwierdzono naruszenie prawa do prywatności chronionego artykułem 8 Konwencji. W uzasadnieniu zauważono m.in., iż odciski palców, profile DNA i próbki materiału komórkowego należą do kategorii „danych osobowych" w rozumieniu Konwencji w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 r.[30].

Trybunał przypomniał swoje stanowisko wyrażone już uprzednio w sprawie Van der Velden przeciwko Niderlandom (decyzja z dnia 7 grudnia 2006 r., skarga nr 29514/05), że pobieranie i przechowywanie materiału genetycznego stanowi ingerencję w prawo do prywatności. Podkreślił przy tym zasadnicze głównie wynikające płynące z możliwości przyszłego wykorzystania materiału genetycznego, które za sprawą dynamicznego rozwoju techniki może przybrać trudne do przewidzenia formy. ETPC zwrócił również uwagę, że materiał komórkowy zawiera sporo „wrażliwych" informacji, w tym danych na temat zdrowia oraz umożliwiających identyfikację pokrewieństwa. Profile DNA zawierają wprawdzie znacznie mniej informacji na temat osoby niż próbki materiału komórkowego. Jednak automatyczne przetwarzanie profili DNA pozwala nie tylko na „neutralną" identyfikacje osoby, jak argumentował rząd Zjednoczonego Królestwa, lecz na uzyskanie znacznie większej ilości informacji o osobie. Informacje te mogą np. prowadzić do zidentyfikowania powiązań genetycznych pomiędzy osobami. Już sam ten fakt, zdaniem ETPC pozwala na uznanie, że gromadzenia profili DNA za ingerencję w prawo do prywatności. Nie zmienia tego fakt, iż informacja ta jest w formie zakodowanej i może być zrozumiała tylko poprzez użycie technologii komputerowej i jej interpretację jedynie przez wąską grupę specjalistów[31].

29 Zob. wyrok w sprawie S. i Marper przeciwko Zjednoczonemu Królestwu z 4 grudnia 2008 r., skargi nr 30562/04 oraz 30566/04.

30 Ibidem, § 68.

31 Ibidem, § 75.

Dokonując przeglądu regulacji obowiązujących w tym zakresie w Anglii i Walii ETPC wyraził zaniepokojenie ich blankietowym charakterem. Nie różnicowały one przy tym statusu informacji pozyskanych od osób następnie skazanych oraz informacji pochodzących od podejrzanych uniewinnionych w toku dalszego postępowania lub uwolnionych od odpowiedzialności karnej wskutek umorzenia postępowania. Negatywnie oceniono również pobieranie i przechowywanie informacji od każdej osoby podejrzanej, niezależnie od wagi zarzucanych jej czynów czy też jej wieku. Nie przewidziano również maksymalnego okresu przechowywania zgromadzonych informacji. Nadto przewidziano, że osoba w stosunku do osoby uniewinnionej ma jedynie ograniczone możliwości ubiegania się o usunięcie z bazy danych dotyczących jej informacji[32]. W co najmniej dwudziestu państwach przewidziano także możliwość pobierania materiału genetycznego i przechowywania go w krajowych bazach danych lub w innej formie. W większości z tych krajów pobieranie materiału DNC w kontekście postępowania karnego nie ma jednak charakteru systematycznej, lecz jest ograniczone do specyficznych okoliczności lub poważnych przestępstw. Natomiast jedynie w Zjednoczonym Królestwie istnieją regulacje wyraźnie zezwalające na systematyczne i długotrwałe przetrzymywanie profili DNA oraz próbek materiału komórkowego osób, które zostały uniewinnione lub w stosunku do których umorzono postępowanie karne[33]. W konkluzji orzeczenia ETPC uznał, iż blankietowe i nieuwzględniające indywidualnych okoliczności przechowywanie odcisków linii papilarnych, próbek materiału biologicznego oraz profili DNA osób podejrzanych, które później nie zostały skazane za przestępstwo, stanowiło naruszenie zasady proporcjonalności i nie było „konieczne w społeczeństwie demokratycznych" w rozumieniu art. 8 Konwencji[34].

Podobne orzeczenie zapadło w 2020 roku sprawie Gaughran przeciwko Zjednoczonemu Królestwu. Zarzut postawiony w tej sprawie przez skarżącego dotyczył bezterminowego przechowywania jego profilu DNA, odcisków palców i fotografii zgodnie z blankietową polityką przechowywania danych osobowych każdej osoby skazanej za czyn zabroniony, podlegający wpisowi do rejestru, co stanowiło nieproporcjonalną ingerencję w prawo do poszanowania życia prywatnego i rodzinnego, której nie da się uzasadnić[35]. ETPC

32 Ibidem, § 119.
33 Ibidem, §§ 45–47.
34 Ibidem, § 129.
35 Wyrok w sprawie Gaughran przeciwko Zjednoczonemu Królestwu z 13 lutego 2020 r., skarga nr 45245/15.

stwierdził naruszenie art. 8 Konwencji uznając, iż nie została osiągnięta równowaga (*fair balance*) pomiędzy konkurującymi interesami publicznym i prywatnym. Chodziło tu zwłaszcza o nieokreślony charakter kompetencji władz krajowych w zakresie przechowywania profilu DNA, odcisków palców i fotografii skarżącego jako osoby skazanej, nawet po zatarciu skazania, bez uwzględnienia wagi czynu ani potrzeby bezterminowego przechowywania danych, oraz braku jakiejkolwiek realnej możliwości kontroli. Znamienne jest, iż ETPC doszedł do takiego wniosku pomimo uznania, iż państwu przysługuje nieco szerszy margines oceny, jeśli idzie o przetrzymywanie odcisków palców i fotografii.[36]

W sprawie Roman Zakharov przeciwko Rosji skarżący zarzucił, że niejawny system informatyczny SORM Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej do podsłuchiwania rozmów i przechwytywania korespondencji elektronicznej nie spełnia wymogów Artykułu 8 Konwencji[37]. Stwierdzając naruszenie tego postanowienia EKTPC, strasburski Trybunał zauważył m.in., iż „przewidywalność w szczególnym kontekście tajnych środków nadzoru, takich jak przechwytywanie komunikacji, nie może oznaczać, że dana osoba powinna być w stanie przewidzieć, kiedy władze mogą przechwycić jej komunikację, aby mogła odpowiednio dostosować swoje zachowanie. Jednak szczególnie tam, gdzie władza wykonawcza jest sprawowana w tajemnicy, ryzyko arbitralności jest oczywiste. Niezbędne jest zatem posiadanie jasnych, szczegółowych zasad przechwytywania rozmów telefonicznych, zwłaszcza że technologia dostępna do wykorzystania jest coraz bardziej zaawansowana. Prawo krajowe musi być wystarczająco jasne, aby dać obywatelom odpowiednie wskazówki co do okoliczności i warunków, na jakich władze publiczne są uprawnione do zastosowania takich środków”[38]. W tekście wyroku nie pojawiło się wprawdzie określenie „sztuczna inteligencja”, można jednak uznać, iż wzmianka o coraz bardziej zaawansowanej technologii może być odnoszona także do systemów opartych na sztucznej inteligencji.

Stosowanie takich systemów opierać się będzie na dyskrecjonalności władz krajowych. Jednak, jak wynika z orzeczenia w sprawie Zakharov, przepisy prawa powinny wyznaczać zakres takich uprawnień dyskrecjonalnych przyznanych właściwym organom oraz sposób ich wykonywania

36 Ibidem, §§ 96–97.

37 Wyrok w sprawie Roman Zakharov przeciwko Rosji z 4 grudnia 2015 r., skarga nr 47143/06.

38 Ibidem, § 229.

z wystarczającą jasnością, tak aby zapewnić jednostce odpowiednią ochronę przed arbitralną ingerencją[39]. Idzie tu zwłaszcza o określenie charakteru przestępstw, które mogą skutkować wydaniem nakazu przechwytywania; kategorii osób, których telefony mogą być podsłuchiwane; ograniczenie czasu trwania podsłuchu telefonicznego; wprowadzenie procedury, której należy przestrzegać w celu zbadania, wykorzystania i przechowywania uzyskanych danych; określenie środków ostrożności, jakie należy podjąć podczas przekazywania danych innym stronom oraz okoliczności, w których nagrania mogą lub muszą zostać usunięte lub zniszczone[40].

Natomiast w innej sprawie Szabó oraz Vissy przeciwko Węgrom z 12 stycznia 2016 r. ETPC uznał, że węgierska ustawa rozszerzająca inwigilacyjne uprawnienia organów ścigania narusza prawo do poszanowania życia prywatnego i rodzinnego oraz prawo do poszanowania korespondencji[41]. W 2011 r. na Węgrzech powołano specjalną jednostkę antyterrorystyczną, której kompetencje zostały określone w znowelizowanej ustawie o policji. Objęły one uprawnienia do prowadzenia, bez zgody osoby zainteresowanej, niejawnych czynności kontrolnych w tym niejawnego przeszukania mieszkania, podsłuchu wraz z rejestracją dźwięku, kontroli listów i przesyłek, kontroli i zapisywania treści elektronicznych lub skomputeryzowanych. Skarżący, pracownicy organizacji pozarządowej krytycznej wobec polityki aktualnego rządu Węgier, zarzucili, że regulacje te stanowią naruszenie prawa do poszanowania życia prywatnego i rodzinnego oraz korespondencji (art. 8 Konwencji o prawach człowieka). Trybunał zgodził się ze stanowiskiem skarżących i uznał naruszenie art. 8 Konwencji stwierdzając, iż węgierskie regulacje nie dają wystarczająco precyzyjnych, skutecznych i szerokich zabezpieczeń" w przypadku stosowania takich środków[42].

W uzasadnieniu tego orzeczenia znalazł się istotny z punktu widzenia systemów SI fragment. ETPC stwierdził bowiem, iż „jest naturalną konsekwencją form, które przybiera współcześnie terroryzm, iż rządy uciekają się do nowatorskich technologii uprzedzających ewentualne ataki, włączając w to monitorowanie na szeroką skalę rozmów, które mogą zawierać wskazówki odnośnie takich zdarzeń. Technologie stosowanie w ramach takich operacji monitorowania wykazały w ostatnich latach niezwykły

39 Ibidem, § 230.
40 Ibidem, § 231.
41 Zob. wyrok w sprawie Szabó oraz Vissy przeciwko Węgrom z 12 stycznia 2016 r. skarga nr 37138/14.
42 Ibidem § 89.

postęp i osiągnęły takich poziom skomplikowania, który jest trudny do wyobrażenia przez przeciętnego obywatela [...] szczególnie w przypadku, gdy zautomatyzowane i systemowe zbieranie danych jest technicznie możliwe i stosowane jest na szeroką skalę. W obliczu tego postępu Trybunał musi zbadać czy rozwojowi metod inwigilacji, w wyniku stosowania których gromadzone są znaczne ilości danych, towarzyszy równoczesny rozwój prawnych gwarancji zabezpieczających poszanowanie praw chronionych Konwencją"[43].

Dane te często prowadzą do gromadzenia dalszych informacji o warunkach, w jakich powstały podstawowe elementy przechwycone przez władze, takie jak czas i miejsce oraz sprzęt użyty do powstania plików komputerowych, zdjęć cyfrowych, wiadomości elektronicznych i tekstowych i tym podobne. W istocie, byłoby to sprzeczne z celem wysiłków rządu zmierzających do powstrzymania terroryzmu, przywracając w ten sposób zaufanie obywateli do ich zdolności do utrzymania bezpieczeństwa publicznego, gdyby zagrożenie terrorystyczne zostało paradoksalnie zastąpione postrzegalną groźbą nieskrępowanej władzy wykonawczej wkraczającej w sferę prywatną obywateli dzięki niekontrolowanym, ale dalekosiężnym technikom i prerogatywom inwigilacji".[44]

W sprawie Breyer przeciwko Niemcom skarżący zarzucali, iż pewne dane osobowe ich jako użytkowników telefonów na kartę były gromadzone przez operatorów w wykonaniu obowiązku prawnego wynikającego z ustawy telekomunikacyjnej[45]. W tej sprawie ETPC nie dopatrzył się naruszenia praw skarżących chronionych art. 8 oraz 10 EKPC, stwierdzając, iż przechowywani takich danych było proporcjonalnej i dlatego również „konieczne w demokratycznym społeczeństwie[46]. Co ciekawe, zasadnicze pytanie w tej sprawie padło w opinii odrębnej sędziego Ranzoli, który zapytał: „jakie są wymogi na podstawie artykułu 8, szczególnie jeśli chodzi o zabezpieczenia, jak idzie o gromadzenie danych osobowych, które kwalifikowane są jako umiarkowanie ważne, ale mogą być z łatwością uzyskiwane przez wiele różnych organów władzy?[47].

43 Ibidem § 68.

44 Ibidem.

45 Wyrok ETPC w sprawie Breyer przeciwko Niemcom z 30 stycznia 2020 r., skarga nr 50001/12.

46 § 109.

47 Ibidem, opinia odrębnego sędziego Ranzoli, pkt 2. Zwróciła na to uwagę Melinda Szappanos, „Artificial Intelligence: Is the European Court of Human Rights Prepared?" *Acta Humana*, nr 1 (2023): 98.

Sprawa ta również nie dotyczyła bezpośrednio problemu sztucznej inteligencji, jednak problem gromadzenia przez władze ogromnych zbiorów danych osobowych dotyczących obywateli z pewnością stwarza problem w kontekście możliwych zastosowań AI. W konkluzji wspomnianej opinii odrębnej sędzia Ranzoli stwierdził m.in., iż jego zdaniem doszło do naruszenia art. 8 Konwencji z uwagi na brak wystarczających zabezpieczeń, które skutecznie mogłyby zapobiec nadużyciu ogromnych ilości danych osobowych. Ingerencja w prawa chronione na podstawie artykułu 8 nie była proporcjonalna do realizacji celów wymienionych w ustępie 2 tego postanowienia EKPC w szczególności z uwagi na to, że prawo krajowe nie ograniczało się w tym przypadku do środków przeciwko terroryzmowi, lub zwalczaniu innych poważnych przestępstw albo do spraw bezpieczeństwa narodowego, ale wykraczało dlatego poza tego typu cele[48]. Zastanawiające w tej sprawie jest to, dlaczego większość składu orzekającego Trybunału nie zwróciła uwagi na zagrożenie, o których wspomniał sędzia Ranzoli.

W jednym z niewielu orzeczeń, w którym pojawiła się bezpośrednia wzmianka na temat sztucznej inteligencji główny zarzut, który doprowadził do stwierdzenia naruszenia EKPC, dotyczył naruszenia art. 6 EKPC z powodu braku bezstronności jednego z sędziów ze składu orzekającego w postępowaniu krajowym Sądu Najwyższego, a nadto m.in. odmowy dostępu do pełnej dokumentacji sprawy[49]. ETPC stwierdził jedynie naruszenie art. 6 w odniesieniu do braku bezstronności jednego z sędziów sądu krajowego orzekającego w sprawie. W częściowo rozbieżnej opinii sędzia Pavli stwierdził m.in., że większości składu orzekającego „umknęła w tej sprawie okazja do wyważenia skomplikowanych kwestii na pograniczu nowych technologii oraz znacznej ilości materiału dowodowego".[50] W sprawie chodziło bowiem o wykorzystanie przez prokuraturę m.in. danych uzyskanych dzięki zastosowaniu zaawansowanych technologii służących do wyszukiwania. Skarżącym odmówiono jednak dostępu do tego typu narzędzi wyszukiwania co, jak zauważył sędzia Pavli, rodziło problem z punktu widzenia zasady równości broni w toku postępowania[51]. Stwierdził on, iż „ogólne podejście większości składu się wydaje się niewystarczająco adekwatne do złożonego problemu elektronicznego

48 Opinia odrębnego sędziego Ranzoli, pkt 26.

49 Wyrok ETPC w sprawie Sigurđur Einarsson i inni przeciwko Islandii z 4 września 2019 r., skarga nr 39757/15, § 39.

50 Ibidem, częściowo odrębna opinia sędziego Pavli, pkt 4.

51 Ibidem, pkt 10.

dostępu do znacznej ilości danych stanowiących dowód w sprawie karnej (lub np. cywilnej); zastosowania nowoczesnych technologii w tym kontekście oraz ich łącznego wpływu na zasadę równości broni"[52].

Sędzia Pavli zwrócił w tym kontekście uwagę, iż niektóre sądy, tj. irlandzkie oraz brytyjskie, „zatwierdziły w ostatnich latach korzystanie z kontroli sądowej wspomaganej technologią, wykorzystującą formę sztucznej inteligencji znanej jako kodowanie predykcyjne, do celów ujawniania elektronicznego w sprawach cywilnych dotyczących sprawach o wysokiej wartości przedmiotu sporu"[53]. Istotny jest tu adekwatny dostęp stron do tak pozyskanych danych, co nie zostało umożliwione w sprawie Sigurđur Einarsson[54].

5 Wnioski

Zarówno Rozporządzenie UE w sprawie SI, jak i projekt Konwencji Ramowej RE należy ocenić jako akty prawne o charakterze z jednej strony pionierskim, jak idzie regulacje dotyczące sztucznej inteligencji na poziomie ponadnarodowym. Jednocześnie ich zasadnicze znaczenie polega na tym, iż wprowadzają określone gwarancje zabezpieczające prawa jednostki przed zagrożeniami, które mogłyby wynikać dla tych praw w przypadku nieskrępowanego rozwoju technologii opartych na sztucznej inteligencji. Pod względem identyfikacji takich zagrożeń zdecydowanie wyróżnia się omawiane już Rozporządzenie UE w sprawie SI, w którym stosunkowo precyzyjnie określono rodzaje ryzyk wiążących się z rozwojem technologii opartych na sztucznej inteligencji. Konwencja Ramowa wprowadza definicję sztucznej inteligencji nie dokonując jednak rozróżnienia na poszczególne poziomy ryzyka związane z rozwojem SI, tak jak to uczyniono w Rozporządzeniu UE w sprawie SI. Istotną cechą Konwencji Ramowej jest też wprowadzenie licznych obowiązków w odniesieniu do państw-stron dotyczących sztucznej inteligencji, podczas gdy Rozporządzenie UE w sprawie SI nakłada szczególne obowiązki na osoby fizyczne i prawne, w tym w szczególności dostawców (*providers*) technologii opartej na SI.

52 Ibidem.
53 Ibidem, pkt 15.
54 Ibidem, pkt 16–18.

Jak zwrócono wcześniej uwagę, Konwencja Ramowa wprowadza wymogi dotyczące zagwarantowania prawa do kontroli decyzji podejmowanych przez system sztucznej inteligencji przez człowieka oraz wymóg zapewnienia każdej osobie możliwość interakcji z człowiekiem oprócz systemu sztucznej inteligencji lub zamiast niego. Podobne wymogi pojawiają się w orzecznictwie Europejskiego Trybunału Praw Człowieka, o którym mowa jest w ostatniej części tego opracowania.

Przyznać trzeba, iż w dotychczasowym orzecznictwie ETPC znajduje się stosunkowo niewiele wyraźnych i bezpośrednich odniesień do problematyki stosowania systemów opartych na sztucznej inteligencji. Tym niemniej, nie ulega wątpliwości, iż Trybunał dostrzega zagrożenia związane z rozwojem technologii związanych z wykorzystaniem SI, zwłaszcza w sprawach, w których pojawia się problem gromadzenia znacznej ilości danych osobowych obywateli przez władze krajowe. Przede wszystkim, według ETPC, rozwojowi tego typu technologii powinien towarzyszyć równoległy rozwój gwarancji praw chronionych Konwencją skutecznie zabezpieczających przed ich naruszeniem. Wymóg taki wynika zwłaszcza z postanowienia art. 8 EKPC chroniącego prawo do prywatności.

Rozwój zaawansowanych technologii, w tym przede wszystkim tych opartych na sztucznej inteligencji, musi wiązać się, jak to jasno stwierdzono w sprawie Zakharov, z określeniem jasnych i szczegółowych zasad ich stosowania. Oznacza to, że prawo krajowe musi być wystarczająco jasne, aby dać obywatelom odpowiednie wskazówki co do okoliczności i warunków, na jakich władze publiczne są uprawnione do zastosowania takich środków, jak przechwytywanie rozmów czy korespondencji elektronicznej za pomocą zawansowanej, rozwiniętej technologii, zwłaszcza, gdy technologię tę wykorzystują tajne służby bezpieczeństwa. Istotna jest tu rola prawa krajowego, które powinno wyznaczać granice dyskrecjonalności władz krajowych przy stosowaniu rozwiniętych technologicznie systemów, istotnie zagrażających nadmiernym naruszeniem praw jednostki. Istotne wskazówki w tym zakresie wynikają właśnie z orzecznictwa strasburskiego.

Jak wynika jednak ze sprawy Sigurđur Einarsson wykorzystanie systemów opartych na sztucznej inteligencji, m.in. także w sprawach sądowych, zwłaszcza do wyszukiwania danych, rodzi potencjalny problem naruszenia także innych praw, w tym także prawa do rzetelnego procesu sądowego, zwłaszcza w aspekcie równości broni. Okoliczność, że w sprawie Sigurđur Einarsson na ten problem zwrócono uwagę dopiero w opinii częściowo odrębnej sygnalizuje, iż większość składu orzekającego strasburskiego

trybunału musi wykazywać zwiększoną czujność jak idzie o dostrzeganie zagrożeń dla praw chronionych Konwencją wynikających z systemów opartych na sztucznej inteligencji.

Nie ulega wątpliwości, iż omawiane to standardy europejskiej odgrywać będą istotną role w ochronie praw jednostki przed zagrożeniami ze strony dynamicznie rozwijających się technologii opartych na sztucznej inteligencji. Zasadnicze znaczenie będzie miała zatem ich skuteczna implementacja na poziomie krajowym. Co więcej, liczyć należy, iż odegrają one rolę inspirującą jak idzie o rozwój podobnych rozwiązań na poziomie powszechnego prawa międzynarodowego.

Bibliografia

Brattnerg Erik, Raculuca Csernatoni, Venesa Rugova, *Europe and AI: Leading, Lagging Behind, or Carving its Own Way*. Carnegie Endowment for International Peace, Lipiec 2020.

Carriço Gonçalo, „The EU and Artificial Intelligence: A Human-Centered Perspective" *European View* nr 1–8 (2018).

Edwards Liliane, *The EU AI Act: A Summary of its Significance and Scope.* London: Ada Lovelace Institute, 2022. Expert-explainer-The-EU-AI-Act-11-April-2022.pdf.

Szappanos Melinda, „Artificial Intelligence: Is the European Court of Human Rights Prepared?" *Acta Humana*, nr 1 (2023): 93–110.

Świerczyński Marek, Zbigniew Więckowski, *Sztuczna inteligencja w prawie międzynarodowym. Rekomendacje wybranych rozwiązań.* Warszawa: Wydawnictwo Difin, 2021.