PAWEŁ CHYC

Europejskie regulacje prawne dotyczące funkcjonowania sztucznej inteligencji

European Legal Regulations on the Operation of Artificial Intelligence

Abstract

The development of new technologies, especially artificial intelligence, creates enormous opportunities for humanity on the way to further progress and development. Nowadays, no one is surprised by the fact that robots work much more efficiently than humans, and the resources of the Internet are many times greater than human memory. Artificial intelligence will also inevitably enter the everyday life of the modern world, and there is no need to fear that the development of computer intelligence will soon surpass the potential of the human mind. However, already at this stage it is necessary to distinguish digital international law by outlining the ethical and legal framework for the operation of artificial intelligence systems. Without a doubt, such a framework must take into account human rights, data protection, the rule of law, protection of intellectual property, and principles of liability for damage caused by the actions of computer intelligence. The current European achievements (within the Council of Europe and the EU) in the field of regulation of initial standards for the principles of functioning of systems based on artificial intelligence are pioneering on a global scale and for this reason it is worth making a synthetic analysis of them. This is also the aim of this study.

SŁOWA KLUCZOWE: sztuczna inteligencja, cyfrowe prawo międzynarodowe, Rada Europy, Unia Europejska, cyberprzestrzeń, prawo nowych technologii, AI Act

KEYWORDS: artificial intelligence, digital international law, Council of Europe, European Union, cyberspace, new technologies law, AI Act

PAWEŁ CHYC – doktor nauk prawnych, Uniwersytet Pomorski w Słupsku, ORCID – 0000-0002-0900-509X, e-mail: pawel-chyc@wp.pl

HTTPS://DOI.ORG/10.36128/NZBVFZ76

1 Wprowadzenie

Sztuczna inteligencja (SI) stanowi jaskrawy dowód postępu technologicznego współczesnego świata, będąc ważną odsłoną rewolucji 4.0, która opiera się przede wszystkim na technologiach informacyjnych (m.in. internetowa wymiana danych, personalizacja świadczonych usług, optymalizacja przydzielania zasobów, automatyzacja oraz cyfryzacja procesów produkcyjnych i decyzyjnych z wykorzystaniem SI)[1]. Bez wątpienia dynamiczne procesy rozwojowe w tym zakresie wymagają podjęcia działań dostosowujących nie tylko prawo, ale również szeroko rozumiane życie społeczno-gospodarcze do nowej rzeczywistości, kreowanej coraz częściej w przestrzeni cyfrowej. Pilnych analiz wymagają nie tylko umowy zawierane z wykorzystaniem SI, ale także odpowiedzialność za szkody spowodowane przez SI, jak również takie wytwory jak zdjęcia, ludzki głos bądź słowo pisane kreowane przez algorytmy. Nowego podejścia wymaga również kształtowanie etyki, a także świadomości oraz postaw społecznych względem nowych technologii. W obliczu tych zjawisk wspomniane działania dostosowujące powinny być podejmowane niezwłocznie i to zarówno na poziomie krajowym, jak i regionalnym oraz międzynarodowym[2].

Obecnie systemy oparte na SI w większości wciąż operują w jurysdykcjach, które tylko częściowo bądź w ogóle nie regulują zagadnień związanych z wykorzystaniem nowych technologii. Systemy SI ponadto z dużą swobodą przemieszczają się wśród różnych jurysdykcji (sieć transnarodowa), a niekiedy funkcjonują wręcz w obszarach eksterytorialnych, poza jakąkolwiek jurysdykcją państw. Wprawdzie na płaszczyźnie międzynarodowej podejmowane są pozarządowe wysiłki mające na celu nakreślenie choćby ram etycznych działania SI[3], to jednak rozwiązania krajowe wydają się dominować w tym zakresie. Niesie to ze sobą ryzyko fragmentarycznych i partykularnych rozwiązań w odniesieniu do SI[4],

1 Klaus Schwab, *Czwarta rewolucja przemysłowa*, tłum. Anna Dorota Kamińska (Warszawa: Studio Emka, 2018), 23. Por. Waldemar Furmanek, „Najważniejsze idee czwartej rewolucji przemysłowej «Industrie 4.0»" *Dydaktyka Informatyki,* nr 13 (2018): 56-57.

2 Marek Świerczyński, Zbigniew Więckowski, *Sztuczna inteligencja w prawie międzynarodowym. Rekomendacje wybranych rozwiązań* (Warszawa: Difin, 2021), 17.

3 Zob. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics. https://futureoflife.org/open-letter/ai-principles/. [dostęp: 18.3.2025].

4 Por. Adam Wiśniewski, „Sztuczna inteligencja i prawa człowieka w kontekście prawa międzynarodowego" *Prawo i Więź*, nr 4 (2023): 33 ; Paweł Księżak, "Sztuczna inteligencja jako wychowawca, opiekun i reprezentant: w poszukiwaniu

definicji rodziny" *Prawo i Więź* nr 3 (2023): 289-298; Piotr Burczaniuk, „Tworzenie prawa sztucznej inteligencji – wyzwania i perspektywy" *Prawo i Więź* nr 3 (2024): 283-300; Magdalena Dziedzic, „Przeciwdziałanie dezinformacji w kontekście wybranych regulacji Aktu o usługach cyfrowych oraz Aktu o Sztucznej Inteligencji" *Prawo i Więź* nr 6 (2024): 223-238; Bogdan Fischer, Marlena Sakowska-Baryła, „Wykorzystywanie otwartych danych jako element zwiększenia wyjaśnialności AI" *Prawo i Więź* nr 6 (2024): 289-305; Zbigniew Więckowski, Marek Świerczyński, „Analiza ryzyka dokonywana na podstawie konwencji ramowej Rady Europy o sztucznej inteligencji na przykładzie zastosowań w sektorze prawnym" *Prawo i Więź* nr 1 (2025): 409-428; Katarzyna Jasińska, „Trenowanie sztucznej inteligencji a naruszenie praw autorskich. Aspekty dowodowe" *Prawo i Więź* nr 1 (2025): 419-434; Katarzyna Jasińska, „Problematyka oznaczania wytworów generatywnej sztucznej inteligencji w świetle polskiej ustawy o zwalczaniu nieuczciwej konkurencji" *Prawo i Więź* nr 1 (2025): 529-544; Zbigniew Więckowski, Grzegorz Kubalski, „Czy sztuczna inteligencja oraz inne technologie informatyczne pomogą w dostępie do wymiaru sprawiedliwości osobom ze szczególnymi potrzebami?" *Prawo i Więź* nr 4 (2022): 146-165; Oliwia Królikiewicz, „Od niewolnika po elektroniczną osobę prawną, czyli rozważania na temat podmiotowości prawnej dla AI" *Prawo i Więź* nr 5 (2025): 653-670; Iga Bałos, „Wpływ generatywnej sztucznej inteligencji na ocenę nowości wynalazku" *Prawo i Więź* nr 1 (2025): 545-563; Iga Bałos, „Konsekwencje braku kompleksowego modelu ochrony wizerunku i innych dóbr niematerialnych aktorów w kontekście stosowania narzędzi sztucznej inteligencji" *Prawo i Więź* nr 4 (2023): 383-397; Kamil Szpyt, Artur Bilski, „Wybrane wyzwania prawne i organizacyjne związane z wdrażaniem systemów AI w działalności samorządów terytorialnych" *Prawo i Więź* nr 1 (2025): 565-596; Michał Kowalski, „Wpływ technologii na konstrukcję uzasadnień orzeczeń sądów administracyjnych" *Prawo i Więź* nr 4 (2023): 265-279; Michał Kowalski, „The Impact of Artificial Intelligence on the Future Functioning of Administrative Courts" *Prawo i Więź* nr 6 (2024): 173-185; Michał Kowalski, „Sztuczna inteligencja a usprawnienie postępowania przed sądami administracyjnymi. Kilka refleksji na tle doświadczeń wybranych systemów prawnych" *Prawo i Więź* nr 1 (2025): 429-442; Michał Kalinowski, „Czy, komu i w jakim zakresie przysługują prawa do wytworów generatywnej sztucznej inteligencji? Analiza prawna z perspektywy warunków użytkowania MidJourney" *Prawo i Więź* nr 1 (2024): 259-280; Tomasz Szanciło, Beata Stępień-Załucka, „Sędzia robotem a robot sędzią w postępowaniu cywilnym w ujęciu konstytucyjnym i procesowym" *Prawo i Więź* nr 4 (2023): 217-247; Marcin Górski, „Treści generowane przez sztuczną inteligencję a ochrona różnorodności form wyrazu kulturowego" *Prawo i Więź* nr 4 (2023): 335-353; Agnieszka Ogrodnik-Kalita, „Wierność w czasach cyfrowej zarazy, czyli o prawach i obowiązkach małżeńskichw dobie sztucznej inteligencji i nowych technologii" *Prawo i Więź* nr 4 (2023): 399-418; Iwona Bień-Węgłowska, „Deepfake w świetle aktu w sprawie sztucznej inteligencji" *Prawo i Więź* nr 5 (2025): 151-169; Marcin Kamiński, „Akt administracyjny zautomatyzowany. Zasadnicze problemy konstrukcyjne zastosowania systemów sztucznej inteligencji w procesach decyzyjnych postępowania administracyjnego na tle prawnoporównawczym" *Prawo i Więź* nr 4 (2023): 281-304; Marcin Kamiński, „Podmiot kompetencji administracyjnej w zautomatyzowanych procesach stosowania prawa na tle

co w obliczu globalnego zasięgu algorytmów, które z niezwykłą swobodą przekraczają granice państwowe, skłania do refleksji nad opracowaniem spójnej rekonstrukcji prawa międzynarodowego celem stworzenia *sui generis* subsystemu międzynarodowego prawa nowych technologii/cyfrowego prawa międzynarodowego powiązanego z cyberprzestrzenią, co jest główną tezą niniejszego artykułu[5].

W takim ujęciu pojawiają się w piśmiennictwie głosy, o potrzebie stworzenia cyfrowego prawa międzynarodowego, regulującego w cyfrowej przestrzeni zachowania ludzkie. Wskazuje się wręcz o możliwości uznania przestrzeni cyfrowej za wspólne dziedzictwo ludzkości, a z drugiej strony widoczne są tendencje do sprawowania suwerenności państwowej nad cyberprzestrzenią, co stanowi zły prognostyk dla uznania jej niezawłaszczalności. Bez wątpienia pilnych działań prawa międzynarodowego wymagają takie kluczowe obszary jak terroryzm i przestępczość cyfrowa, a także ochrona infrastruktury krytycznej. Elementem uzasadniającym wyodrębnienie cyfrowego prawa międzynarodowego jest również nieadekwatność klasycznych koncepcji terytorium oraz suwerenności powiązanych z przestrzenią fizyczną, w zestawieniu z przestrzenią cyfrową o charakterze transnarodowym[6]. W doktrynie można zauważyć coraz śmielszą dyskusję nad tą problematyką, nierzadko wzbogaconą o ciekawe

problematyki legitymacji prawno-demokratycznej delegowania kompetencji na systemy sztucznej inteligencji i odpowiedzialności prawnej za ich działania lub zaniechania" *Prawo i Więź* nr 6 (2024): 239-263; Marek Świerczyński, Zbigniew Więckowski, „Intellectual Property and Artificial Intelligence – Selected Issue" *Prawo i Więź* nr 3 (2022): 179-202; Iwona Gredka-Ligarska, „In Search of Adequate Principles for AI Civil Liability" *Prawo i Więź* nr 3 (2024): 157-190; Jan Olszewski, „Wybrane problemy prawa Piaskownic Regulacyjnych we wspieraniu działalności gospodarczej" *Prawo i Więź* nr 3 (2024): 61-91; Mohammad Bitar, Ahmad Khalil, S. Anandha Krishna Raj, Rupal Malik, „Legal Assessment of Bias and Discrimination of AI Tools in Higher Education and Research" *Prawo i Więź* nr 3 (2025): 9-37; Julia Bernacka, „Problematyka prawna technologii deepfake – analiza legalności tworzenia i rozpowszechniania deepfake'ów po uchwaleniu AI Act" *Prawo i Więź* nr 5 (2025): 671-694; Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, „Artificial Intelligence in e-Administration" *Prawo i Więź* nr 1 (2025): 383-407.

5 Szerzej o postulacie wyodrębnienia cyfrowego prawa międzynarodowego: Zob. Cezary Mik, *Państwo i prawo wobec procesów internacjonalizacji, integracji i globalizacji*, t. II, *Wpływ globalizacji na klasyczny paradygmat państwa i prawa. W cieniu pandemii SARS-COVID 19* (Toruń: TNOiK, 2022), 543 i n.

6 Zob. Mik, *Państwo i prawo wobec procesów internacjonalizacji, integracji i* globalizacji, 545-546. Autor w tej wybitnej publikacji prezentuje analizę światowej literatury w zakresie cyberprzestrzeni oraz pogłębione refleksje dotyczące m.in. cyfrowego prawa międzynarodowego.

pomysły, do których zaliczyć można postulat stworzenia Międzynarodowej Rady ds. Internetu[7].

Jak już wspomniano na płaszczyźnie międzynarodowej podejmowane są próby unifikacji prawa przestrzeni cyfrowej (gównie dotyczące SI), mające na celu stworzenie właściwych ram i zasad dotyczących etyki, jak również likwidacji potencjalnych szkód powstałych wskutek działania SI. Warto wskazać, iż wybrane normy prawa międzynarodowego publicznego już obecnie nadają się do bezpośredniego uwzględnienia w procesie projektowania algorytmów SI oraz powinny być uwzględniane dla oceny jej funkcjonowania. Do tych norm prawa międzynarodowego zaliczyć należy przede wszystkim prawa człowieka, prawo ochrony danych osobowych, prawo własności intelektualnej oraz prawo ochrony konsumentów[8]. Wciąż brakuje jednak regulacji międzynarodowych i ponadnarodowych dotyczących odpowiedzialności za szkodę spowodowaną działaniem SI. Całościowe i spójne ramy określające zasady funkcjonowania SI (w tym jasne zasady odpowiedzialności) na poziomie prawa międzynarodowego z pewnością zbudują solidne zaufanie dla sztucznej inteligencji, co tym samym pozytywnie wpłynie na jej dalszy zrównoważony rozwój[9]. Bez wątpienia jednak dynamika rozwoju SI wymaga stworzenia autonomicznego reżimu prawnego na poziomie międzynarodowym oraz regionalnym.

Co warte podkreślenia dotychczasowy dorobek regulacyjny w zakresie sztucznej inteligencji wskazuje, iż Europa ma ambicje stać się światowym liderem w zakresie tworzenia ponadnarodowych regulacji dotyczących sztucznej inteligencji, akcentując wartości etyczne oraz ochronę praw człowieka w tym zakresie. Z tego względu niniejszy artykuł odnosi się przede wszystkim do dwóch europejskich aktów w postaci Konwencji ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności[10] oraz Rozporządzenia UE w sprawie sztucznej inteligencji[11], które – pomijając partykularne rozwiązania krajowe – są przykładem

---

7 Joanna Kulesza, *Międzynarodowe prawo Internetu* (Poznań: Ars boni et aequi, 2010), 305 i n.

8 Świerczyński, Więckowski, *Sztuczna inteligencja w prawie międzynarodowym*, 10-11.

9 Ibidem, 12.

10 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series – No. 225, Vilnius, 5.IX.2024. https://rm.coe.int/1680afae3c. [dostęp: 25.3.2025].

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów

pierwszych w świecie wiążących porozumień w sferze AI o charakterze międzynarodowym.

2 Europejskie porozumienia ponadnarodowe w dziedzinie SI

W perspektywie regionalnej znaczące działania w zakresie projektowania prawnych rozwiązań problematyki stosowania sztucznej inteligencji podjęły Rada Europy oraz Unia Europejska. Obie te organizacje od lat akcentują idee praworządności oraz praw człowieka, mając doniosły dorobek legislacyjny w tym zakresie i obie organizacje ściśle współpracują ze sobą w celu osiągnięcia przez Europę pozycji światowego lidera w zakresie rozwoju bezpiecznej i etycznej sztucznej inteligencji[12]. Nie może więc zaskakiwać fakt, iż jako pierwsze regionalne organizacje dostrzegły konieczność stworzenia ponadnarodowych mechanizmów mających na celu wprowadzenie wyjściowych standardów dla zasad działania systemów opartych na SI, jako grupie technologii z jednej strony rozwijającej się niezwykle dynamicznie i niosącej ze sobą perspektywę skokowego rozwoju gospodarczego, a z drugiej strony niosących obawy o zachowanie właściwych standardów etycznych powiązanych z podstawowymi wolnościami i prawami człowieka.

Rada Europy w roku 2024 przyjęła na nieformalnej konferencji ministrów sprawiedliwości Rady Europy w Wilnie Konwencję ramową Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności[13]. Konwencja ta jest pierwszą w historii wiążącą umową międzynarodową dotyczącą sztucznej inteligencji i potwierdza znaczenie istniejących

dotyczących sztucznej inteligencji: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689. [dostęp: 23.3.2025].

12 Rada Europejska, Nadzwyczajne posiedzenie Rady Europejskiej (1 i 2 października 2020 r.) – Konkluzje, EUCO 13/20, 2020, 6. Dowodem współpracy UE oraz Rady Europy jest bez wątpienia fakt podpisania w dniu 5 września 2024 r. przez Wiceprzewodniczącą Komisji Europejskiej do spraw wartości i przejrzystości Věrę Jourovą w imieniu Unii Europejskiej Konwencji Ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności.

13 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series – No. 225, Vilnius, 5.IX.2024. https://rm.coe.int/1680afae3c. [dostęp: 25.3.2025].

zobowiązań międzynarodowych dotyczących praw człowieka w kontekście użytkowania nowych technologii. Konwencja odnosi się również m.in. do ochrony danych osobowych, zarządzania ryzykiem, właściwych zabezpieczeń proceduralnych oraz społecznej edukacji cyfrowej[14]. Jeszcze przed jej podpisaniem wskazywano, że potencjał tej Konwencji – w odróżnieniu od ustawodawstwa UE w zakresie SI – może wykraczać poza kraje europejskie, co pozwoliłoby jej uzyskać globalne oddziaływanie[15]. I w istocie – co warte podkreślenia – według stanu na dzień 1 marca 2025 r. do konwencji przystąpiły nie tylko sama Unia Europejska oraz kraje europejskie spoza UE[16], ale także państwa spoza Europy, takie jak Kanada, Izrael, Japonia oraz Stany Zjednoczone[17].

Istotą Konwencji ramowej Rady Europy dotyczącej sztucznej inteligencji jest zatem określenie podstawowych (ramowych) zasad dotyczących projektowania, wdrażania i użytkowania systemów SI w sposób odpowiedzialny, przejrzysty oraz zgodny z obowiązującym porządkiem prawnym – przede wszystkim w ramach UE[18]. Jej istota koncentruje się na:

- zapewnieniu zgodności z prawami człowieka: każda technologia SI powinna respektować prawa jednostki, w tym prawo do prywatności,

14 Zob. art. 11, 15, 16 oraz 20 Konwencji ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności.

15 Gibson Dunn, *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law* (Washington: Gibson, Dunn & Crutcher LLP, 2024), 1. Zob. https://www.gibsondunn.com/wp-content/uploads/2024/06/council-of-europe-framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-rule-of-law.pdf. [dostęp: 26.03.2025].

16 Konwencję podpisały również państwa europejskie nienależące do UE: Wielka Brytania, Gruzja, Islandia, Mołdawia, Czarnogóra oraz Norwegia. Zob. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225. [dostęp: 25.3.2025].

17 https://www.state.gov/bureau-of-democracy-human-rights-and-labor/the-council-of-europes-framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-the-rule-of-law. [dostęp: 25.3.2025].

18 Konwencja jest w pełni zgodna z rozporządzeniem UE w sprawie sztucznej inteligencji (AI Act – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji), pierwszym kompleksowym rozporządzeniem UE w sprawie sztucznej inteligencji. Zob. https://digital-strategy.ec.europa.eu/pl/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights. [dostęp: 25.3.2025].

wolność słowa, ochronę przed dyskryminacją oraz prawo do sprawiedliwego procesu;
- ochronie demokracji: konwencja kładzie nacisk na przeciwdziałanie zagrożeniom wynikającym z automatyzacji procesów decyzyjnych w sferze publicznej oraz manipulacji informacjami w przestrzeni politycznej.
- wzmacnianiu praworządności: zapewnia mechanizmy nadzoru nad wykorzystaniem SI w administracji publicznej oraz wymiarze sprawiedliwości w taki sposób, aby nie naruszało to zasady równości wobec prawa i dostępu do niezależnego sądu.

Pomimo, iż Konwencja ramowa Rady Europy dotycząca sztucznej inteligencji ma charakter ogólny i jedynie wprowadzający rozwiązania partykularne[19], to pełni ona wieloaspektowe funkcje w zakresie regulacji sztucznej inteligencji, w szczególności poprzez:

1. Normatywną funkcję ochronną – ustanawia minimalne standardy ochrony praw człowieka w kontekście SI, w tym mechanizmy oceny ryzyka oraz odpowiedzialności za decyzje podejmowane przez systemy SI;
2. Koordynacyjną funkcję regulacyjną – służy jako wspólna podstawa dla państw-stron w zakresie harmonizacji przepisów dotyczących SI oraz ujednolicenia podejścia do jej nadzoru i kontroli;
3. Funkcję prewencyjną – zobowiązuje państwa do wdrażania środków zapobiegających negatywnym skutkom wynikającym z niekontrolowanego rozwoju i stosowania SI, np. poprzez obowiązek przeprowadzania ocen wpływu na prawa człowieka;
4. Funkcję współpracy międzynarodowej – tworzy ramy dla współpracy między państwami, organizacjami międzynarodowymi oraz podmiotami prywatnymi w zakresie odpowiedzialnego rozwoju SI[20].

19 Preambuła Konwencji ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności wskazuje, iż „[...] Recognising the framework character of this Convention, which may be supplemented by further instruments to address specific issues relating to the activities within the lifecycle of artificial intelligence systems [...]".

20 Preambuła Konwencji ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności – https://rm.coe.int/1680afae3c. [dostęp: 26.3.2025].

Jak już wspomniano, Konwencja Rady Europy dotycząca sztucznej inteligencji, mając charakter ramowy wymaga podjęcia środków implementacyjnych i wykonawczych na poziomie międzynarodowym, jak również działań dostosowujących i harmonizujących prawne systemy krajowe w zakresie ochrony praw człowieka, danych osobowych, własności intelektualnej, nadzoru nad algorytmami oraz odpowiedzialności prawnej za decyzje podejmowane przez systemy SI w całym cyklu jej życia[21]. W celu wdrażania postanowień konwencyjnych przez strony, Konwencja ustanawia mechanizm monitorowania i nadzoru oraz procedury egzekwowania zgodności z jej postanowieniami oraz obowiązek raportowania o wpływie SI na prawa obywateli i przewiduje współpracę międzynarodową w tym zakresie (art. 1 ust. 3 oraz art. 25 Konwencji). Z drugiej strony Konwencja w odniesieniu do działalności badawczo-rozwojowej w zakresie opracowywania algorytmów SI wyłącza znaczącą część swoich postanowień po to, by nie spowalniać prac rozwojowych nad systemami jeszcze nieudostępnionymi dla odbiorców, z wyłączeniem sytuacji zagrażającym naruszeniom praw człowieka, wartościom demokratycznym oraz praworządności (art. 3 ust. 3 Konwencji).

Konwencja ramowa Rady Europy o sztucznej inteligencji stanowi bez wątpienia ważny krok w kierunku uregulowania wpływu SI na relacje społeczno-gospodarcze w wymiarze międzynarodowym. Jej przyjęcie i implementacja przez państwa również spoza Europy ma na celu zapewnienie, że światowy rozwój technologii SI będzie odbywał się w sposób zrównoważony, a zatem zgodny z wartościami demokratycznymi i zasadami praworządności, eliminując jednocześnie ryzyko nadużyć i naruszeń praw człowieka, a z drugiej strony zapewniona zostanie dotychczasowa dynamika innowacji w zakresie sztucznej inteligencji oraz zaufanie społeczne do nowych technologii. Konwencja ta obejmuje ponadto kluczowe zagadnienia regulowane również przez unijne Rozporządzenie w sprawie sztucznej inteligencji (AI Act). Zakres regulacji obu tych aktów pokrywa się w zakresie m.in. zgodności SI z prawami człowieka, analizie ryzyka

21 Zob. art. 1 ust. 2 Konwencji ramowej Rady Europy o sztucznej inteligencji i prawach człowieka, demokracji i praworządności: „Each Party shall adopt or maintain appropriate legislative, administrative or other measures to give effect to the provisions set out in this Convention. These measures shall be graduated and differentiated as may be necessary in view of the severity and probability of the occurrence of adverse impacts on human rights, democracy and the rule of law throughout the lifecycle of artificial intelligence systems. This may include specific or horizontal measures that apply irrespective of the type of technology used".

związanego ze stosowaniem SI, uwzględnianiem ochrony danych oraz zasad bezpieczeństwa cyfrowego, przejrzystości treści generowanych przez SI, czy wprowadzaniem mechanizmów nadzoru nad algorytmami SI[22].

W tym miejscu warto również wspomnieć o wcześniejszej konwencji Rady Europy, jaką jest Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych przyjęta w 1981 roku (Konwencja nr 108)[23], która dość wyraźnie koresponduje ze współczesnym rozwojem SI. Konwencja ta jest pierwszym międzynarodowym traktatem prawnie wiążącym w zakresie ochrony danych osobowych. W odpowiedzi na dynamiczne zmiany technologiczne i społeczne w 2018 roku przyjęto jej zaktualizowaną wersję – tzw. Konwencję 108+ (Protokół zmieniający Konwencję nr 108). Konwencja 108+ wprowadza nowoczesne ramy ochrony danych osobowych, dostosowane do wyzwań XXI wieku, w tym do rosnącego znaczenia sztucznej inteligencji, big data, chmury obliczeniowej i automatyzacji procesów decyzyjnych. Zawarte w niej przepisy wzmacniają standardy ochrony prywatności oraz zwiększają przejrzystość przetwarzania danych osobowych, co ma szczególne znaczenie w kontekście SI, gdzie dane stają się kluczowym zasobem determinującym jakość i bezpieczeństwo algorytmów. Konwencja ta wprowadza m.in. zasadę proporcjonalności i minimalizacji danych (art. 10-11) oraz zakaz dyskryminacji oraz ochronę praw człowieka (art.1).

Konwencja 108+ wprowadza mechanizmy odpowiedzialności i rozliczalności, co ma kluczowe znaczenie w procesie projektowania i wdrażania systemów SI przez podmioty publiczne i prywatne. W odróżnieniu od RODO, Konwencja 108+ ma charakter globalny, jej stronami mogą być nie tylko państwa członkowskie Rady Europy, ale również państwa trzecie. Umożliwia to stworzenie wspólnego, uniwersalnego standardu ochrony danych, co jest niezbędne w obliczu globalnego charakteru systemów SI. Konwencja 108+ może pełnić funkcję fundamentu etycznego i prawnego pod rozwój regulacji dotyczących sztucznej inteligencji. Jej normy, choć ogólne, dają się adaptować do realiów technologicznych, stanowiąc punkt wyjścia dla bardziej szczegółowych regulacji sektorowych i branżowych (np. unijnego AI Act). W tym sensie, Konwencja 108+ pozostaje nie tylko aktem ochrony

22 Zob. https://digital-strategy.ec.europa.eu/pl/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights. [dostęp: 30.3.2025].

23 Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. – Dz.U. z 2003 r., nr 3 poz. 25.

danych, ale także instrumentem kształtującym odpowiedzialne i zgodne z prawami człowieka podejście do rozwoju SI[24].

Co ciekawe, jedno z pierwszych orzeczeń Europejskiego Trybunału Praw Człowieka w Strasburgu pośrednio dotyczące stosowania sztucznej inteligencji[25] uwzględnia właśnie wspomnianą Konwencję nr 108. Orzeczenie to dotyczyło sprawy Marper przeciwko Zjednoczonemu Królestwu[26], a istotą sprawy był zarzut skarżących dotyczący bezterminowego przetrzymywania przez brytyjskie organy ścigania odcisków palców oraz materiału DNA po zakończeniu postępowania karnego. W uzasadnieniu orzeczenia sędziowie ETPC wskazali, że taki stan rzeczy naruszał art. 8 EKPC dotyczący prawa do poszanowania swojego życia prywatnego i rodzinnego, jak również Konwencję nr 108 z uwagi na fakt, iż profile DNA oraz odciski palców należą do wrażliwych danych osobowych, których dotyczy wspomniana konwencja. W orzeczeniu wskazano, że „dynamiczny rozwój techniki"[27] w przyszłości może prowadzić do trudnych do przewidzenia nadużyć.

W chwili obecnej znaczący dorobek kodyfikacyjny w zakresie regulacji nowych technologii posiada również Unia Europejska, która w maju 2024 roku przyjęła Akt w sprawie sztucznej inteligencji[28] (dalej: AI Act). Jest to pierwszy akt prawa ponadnarodowego regulujący rozwój, wdrażanie i użytkowanie systemów sztucznej inteligencji w Unii Europejskiej[29]. Akt ten został okrzyknięty przełomowym nie tylko dlatego, że naówczas na świecie nie wprowadzono jeszcze podobnych regulacji, ale także dlatego, że jako pierwszy klasyfikuje sztuczną inteligencję pod kątem potencjalnego ryzyka dla użytkowników, w myśl zasady, że im większe szkody może

---

24 Szerzej: Kimpian, „Rights to Privacy and to Personal Data Protection and Convention 108", 19-28.

25 Należy zaznaczyć, iż do chwili obecnej (maj 2025 r.) ETPC w Strasburgu wydał stosunkowo niewiele orzeczeń bezpośrednio odnoszących się do sztucznej inteligencji.

26 Wyrok EPTC z dnia 4 grudnia 2008 r. w sprawie S. i Marper vs. Zjednoczone Królestwo, nr skargi: 30562/04 i 30566/044.

27 Sformułowanie to można odnieść do rozwoju sztucznej inteligencji wykorzystywanej współcześnie przez organy ścigania. Zob. pkt 68 wyroku w sprawie S. i Marper vs. Zjednoczone Królestwo.

28 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689. [dostęp: 23.3.2025].

29 Świerczyński, Więckowski, Sztuczna inteligencja w prawie międzynarodowym, 31. Por. Wiśniewski, „Sztuczna inteligencja i prawa człowieka", 32.

wyrządzić sztuczna inteligencja, tym surowsze będą przepisy regulujące jej użycie[30]. Główny rdzeń AI Act klasyfikuje zagrożenia związane ze stosowaniem SI, w ramach których określono różne poziomy ryzyka związanego z aplikacjami SI oraz odpowiednie środki regulacyjne. Jak wskazuje uzasadnienie do AI Act[31], w rozporządzeniu tym zastosowano kategorie ryzyka w oparciu o analizę zakazanych praktyk odnośnie algorytmów sztucznej inteligencji, wprowadzając kategorie w odniesieniu do SI, które stwarzają:

1. niedopuszczalne ryzyko obejmujące technologie uznane za zagrożenie dla praw podstawowych, np. systemy oceny obywateli (*social scoring*) lub techniki SI znajdujące się poza świadomością danej osoby, mające na celu istotne zniekształcenie zachowań ludzkich. Są one zakazane (art. 5 AI Act);
2. wysokie ryzyko – dotyczy to SI stosowanej w krytycznych obszarach, takich jak infrastruktura, edukacja, zatrudnienie, sądownictwo czy biometria. Wymagają one rygorystycznych ocen zgodności (art. 6-27 AI Act);
3. niskie (ograniczone) ryzyko – obejmuje np. chatboty i systemy rekomendacji, które podlegają wymogom przejrzystości;
4. minimalne ryzyko – takim statusem objęta będzie większość aplikacji SI, np. filtry antyspamowe, niepodlegające szczególnym regulacjom. Takie systemy są dopuszczane do użytku bez ograniczeń.

Zgodnie z art. 1 ust. 2 lit. c Rozporządzenia UE ws. sztucznej inteligencji ustanawia się szczególne wymogi związane z algorytmami SI wysokiego ryzyka, jak również obowiązki operatorów takich systemów, przy czym rozporządzenie stosując określenie „operator" obejmuje nim dostawcę systemu, producenta systemu, podmiot stosujący, upoważnionego przedstawiciela,

30 Adam Wiśniewski, „Wokanda europejska – ETPC", [w:] *Przedwiośnie ery sztucznej inteligencji. Technologia-zarządzanie-prawo*, t. I, red. Edmund Wittbrodt, Zdzisław Brodecki, Marta Dargas-Draganik (Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego, 2024), 280.

31 Uzasadnienie do Rozporządzenie Parlamentu Europejskiego i Rady (COM/2021/206 final) ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze unii, s. 15. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0012.02/DOC_1&format=PDF. [dostęp: 25.3.2025].

importera lub dystrybutora[32]. AI Act koncentruje się zatem na systemach SI, których wykorzystywanie uznaje się za niedopuszczalne ze względu na ich sprzeczność z wartościami UE, w tym prawa człowieka, ochronę danych osobowych, prawa konsumentów, bądź wprowadzanie przez administrację publiczną zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej[33] oraz oceny punktowej ludności (tzw. *social scoring*)[34].

Rozporządzenie to dotyka przede wszystkim sposobu, w jaki SI jest wykorzystywana pod kątem praw podstawowych obywateli UE, a przez to zapewnienia zaufania społecznego do systemów SI oraz finalnie stworzenia jednolitego rynku dla rozwiązań opartych na sztucznej inteligencji. Jednocześnie stawia wyzwania dla sektora technologicznego, szczególnie w zakresie zgodności i odpowiedzialności za algorytmy[35]. AI Act jest rezultatem kilkuletnich inicjatyw podejmowanych przez Unię Europejską w zakresie nakreślenia ram funkcjonowania nowych technologii (np. Biała Księga w sprawie sztucznej inteligencji wydana przez Komisję Europejską w 2020 r.[36]). Rozbudowane uzasadnienie dla projektu AI Act[37] wskazuje m.in. na przyczyny i cele tego rozporządzenia, spójność z politykami i strategiami UE, traktatową podstawę prawną (przede wszystkim art. 114 ust.1 TfUE[38]), a także zasady UE dotyczące pomocniczości i proporcjonalności

32 Art. 3 pkt 8 AI Act.

33 Pkt 30-39 Preambuły do AI Act.

34 Paweł Tomaszewski, „Inteligentne kontrakty jako narzędzie regulacji sztucznej inteligencji", [w:] *Prawo w erze sztucznej inteligencji. Cyfryzacja i autonomizacja życia publicznego*, red. Zdzisław Brodecki, Marta Nowicka (Gdynia-Pelplin: Bernardinum, 2022), 196.

35 Por. https://digital-strategy.ec.europa.eu/pl/policies/regulatory-framework-ai. [dostęp: 30.3.2025].

36 Zob. Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania – Bruksela, dnia 19.2.2020 r. COM(2020) 65 final. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0065. [dostęp: 31.3.2025]. Por. Paweł Chyc, „Załączniki – Materiał źródłowy" w *Świątynia w kosmicznej wiosce. Bezpieczeństwo przyszłych pokoleń w erze sztucznej inteligencji*, red. Zdzisław Brodecki (Warszawa: EuroPrawo, 2021), 171-72.

37 Uzasadnienie do Rozporządzenie Parlamentu Europejskiego i Rady (COM/2021/206 final) ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0012.02/DOC_1&format=PDF. [dostęp: 25.3.2025].

38 Traktat o funkcjonowaniu Unii Europejskiej, Dziennik Urzędowy Unii Europejskiej C 326/49, art. 114 ust. 1: „[...] Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą i po konsultacji z Komitetem

w odniesieniu do zastosowanych mechanizmów prawnych oraz wyniki ocen i konsultacji z zainteresowanymi stronami.

Z kolei preambuła AI Act[39] wskazuje, że jednym z głównych celów tego rozporządzenia jest zapewnienie transgranicznej swobody przepływu towarów i usług wykorzystujących sztuczną inteligencję, która powinna być zorientowana na zapewnienie wysokiego poziomu ochrony bezpieczeństwa, praworządności, środowiska oraz praw podstawowych ujętych w Karcie Praw Podstawowych Unii Europejskiej, przy czym zabronione jest nakładanie ograniczeń na wykorzystywanie i rozwój algorytmów SI. W tym celu niezbędne jest ustanowienie jednolitych obowiązków dla operatorów i zagwarantowanie jednolitej ochrony interesu publicznego, m.in. w zakresie ochrony danych osobowych, np. w kontekście zdalnej identyfikacji biometrycznej. Preambuła wskazuje również na zagrożenia związane z wykorzystywaniem nowych technologii dla podstawowych praw człowieka oraz interesu publicznego, wskazując na potencjalne szkody fizyczne, psychiczne, społeczne oraz ekonomiczne spowodowane przez sztuczną inteligencję i rekomendując zarazem cel dla twórców algorytmów SI, jakim powinien zawsze być zwiększanie dobrostanu człowieka[40].

Preambuła do AI Act wskazuje ponadto na wartości etyczne, wprost odwołując się do Wytycznych w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji z 2019 r.[41] opracowanych na zlecenie Komisji Europejskiej przez Grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji. Dokument ten wskazuje na główne zasady etyczne związane z programowaniem sztucznej inteligencji, mające zbudować zaufanie społeczne do algorytmów SI. Preambuła AI Act zalicza do nich:

- nadzorczą i przewodnią rolę człowieka;
- bezpieczeństwo i solidność techniczną;
- zarządzanie danymi oraz ochronę prywatności;

Ekonomiczno-Społecznym, przyjmują środki dotyczące zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego".

39 Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689. [dostęp: 31.3.2025].

40 Pkt 1-6 Preambuły do AI Act. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689. [dostęp: 31.3.2025].

41 Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, opracowane przez Grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_PL.pdf. [dostęp: 1.4.2025].

- przejrzystość;
- różnorodność,
- sprawiedliwość oraz niedyskryminację;
- odpowiedzialność;
- dobrostan społeczny i środowiskowy [42].

Zasady te mają w założeniu przyczynić się do stworzenia wiarygodnej technologii zorientowanej przede wszystkim na człowieka zgodnie z Kartą Praw Podstawowych UE oraz z wartościami ujętymi m.in. w art. 2 Traktatu o Unii Europejskiej[43]. Założeniem AI Act jest zatem każdorazowa kontrola człowieka na algorytmami sztucznej inteligencji, stanowiąca swego rodzaju system „bezpieczników" etycznych, eliminujący wszelkie ryzyka niekontrolowanego rozwoju tej technologii w duchu poszanowania autonomii człowieka oraz jego godności, a zatem podstawowych wartości wynikających z praw człowieka[44]. Przykładem takich ryzyk mogą być techniki manipulacyjne i podprogowe, wykorzystujące sztuczną inteligencję w celu wprowadzania odbiorców w błąd, bądź wywołania niechcianych zachowań poprzez zniekształcanie i ograniczanie ludzkiej percepcji. Systemy wykorzystujące SI powinny mieć na celu wzmacnianie i uzupełnianie zdolności poznawczych człowieka[45] i z tego względu rozporządzenie UE w sprawie sztucznej inteligencji zostało skonstruowane w oparciu o analizę ryzyka, stosując rozróżnienie dla systemów SI stwarzających niedopuszczalne ryzyko, wysokie ryzyko oraz niskie lub minimalne ryzyko.

Preambuła do AI Act wskazuje także na kilka kluczowych zagadnień, którymi powinni kierować się zarówno operatorzy systemów wykorzystujących SI, w tym przede wszystkim dostawcy systemów, jak również organy administracyjne zobowiązane do działań nadzorczych, monitorujących oraz kontrolnych w tym zakresie. Wśród ważnych zagadnień ujętych w Preambule warto zwrócić uwagę na obowiązek projektowania

---

42 Pkt 27 Preambuły do AI Act.

43 Art. 2 TUE: „Unia opiera się na wartościach poszanowania godności osoby ludzkiej, wolności, demokracji, równości, państwa prawnego, jak również poszanowania praw człowieka, w tym praw osób należących do mniejszości. Wartości te są wspólne Państwom Członkowskim w społeczeństwie opartym na pluralizmie, niedyskryminacji, tolerancji, sprawiedliwości, solidarności oraz na równości kobiet i mężczyzn".

44 W aspekcie ochrony praw człowieka por. pkt 48 Preambuły do AI Act.

45 Tomaszewski, „Inteligentne kontrakty jako narzędzie regulacji sztucznej inteligencji", 198-199.

technologii SI w sposób umożliwiający osobom fizycznym stały nadzór nad ich działaniem[46]. Kluczowym adresatem ponoszącym odpowiedzialność za spełnienie określonych w AI Act wymogów jest Dostawca systemów SI[47]. W ramach procedury oceny zgodności systemy SI, mające status wysokiego ryzyka, powinny posiadać oznakowanie CE zgodnie z art. 48 AI Act[48] wskazujące na zgodność ich działania z unijnym Rozporządzeniem ws. sztucznej inteligencji, co umożliwia korzystanie ze swobody przepływu takiego oprogramowania na wewnętrznym rynku UE[49]. Ponadto, Preambuła zapowiada również powołanie Europejskiej Rady do spraw Sztucznej Inteligencji (art. 65-66 AI Act), ściśle współpracującej m.in. z Agencją Praw Podstawowych w celu skutecznej realizacji założeń AI Act na poziomie unijnym oraz państw członkowskich, pełniących kluczową rolę w stosowaniu i egzekwowaniu tego rozporządzenia[50].

Na uwagę zasługują merytoryczne normy Rozporządzenia ws. sztucznej inteligencji, przede wszystkim dotyczące zakresu oddziaływania AI Act, wymogów w odniesieniu do systemów sztucznej inteligencji, obowiązków operatorów SI, a także organów nadzorczych oraz procedur monitorujących systemy wykorzystujące sztuczną inteligencję. Zgodnie z art. 2 ust.1 AI Act rozporządzenie to ma zastosowanie do:

1. dostawców systemów SI niezależnie od ich siedziby (jeżeli systemy te są udostępniane na rynku UE lub wykorzystywane w UE bądź gdy wyniki wytworzone przez takie systemy są wykorzystywane w Unii Europejskiej);
2. podmiotów korzystających z systemów SI, które mają siedzibę w UE.
3. dystrybutorów i importerów systemów SI;
4. producentów produktu, którzy pod własną nazwą lub znakiem towarowym oraz wraz ze swoim produktem wprowadzają do obrotu lub oddają do użytku system SI;

46 Pkt 73 Preambuły do AI Act.
47 Pkt 101 Preambuły do AI Act.
48 Oznakowanie CE wskazuje, że dany wyrób został zbadany przez producenta i uznany za spełniający wymogi UE dotyczące bezpieczeństwa, zdrowia i ochrony środowiska. Oznakowanie jest wymagane w przypadku produktów wytwarzanych w dowolnym miejscu na świecie i wprowadzanych do obrotu na terenie Unii Europejskiej.
49 Pkt 129 Preambuły do AI Act.
50 Pkt 149 i 153 Preambuły do AI Act.

5. upoważnionych przedstawicieli dostawców niemających siedziby w Unii Europejskiej;
6. osób, na które SI ma wpływ i które znajdują się na terenie Unii Europejskiej.

Co istotne, zgodnie z art. 2 ust.3 i 4 AI Act przewidziane są wyłączenia w stosowaniu rozporządzenia, które obejmują systemy SI wykorzystywane wyłącznie do celów obronnych, wojskowych lub do celów bezpieczeństwa narodowego. Ponadto, postanowień AI Act nie stosuje się również w sytuacji wykorzystania systemów SI przez organizacje międzynarodowe lub organy publiczne państw trzecich w ramach współpracy międzynarodowej w sprawach o ściganie przestępstw i współpracy sądowej z udziałem Unii Europejskiej lub państw członkowskich UE[51]. Przepisy AI Act nie będą miały zastosowania również w odniesieniu do systemów SI wykorzystywanych wyłącznie w celach naukowo-rozwojowych oraz w sytuacji badań testowych systemów SI przed wprowadzeniem ich do obrotu lub oddaniem ich do użytku[52].

W rozdziale II Rozporządzenia ws. sztucznej inteligencji prawodawca unijny ujął kluczowe regulacje dotyczące zakazanych praktyk w zakresie wykorzystywania sztucznej inteligencji, opierające się na poziomach ryzyka[53]. W art. 5 AI Act uregulowano zakazane praktyki w zakresie wykorzystywania sztucznej inteligencji i zgodnie z tym zakazane są systemy SI, które:

- wykorzystują podprogowe techniki manipulacji, polegające na manipulacji świadomością[54];
- wykorzystują słabości określonych grup (np. dzieci, osób niepełnosprawnych)[55];
- służą do krzywdzącej bądź niekorzystnej oceny „społecznej wartości" jednostek (*social scoring*)[56];
- przeprowadzają oceny ryzyka osób fizycznych w celu profilowania w zakresie ryzyka popełniania przestępstw wyłącznie

51 Art. 2 ust. 4 AI Act.
52 Art. 2 ust. 6 i 8 AI Act.
53 Por. Wiśniewski, „Sztuczna inteligencja i prawa człowieka", 34.
54 Art. 5 ust. 1 lit. a) AI Act.
55 Art. 5 ust. 1 lit. b) AI Act.
56 Art. 5 ust. 1 lit. c) AI Act.

na podstawie cech osobowości i innych charakterystycznych cech danej jednostki[57];
- tworzą bazy danych mające na celu rozpoznawanie twarzy poprzez nieukierunkowane pozyskiwanie wizerunków twarzy (*untargeted scraping*) z internetu lub nagrań z telewizji przemysłowej (tzw. identyfikacja biometryczna w czasie rzeczywistym)[58];
- wykorzystują algorytmy celem zbierania danych dotyczących ludzkich emocji w miejscu pracy oraz instytucjach edukacyjnych i wyciągają z tego wnioski (z wyjątkiem względów medycznych i kwestii bezpieczeństwa)[59];
- wprowadzają kategoryzację biometryczną, profilującą osoby fizyczne pod kątem ich rasy, wyznania, orientacji seksualnej, poglądów politycznych bądź przynależności do określonych organizacji – z wyjątkiem ścigania przestępstw[60].

Rozporządzenie ws. sztucznej inteligencji w rozdziale III (art. 6-27) odnosi się do systemów SI wysokiego ryzyka, wykorzystywanych w sektorach o istotnym znaczeniu dla zdrowia, bezpieczeństwa lub praw podstawowych, takich jak infrastruktura krytyczna, edukacja i zatrudnienie, administracja publiczna (np. ocena wiarygodności beneficjentów świadczeń), bądź wymiar sprawiedliwości[61]. Dodatkowo Załącznik III do AI Act[62] wskazuje na systemy wykorzystujące sztuczną inteligencję uznawane za systemy wysokiego ryzyka w określonych obszarach życia społeczno-gospodarczego. Do tych obszarów należą m.in. biometria (np. zdalna identyfikacja biometryczna), procesy zarządzania infrastrukturą krytyczną (np. zaopatrzenie w wodę, gaz, ciepło lub energię elektryczną, a także zarządzanie ruchem drogowym), ściganie przestępstw oraz sprawowanie wymiaru sprawiedliwości i procesy demokratyczne (pkt 1,2,6 i 8 Załącznika III do AI Act). Systemy SI wymienione w załączniku III są uznawane za wysokiego ryzyka.

W art. 8 i 9 AI Act określone zostały kluczowe obowiązki dostawców systemów sztucznej inteligencji, w szczególności tych zakwalifikowanych

57 Art. 5 ust. 1 lit. d) AI Act.
58 Art. 5 ust. 1 lit. e) AI Act.
59 Art. 5 ust. 1 lit. f) AI Act.
60 Art. 5 ust. 1 lit. g) AI Act.
61 Wiśniewski, „Sztuczna inteligencja i prawa człowieka", 35.
62 Załącznik III do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 – Systemy AI wysokiego ryzyka, o których mowa w art. 6 ust. 2.

jako systemy wysokiego ryzyka. Do obowiązków tych zaliczyć należy m.in. konieczność stworzenia ocen zgodności i dokumentacji technicznej, zapewnienie przejrzystości działania, zaplanowanie zarządzania ryzykiem i jego identyfikacja, zapewnienie nadzoru ludzkiego oraz rejestracja w unijnym rejestrze systemów SI wysokiego ryzyka[63]. Artykuł 8 stanowi fundament dla zapewnienia zgodności systemów SI wysokiego ryzyka z obowiązującymi przepisami. Podkreśla on konieczność uwzględnienia zarówno aktualnego stanu wiedzy technologicznej, jak i specyfiki danego zastosowania systemu SI. Mechanizm ten umożliwia integrację procesów zgodności z istniejącymi procedurami wynikającymi z innych aktów prawnych Unii Europejskiej, co ma na celu redukcję obciążeń administracyjnych dla dostawców[64]. W art. 16 AI Act doprecyzowane zostały obowiązki dostawców systemów AI wysokiego ryzyka, m.in. w zakresie sporządzania deklaracji zgodności UE[65] oznaczania produktu symbolem CE oraz znakiem towarowym bądź nazwą celem ułatwienia kontaktu z dostawcą[66]. Bez wątpienia weryfikacja systemowa mechanizmów wynikających z art. 8-16 AI Act wymaga wsparcia i ścisłej współpracy organów publicznych (zarówno na poziomie unijnym, jak i krajowym) z programistami algorytmów SI oraz ekspertami w dziedzinie IT celem oceny niezbędnej dokumentacji, a także weryfikacji m.in. ocen zgodności, wdrożenia procesu rejestracji oraz efektywnego nadzoru nad systemami SI.

Niezwykle istotnym wydaje się art. 14 AI Act dotyczący nadzoru systemów SI przez człowieka, ponieważ ustanawia on jedną z ważniejszych zasad związanych z nadzorem człowieka nad funkcjonowaniem sztucznej inteligencji klasyfikowanych jako systemy wysokiego ryzyka. Zasada ta stanowi, iż na każdym etapie wykorzystywania systemów SI istnieje obowiązek zapewnienia adekwatnego, skutecznego i proporcjonalnego nadzoru osób fizycznych nad działaniem tych systemów, w celu zapobieżenia lub zminimalizowania zagrożeń dla zdrowia, bezpieczeństwa lub praw podstawowych[67]. Nadzór sprawowany przez człowieka ma na celu szybkie rozpoznanie i przeciwdziałanie potencjalnym niepożądanym skutkom działania systemu SI. Osoby sprawujące nadzór powinny posiadać

63 Por. art. 9 AI Act.

64 Zob. https://artificialintelligenceact.eu/article/8/. [dostęp: 7.4.2025].

65 W związku z art. 47 AI Act.

66 Analogiczne wymagania z uwzględnieniem właściwej specyfiki dotyczą również importerów oraz dystrybutorów systemów SI na obszarze UE – zgodnie z art. 23 i 24 AI Act.

67 Art. 14 ust. 2 AI Act.

niezbędną wiedzę, kwalifikacje i uprawnienia w zakresie znajomości systemów SI tak, by móc wykrywać wszelkie anomalie oraz nieprzewidziane zachowania algorytmów. Osoby takie na każdym etapie powinny również mieć możliwość przerwania, zawieszenia lub zmiany sposobu działania systemu SI w sytuacjach zagrożenia. Zgodnie z ust. 3, poziom i zakres nadzoru człowieka powinien być dostosowany do charakteru, przeznaczenia i ryzyka danego systemu SI[68].

Ważna regulacja znajduje się z art. 25 AI Act, gdzie unijny prawodawca ustanawia ramy odpowiedzialności w całym łańcuchu wartości systemów sztucznej inteligencji od projektowania, przez rozwój, aż po wdrożenie i eksploatację tych systemów. Artykuł ten rozszerza odpowiedzialność poza dostawców[69], także na dystrybutorów, importerów, integratorów oraz na podmioty stosujące systemy SI. Ma to na celu zapewnienie, że wszystkie podmioty zaangażowane w cykl życia systemów SI ponoszą odpowiedzialność za zgodność tych systemów z przepisami prawa Unii Europejskiej. Oznacza to, że każdy z tych podmiotów ma obowiązek zapewnienia, że systemy AI, które wprowadzają na rynek spełniają określone w rozporządzeniu wymogi dotyczące bezpieczeństwa, przejrzystości, nadzoru i zarządzania ryzykiem. W przypadku naruszenia przepisów rozporządzenia, odpowiedzialność może być przypisana nie tylko dostawcy systemu AI, ale również innym podmiotom w łańcuchu wartości, jeżeli ich działania lub zaniechania przyczyniły się do danego naruszenia.

Rozporządzenie UE w sprawie sztucznej inteligencji w art. 51 ustanawia kryteria służące klasyfikacji modeli sztucznej inteligencji ogólnego przeznaczenia jako modele ograniczonego ryzyka, ze szczególnym uwzględnieniem modeli stanowiących zagrożenie systemowe (tzw. *systemic GPAI models*), które wymagają zastosowania zaostrzonych wymogów regulacyjnych. Dla przykładu operatorzy systemów ograniczonego ryzyka mają obowiązek informacyjny dotyczący faktu, iż użytkownik danego systemu wchodzi w interakcję ze sztuczną inteligencją (np. chatboty symulującą

68 Oznacza to, że środki nadzoru powinny być proporcjonalne – bardziej restrykcyjne dla systemów wykorzystywanych w krytycznych obszarach, np. w wymiarze sprawiedliwości czy opiece zdrowotnej, a w mniejszym stopniu dla systemów o nieznacznym potencjale szkodliwości. Por. Art. 14 ust. 3 AI Act.

69 W rozumieniu definicji ujętej w art. 3 pkt 3 AI Act: „dostawca oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które rozwijają system AI lub model AI ogólnego przeznaczenia lub zlecają rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz które – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadzają do obrotu lub oddają do użytku system AI".

ludzką rozmowę). Artykuł 51 AI Act stanowi, że system SI ogólnego przeznaczenia (ograniczonego ryzyka) może zostać uznany za stanowiący zagrożenie systemowe, jeżeli spełnia określone przesłanki ilościowe lub jakościowe, w tym w szczególności:

- wykorzystuje zasoby obliczeniowe przekraczające określony próg;
- posiada duże oddziaływanie społeczno-gospodarcze;
- charakteryzuje się powszechnością wdrożenia w różnych sektorach gospodarki i życia społecznego;
- posiada zdolność do samodzielnego generowania treści, rozumowania, przewidywania lub wpływania na procesy decyzyjne użytkowników na dużą skalę;
- wykorzystanie takiego systemu niesie ze sobą możliwość wywołania poważnych szkód dla zdrowia, bezpieczeństwa, praw podstawowych, środowiska lub demokracji[70].

Zgodnie z art. 53 dostawcy modeli SI ogólnego przeznaczenia (ograniczonego ryzyka), są zobowiązani do sporządzania właściwej dokumentacji technicznej dla danego systemu. Dokumentacja ta powinna obejmować także informacje odnośnie procesu jego trenowania i testowania, jak również zawierać niezbędne dane dla podmiotów zamierzających legalnie zintegrować kilka systemów SI. Ponadto dostawcy zobowiązani są podawać do publicznej wiadomości streszczenie dotyczące wykorzystanych algorytmów w procesie trenowania danego modelu SI.

Rozdział VI AI Act odnosi się do środków wspierających innowacyjność sztucznej inteligencji, w tym przede wszystkim do tzw. piaskownic regulacyjnych będących narzędziami umożliwiającymi dostawcom systemów SI możliwość rozwoju, trenowania, walidacji i testowania innowacyjnych rozwiązań SI[71]. W artykule 57 AI Act w odniesieniu do państw członkowskich sformułowano obowiązek ustanowienia piaskownic regulacyjnych w zakresie wspierania systemów SI, które mają na celu stworzenie kontrolowanego środowiska wspierającego innowacje oraz rozwój i testowanie systemów SI przed ich wprowadzeniem na rynek[72]. Z piaskownic regulacyjnych mogą korzystać w szczególności *start-upy* oraz innowacyjne małe

70 Zob. Art. 51 ust. 1 i 2 AI Act oraz Załącznik XIII do tego Rozporządzenia pt. „Kryteria identyfikowania modeli AI ogólnego przeznaczenia z ryzykiem systemowym, o których mowa w art. 51".

71 Por. Art. 3 pkt 55 AI Act.

72 Art. 57 ust. 5 AI Act.

i średnie przedsiębiorstwa, przy czym państwa członkowskie są zobowiązane do zapewnienia im proporcjonalnego i niedyskryminującego dostępu do tych mechanizmów wsparcia. Zgodnie z art. 57 ust. 9 AI Act celem piaskownic regulacyjnych dla systemów SI jest m.in. wspieranie wymiany najlepszych praktyk poprzez współpracę z organami uczestniczącymi w piaskownicy regulacyjnej oraz wzmacnianie innowacyjności i konkurencyjności oraz ułatwianie rozwoju ekosystemu sztucznej inteligencji.

W celu wdrożenia postanowień Rozporządzenia ws. sztucznej inteligencji w oparciu o art. 64 AI Act powołany został Europejski Urząd ds. Sztucznej Inteligencji (*European Artificial Intelligence Office* – EAIO) jako wyspecjalizowany organ Unii Europejskiej. Zadaniem tego urzędu jest m.in. klasyfikowanie systemów SI, badanie naruszeń oraz wspieranie rozwoju SI poprzez zapewnienie jednolitego stosowania, skutecznego egzekwowania oraz nadzoru nad wdrażaniem przepisów dotyczących sztucznej inteligencji na terytorium Unii Europejskiej[73]. Oprócz tego Rozporządzenie w art. 65 przewiduje powołanie Europejskiej Rady ds. Sztucznej Inteligencji, której celem jest m.in. przyczynianie się do koordynacji między właściwymi organami krajowymi odpowiedzialnymi za stosowanie AI Act, zapewnienie doradztwa w zakresie wdrażania AI Act oraz przyczynianie się do harmonizacji praktyk administracyjnych w zakresie sztucznej inteligencji w państwach członkowskich[74]. Skład rady tworzą przedstawiciele państw członkowskich, Europejski Urząd ds. Sztucznej Inteligencji[75] oraz Europejski Inspektor Ochrony Danych w charakterze obserwatora.

Rozporządzenie ws. sztucznej inteligencji wprowadza w art. 72 obowiązek monitorowania systemów SI po wprowadzeniu ich do obrotu. System ten ma na celu zbieranie właściwej dokumentacji i analiz związanych ze skutecznością działania systemów SI w całym ich cyklu życia, co pozwala dostawcom oceniać, czy zapewniona jest ciągła zgodność systemów SI z wymogami ustanowionymi przez AI Act[76]. Konsekwencją tego jest określenie w art. 79 procedury postępowania na poziomie krajowym w przypadku systemów SI stwarzających ryzyko. Zgodnie z tym

73 https://digital-strategy.ec.europa.eu/pl/policies/ai-office#ecl-inpage-tasks-of-the-ai-office. [dostęp: 10.4.2025].

74 Szerzej: art. 66 AI Act.

75 Bez prawa głosu – Europejski Urząd ds. Sztucznej Inteligencji pełni funkcję sekretariatu dla Rady ds. Sztucznej Inteligencji – art. 65 ust. 8 AI Act.

76 Co istotne obowiązek ten nie obejmuje wrażliwych danych operacyjnych wykorzystywanych przy stosowaniu systemów SI przez organy ścigania – zob. art. 72 ust. 2 AI Act.

artykułem ryzyko systemu SI dotyczyć może przede wszystkim zdrowia, bezpieczeństwa oraz praw podstawowych użytkowników i odbiorców systemów SI. Rozporządzenie wskazuje, że postępowanie w sytuacji działania systemów SI stwarzających ryzyko prowadzą właściwe organy krajowe (np. urzędy ds. ochrony konsumentów, danych osobowych, bądź rynku)[77]. Mechanizm ten pozwala państwom członkowskim na szybką i skuteczną reakcję wobec systemów SI, które – mimo formalnej zgodności z przepisami – faktycznie stwarzają istotne zagrożenia. Jednocześnie wprowadza proceduralne zabezpieczenia w postaci obowiązku notyfikacji i możliwości interwencji Komisji, co zapewnia spójność regulacyjną na poziomie Unii Europejskiej i chroni bezpieczeństwo oraz integralność rynku wewnętrznego[78].

Wartym uwagi jest również Rozdział XII Rozporządzenia ws. Sztucznej Inteligencji. W art. 99 AI Act ustanowiono ramy odpowiedzialności administracyjnej za naruszenia Rozporządzenia przez operatorów SI, przewidując nałożenie kar pieniężnych za określone kategorie naruszeń. Zgodnie z postanowieniami tego artykułu najsurowsza sankcja dotyczy przypadków niezgodnego z prawem udostępniania lub stosowania systemów SI o niedopuszczalnym ryzyku (tj. zakazanych systemów SI określonych w art. 5 AI Act). W tym przypadku maksymalna kara wynosi do 35 mln EUR lub 7% całkowitego rocznego obrotu światowego danego podmiotu[79]. Niższe kary wprowadzono za naruszenie istotnych obowiązków w zakresie funkcjonowania systemów wysokiego ryzyka, obowiązków notyfikacyjnych lub nadzorczych, co może skutkować nałożeniem kary do 15 mln EUR lub 3% obrotu danego przedsiębiorstwa[80]. Dodatkowo przewidziano możliwość nakładania kar w wysokości do 7,5 mln EUR lub 1% obrotu za dostarczenie nieprawidłowych, wprowadzających w błąd lub niekompletnych informacji organom nadzorczym[81].

Administracyjne kary pieniężne mogą być nakładane również na organy i jednostki organizacyjne Unii Europejskiej. Zgodnie z art. 100 AI Act Europejski Inspektor Ochrony Danych może nakładać takie kary na instytucje,

77 Art. 79 ust. 2 AI Act.

78 Zgodnie z art. 89 AI Act również Europejski Urząd ds. Sztucznej Inteligencji może podejmować działania monitorujące niezbędne do skutecznego wdrożenia i zapewnienia zgodności z AI Act przez dostawców modeli AI.

79 Art. 99 ust. 3 AI Act.

80 Art. 99 ust. 4 AI Act.

81 Art. 99 ust. 5 AI Act.

organy i jednostki organizacyjne Unii w związku ze stosowaniem AI Act[82]. Nieprzestrzeganie norm w zakresie systemów SI stanowiących niedopuszczalne ryzyko (o których mowa w art. 5 AI Act) podlega administracyjnym karom pieniężnym w wysokości do 1.500.000 EUR. W przypadku nieprzestrzegania przepisów w zakresie systemów SI, stanowiących wysokie, niskie bądź minimalne ryzyko w związku z wymogami określonymi w AI Act, kary są limitowane do wysokości do 750.000 EUR[83]. Wysokość kar uzależniona jest zarówno od m.in. liczby poszkodowanych osób oraz podmiotów, rozmiaru szkód, stopnia odpowiedzialności danej instytucji UE (z uwzględnieniem wdrożonych przez nie środków technicznych i organizacyjnych), jak również od charakteru oraz czasu trwania danego naruszenia.

Rozporządzenie UE w sprawie sztucznej inteligencji nie odnosi się wprost do norm technicznych, czy procesów rozwoju i trenowania algorytmów budujących systemy SI, natomiast dotyczy sposobów w jakich systemy te mogą być wykorzystywane w otoczeniu społeczno-gospodarczym[84]. W rozporządzeniu nie zdecydowano się jednak na uregulowanie odpowiedzialności deliktowej za szkody powstałe w związku z wykorzystywaniem systemów SI. Powstał natomiast unijny projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za sztuczną inteligencję[85] mającej na celu zharmonizowanie prawa krajowego w zakresie odpowiedzialności cywilnoprawnej za systemy SI poprzez stworzenie bądź ujednolicenie właściwych regulacji prawnych na poziomie państw członkowskich[86].

Istotą projektu Dyrektywy jest zapewnienie, aby jednostki mogły skutecznie dochodzić roszczeń odszkodowawczych w sytuacjach, gdy szkoda powstała w wyniku działania lub zaniechania związanego z użyciem systemu sztucznej inteligencji – zarówno autonomicznego, jak i wspomagającego decyzje człowieka. Zgodnie z piśmiennictwem proponowana

82 Art. 100 ust. 1 AI Act.

83 Art. 100 ust. 2 i 3 AI Act.

84 Świerczyński, Więckowski, Sztuczna inteligencja w prawie międzynarodowym, 31.

85 Projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji z dnia 28 września 2022 r. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022PC0496. [dostęp: 24.3.2025].

86 Zdzisław Brodecki, *Świątynia w sieci algorytmów – kod idei* (Warszawa: EuroPrawo, 2024), 66-67.

dyrektywa wprowadzi zasady gwarantujące jednolity poziom ochrony ofiar szkód związanych z technologiami wykorzystującymi SI, jak z podmiotami poszkodowanymi przez inne technologie[87]. Do kluczowych rozwiązań prawnych tego projektu zaliczyć można:

1. domniemania prawne ułatwiające dochodzenie roszczeń, w tym domniemanie związku przyczynowego między niewykonaniem obowiązku a szkodą w przypadku naruszenia określonych obowiązków regulacyjnych w zakresie SI (art. 4 projektu);
2. Mechanizm ujawnienia dowodów umożliwiający sądom nakazanie producentom lub operatorom systemów SI przedstawienia danych technicznych niezbędnych do wykazania podstaw odpowiedzialności (art. 3 projektu);
3. Zakres stosowania obejmujący zarówno szkody majątkowe, jak i niemajątkowe, wyrządzone przez systemy SI o wysokim stopniu ryzyka[88].

Projekt Dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję ma charakter komplementarny względem innych regulacji UE w obszarze sztucznej inteligencji i stanowi próbę zbalansowania interesów innowacyjności technologicznej z koniecznością ochrony praw jednostek. Jego przyjęcie ma zapewnić jednolite standardy odpowiedzialności w całej Unii Europejskiej oraz dostosować prawo cywilne do nowych wyzwań technologicznych. Dyrektywa ta bez wątpienia byłaby w stanie uzupełnić unijne ramy odpowiedzialności cywilnej, wprowadzając regulacje dotyczące szkód powstałych w związku z użytkowaniem SI w duchu większej ochrony poszkodowanych przez systemy SI za sprawą ułatwienia dochodzenia

87 Zob. Paolo Sasdelli, *Proposed liability rules aim to shape AI responsibilities*. https://www.twobirds.com/en/insights/2025/proposed-liability-rules-aim-to-shape-ai-responsibilities. [dostęp: 15.4.2025]. Autor wskazuje, że projekt Dyrektywy m.in. zmniejsza ciężar dowodu dla ofiar, umożliwiając wzruszalne domniemanie związku przyczynowego, co oznacza, że jeśli ofiara może wykazać, że system SI prawdopodobnie spowodował szkodę (np. w razie nieprzestrzegania obowiązku dochowania należytej staranności przez pozwanego), pozwany musi wykazać argumenty przeciwne (zob. art.4 projektu Dyrektywy).

88 Uzasadnienie do Projektu Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji, COM(2022) 496 final, s. 4. Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022PC0496. [dostęp: 15.4.2025].

roszczeń odszkodowawczych[89]. Niestety na chwilę obecną (kwiecień 2025 r.) projekt wspomnianej Dyrektywy został wycofany z dalszych prac legislacyjnych z powodu obawy o nadmierne obciążenia regulacyjne i brak konsensusu politycznego co do kształtu tej dyrektywy. Pozostaje mieć nadzieję na powrót UE do dalszych prac na tym projektem.

Bez wątpienia w obliczu kształtowania się praktyki stosowania AI Act oraz powiązanych i nim ram prawnych SI, ważną rolę odegra orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej. Wskazuje się, że już obecnie orzecznictwo to incydentalnie odnosiło się do problematyki SI, w szczególności w takich obszarach jak ochrona danych osobowych, ochrona własności intelektualnej[90], dostęp do dokumentów, handlu elektronicznego, czy ochrony konsumentów na unijnym rynku jednolitym[91].

W aspekcie ochrony danych osobowych dość szeroko komentowany był wyrok TSUE z 2020 roku w sprawie Schrems II[92]. Wyrok ten dotyczy przekazywania danych osobowych pomiędzy UE a Stanami Zjednoczonymi z zastosowaniem sztucznej inteligencji, która przetwarza dane w aspekcie inwigilacji. Zasadniczą kwestią w tym wyroku było pytanie o ważność decyzji Komisji Europejskiej (tzw. *Privacy Shield*[93]), dzięki której możliwe było przekazywanie danych osobowych z UE do Stanów Zjednoczonych. Austriacki obywatel Maximilian Schrems wniósł skargę do irlandzkiego Inspektora Ochrony Danych Osobowych zarzucając spółce Facebook Ireland fakt przekazywania wrażliwych danych osobowych do spółki Facebook Inc. w Stanach Zjednoczonych, co mogło go narażać na inwigilację przez amerykańskie służby wywiadowcze, naruszając tym samym

89 Wiśniewski, „Sztuczna inteligencja i prawa człowieka", 33.

90 Céline Castets-Renard, „The Intersection Between AI and IP: Conflict or Complementarity?" *International Rewiew of Intellectual Property and Competition Law*, t. LI (2020): 141-143.

91 Magdalena Konopacka, „Wokanda europejska – TSUE", [w:] *Przedwiośnie ery sztucznej inteligencji. Technologia-zarządzanie-prawo*, t. I, red. Edmund Wittbrodt, Zdzisław Brodecki, Marta Dargas-Draganik (Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego, 2024), 290.

92 Wyrok TSUE z dnia 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commisioner vs. Facebook Ireland Ltd i Maximilian Schrems. https://curia.europa.eu/juris/liste.jsf?num=C-311/18. [dostęp: 15.5.2025].

93 Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA (Dz. Urz. UE L 207, s. 1). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016D1250. [dostęp: 15.5.2025].

przepisy UE. Sędziowie w wyroku tym stwierdzili, że decyzja Komisji Europejskiej (tzw. *Privacy Shield*) jest nieważna, bowiem nie zapewnia obywatelom UE właściwej ochrony danych przed dostępem służb wywiadowczych Stanów Zjednoczonych, podkreślając tym samym znaczenie efektywnych zabezpieczeń prywatności w procesie przekazywania danych. Orzeczenie to miało poważne konsekwencje dla podmiotów prowadzących działalność transatlantycką, poprzez konieczność reorganizacji procesu transferu danych[94].

3 Podsumowanie

W obecnej chwili europejskie porozumienia międzynarodowe wiodą prym, jeśli chodzi o unifikację przynajmniej podstaw prawa sztucznej inteligencji, regulowanej jak dotąd przede wszystkim na poziomie krajowym, co zagrażałoby dalszą fragmentaryzacją rozwiązań. Dodać należy, iż sama sztuczna inteligencja nie posiada jednego jądra, wokół którego rozwijane są poszczególne metody rozwiązywania problemów przez algorytmy. Metody sztucznej inteligencji, do których zaliczyć można m.in. systemy uczące się, sieci neuronowe, logikę rozmytą bądź algorytmy genetyczne rozwijały się w izolacji od siebie i do chwili obecnej nie ma możliwości prostego przejścia z jednej metody do drugiej. Taka specyfika struktury SI skłania do posługiwania się metaforą „archipelag sztucznej inteligencji" odnoszącą się do „wyspowego" charakteru SI[95].

Przy braku norm prawa międzynarodowego porządkujących prawne aspekty powiązanie z użyciem sztucznej inteligencji to właśnie Konwencja ramowa Rady Europy o sztucznej inteligencji[96] oraz unijne Rozporządzenie

94 Szerzej: Konopacka, „Wokanda europejska – TSUE", 291.

95 Ryszard Tadeusiewicz, „Archipelag sztucznej inteligencji", [w:] *Przedwiośnie ery sztucznej inteligencji. Technologia-zarządzanie-prawo*, t. I, red. Edmund Wittbrodt, Zdzisław Brodecki, Marta Dargas-Draganik (Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego, 2024), 44-45. Por. Brodecki, *Świątynia w sieci algorytmów – kod idei*, 11-12.

96 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series – No. 225, Vilnius, 5.IX.2024. https://rm.coe.int/1680afae3c [dostęp: 25.3.2025].

ws. sztucznej inteligencji (AI Act)[97] jako pierwsze akty prawa ponadnarodowego są wyrazem dążenia do stworzenia ponadnarodowych i pośrednio również międzynarodowych mechanizmów oraz standardów dla twórców i użytkowników systemów SI. Europejska perspektywa wyrażana zarówno przez UE, jak i Radę Europy, akcentuje konieczność rozwoju SI według określonych reguł etycznych oraz praw człowieka, co ma zapewnić rozwój systemów SI w kierunkach nakreślonych przez człowieka[98]. Relacja pomiędzy tymi aktami prawa ponadnarodowego kształtuje się w oparciu o wzajemnie uzupełniające się cele i zakresy regulacyjne, choć obie inicjatywy wywodzą się z różnych porządków prawnych i różnią się charakterem normatywnym.

W praktyce dla państw członkowskich UE, które będą stronami Konwencji, konieczna będzie koherencja implementacyjna, zapewnienie, by stosowanie AI Act nie naruszało postanowień Konwencji, zwłaszcza w obszarach takich jak dyskryminacja algorytmiczna, przejrzystość czy odpowiedzialność. Z drugiej strony państwa spoza UE, które przyjmą Konwencję, mogą ją traktować jako podstawę do tworzenia własnych regulacji AI, wzorowanych na europejskich standardach obejmujących ramy etyczne oraz wartości związane przestrzeganiem praw podstawowych. Fakt, iż do Konwencji ramowej Rady Europy o sztucznej inteligencji przystąpiły już takie państwa jak Kanada, Izrael, Japonia oraz Stany Zjednoczone[99], świadczy o sporym potencjale tej konwencji w zakresie mocy oddziaływania w skali międzynarodowej. Daje to nadzieję na skuteczność europejskich prób scalenia w skali międzynarodowej systemów prawnych zarządzających sztuczną inteligencją[100]. Powstanie nowego subsystemu międzynarodowego odnoszącego się całościowo do eksterytorialnej przestrzeni cyfrowej pozwoli na przejście przez wody archipelagowe sztucznej inteligencji w kierunku metaforycznego „oceanu sztucznej inteligencji"[101].

---

97 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689. [dostęp: 23.3.2025].

98 Świerczyński, Więckowski, *Sztuczna inteligencja w prawie międzynarodowym*, 20.

99 Zob. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225. [dostęp: 20.4.2025].

100 Nadzieje autora obejmują dyskusje na forum G-7, OECD, G-20 i Organizacji Narodów Zjednoczonych.

101 Metafory tej używa prof. Zdzisław Brodecki w kontekście *Artificial Superintelligence* (AS). Zob. Brodecki, *Świątynia w sieci algorytmów – kod idei*, 12.

Bibliografia

Bałos Iga, „Konsekwencje braku kompleksowego modelu ochrony wizerunku i innych dóbr niematerialnych aktorów w kontekście stosowania narzędzi sztucznej inteligencji" *Prawo i Więź* nr 4 (2023): 383-397. https://doi.org/10.36128/PRIW.VI47.825.

Bałos Iga, „Wpływ generatywnej sztucznej inteligencji na ocenę nowości wynalazku" *Prawo i Więź* nr 1 (2025): 545-563. https://doi.org/10.36128/PRIW.VI54.1167.

Bernacka Julia, „Problematyka prawna technologii deepfake – analiza legalności tworzenia i rozpowszechniania deepfake'ów po uchwaleniu AI Act" *Prawo i Więź* nr 5 (2025): 671-694. https://doi.org/10.36128/hg1acq35.

Bień-Węgłowska Iwona, „Deepfake w świetle aktu w sprawie sztucznej inteligencji" *Prawo i Więź* nr 5 (2025): 151-169. https://doi.org/10.36128/4dr67e80.

Bierecki Dominik, Christophe Gaie, Mirosław Karpiuk, „Artificial Intelligence in e-Administration" *Prawo i Więź* nr 1 (2025): 383-407. https://doi.org/10.36128/PRIW.VI54.1201.

Bitar Mohammad, Ahmad Khalil, S. Anandha Krishna Raj, Rupal Malik, „Legal Assessment of Bias and Discrimination of AI Tools in Higher Education and Research" *Prawo i Więź* nr 3 (2025): 9-37. https://doi.org/10.36128/PRIW.VI56.896.

Brodecki Zdzisław, *Świątynia w sieci algorytmów – kod idei*. Warszawa: EuroPrawo, 2024.

Burczaniuk Piotr, „Tworzenie prawa sztucznej inteligencji – wyzwania i perspektywy" *Prawo i Więź* nr 3 (2024): 283-300. https://doi.org/10.36128/PRIW.VI51.707

Castets-Renard Celine, „The Intersection Between AI and IP: Conflict or Complementarity?" *International Review of Intellectual Property and Competition Law*, t. LI (2020): 141-143.

Chyc Paweł, „Załączniki – Materiał źrodłowy, [w:] *Świątynia w kosmicznej wiosce. Bezpieczeństwo przyszłych pokoleń w erze sztucznej inteligencji*, red. Zdzisław Brodecki. 165-254. Warszawa: EuroPrawo, 2021.

Dunn Gibson, „Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law *Gibson, Dunn & Crutcher LLP* (2024).

Dziedzic Magdalena, „Przeciwdziałanie dezinformacji w kontekście wybranych regulacji Aktu o usługach cyfrowych oraz Aktu o Sztucznej Inteligencji" *Prawo i Więź* nr 6 (2024): 223-238. https://doi.org/10.36128/PRIW.VI53.1103.

Fischer Bogdan, Marlena Sakowska-Baryła, „Wykorzystywanie otwartych danych jako element zwiększenia wyjaśnialności AI" *Prawo i Więź* nr 6 (2024): 289-305. https://doi.org/10.36128/PRIW.VI53.11166.

Furmanek Waldemar, „Najważniejsze idee czwartej rewolucji przemysłowej «Industrie 4.0 »" *Dydaktyka Informatyki*, nr 13 (2018): 55-63. https://doi.org/10.15584/di.2018.13.8.

Górski Marcin, „Treści generowane przez sztuczną inteligencję a ochrona różnorodności form wyrazu kulturowego" *Prawo i Więź* nr 4 (2023): 335-353. https://doi.org/10.36128/PRIW.VI47.791.

Gredka-Ligarska Iwona, „In Search of Adequate Principles for AI Civil Liability" *Prawo i Więź* nr 3 (2024): 157-190. https://doi.org/10.36128/PRIW.VI50.829.

Jasińska Katarzyna, „Problematyka oznaczania wytworów generatywnej sztucznej inteligencji w świetle polskiej ustawy o zwalczaniu nieuczciwej konkurencji" *Prawo i Więź* nr 1 (2025): 529-544. https://doi.org/10.36128/PRIW.VI54.1169.

Jasińska Katarzyna, „Trenowanie sztucznej inteligencji a naruszenie praw autorskich. Aspekty dowodowe" *Prawo i Więź* nr 1 (2025): 419-434. https://doi.org/10.36128/PRIW.VI47.796.

Kamiński Marcin, „Akt administracyjny zautomatyzowany. Zasadnicze problemy konstrukcyjne zastosowania systemów sztucznej inteligencji w procesach decyzyjnych postępowania administracyjnego na tle prawnoporównawczym" *Prawo i Więź* nr 4 (2023): 281-304. https://doi.org/10.36128/PRIW.VI47.798.

Kamiński Marcin, „Podmiot kompetencji administracyjnej w zautomatyzowanych procesach stosowania prawa na tle problematyki legitymacji prawno-demokratycznej delegowania kompetencji na systemy sztucznej inteligencji i odpowiedzialności prawnej za ich działania lub zaniechania" *Prawo i Więź* nr 6 (2024): 239-263. https://doi.org/10.36128/PRIW.VI53.1102.

Kimpian Peter, „Rights to Privacy and to Personal Data Protection and Convention 108", [w:] *African Data Protection Laws*. 19-28. Berlin-Boston: Walter de Gruyter, 2024.

Konopacka Magdalena, „Wokanda europejska – TSUE, [w:] *Przedwiośnie ery sztucznej inteligencji. Technologia-zarządzanie-prawo*, t. I, red. Edmund Wittbrodt, Zdzisław Brodecki, Marta Dargas-Draganik. 288-302. Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego, 2024.

Kowalski Michał, „Czy, komu i w jakim zakresie przysługują prawa do wytworów generatywnej sztucznej inteligencji? Analiza prawna z perspektywy warunków użytkowania MidJourney" *Prawo i Więź* nr 1 (2024): 259-280. https://doi.org/10.36128/PRIW.VI48.792.

Kowalski Michał, „Sztuczna inteligencja a usprawnienie postępowania przed sądami administracyjnymi. Kilka refleksji na tle doświadczeń wybranych systemów prawnych" *Prawo i Więź* nr 1 (2025): 429-442. https://doi.org/10.36128/PRIW.VI54.1161.

Kowalski Michał, „The Impact of Artificial Intelligence on the Future Functioning of Administrative Courts" *Prawo i Więź* nr 6 (2024): 173-185. https://doi.org/10.36128/PRIW.VI53.988.

Kowalski Michał, „Wpływ technologii na konstrukcję uzasadnień orzeczeń sądów administracyjnych" *Prawo i Więź* nr 4 (2023): 265-279. https://doi.org/10.36128/PRIW.VI47.810.

Królikiewicz Oliwia, „Od niewolnika po elektroniczną osobę prawną, czyli rozważania na temat podmiotowości prawnej dla AI" *Prawo i Więź* nr 5 (2025): 653-670. https://doi.org/10.36128/qjfzg275.

Księżak Paweł, "Sztuczna inteligencja jako wychowawca, opiekun i reprezentant: w poszukiwaniu definicji rodziny" *Prawo i Więź* nr 3 (2023): 289 – 298. https://doi.org/10.36128/PRIW.VI46.666.

Kulesza Joanna, *Międzynarodowe prawo Internetu*. Poznań: Ars boni et aequi, 2010.

Mik Cezary, *Państwo i prawo wobec procesów internacjonalizacji, integracji i globalizacji*, t. II, *Wpływ globalizacji na klasyczny paradygmat państwa i prawa. W cieniu pandemii SARS-COVID 19*. Toruń: TNOiK, 2022.

Ogrodnik-Kalita Agnieszka, „Wierność w czasach cyfrowej zarazy, czyli o prawach i obowiązkach małżeńskichw dobie sztucznej inteligencji i nowych technologii" *Prawo i Więź* nr 4 (2023): 399-418. https://doi.org/10.36128/PRIW.VI47.800.

Olszewski Jan, „Wybrane problemy prawa Piaskownic Regulacyjnych we wspieraniu działalności gospodarczej" *Prawo i Więź* nr 3 (2024): 61-91. https://doi.org/10.36128/PRIW.VI52.1003.

Sasdelli Paolo, *Proposed Liability Rules Aim to Shape AI Responsibilities*. 2025.

Schwab Klaus, *Czwarta rewolucja przemysłowa*, tłum. Anna Dorota Kamińska. Warszawa: Studio Emka, 2018.

Szanciło Tomasz, Beata Stępień-Załucka, „Sędzia robotem a robot sędzią w postępowaniu cywilnym w ujęciu konstytucyjnym i procesowym" *Prawo i Więź* nr 4 (2023): 217-247. https://doi.org/10.36128/PRIW.VI47.827.

Szpyt Kamil, Artur Bilski, „Wybrane wyzwania prawne i organizacyjne związane z wdrażaniem systemów AI w działalności samorządów terytorialnych" *Prawo i Więź* nr 1 (2025): 565-596. https://doi.org/10.36128/PRIW.VI54.1048.

Świerczyński Marek, Zbigniew Więckowski, „Intellectual Property and Artificial Intelligence – Selected Issue" *Prawo i Więź* nr 3 (2022): 179-202. https://doi.org/10.36128/priw.vi41.469.

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

Tadeusiewicz Ryszard, „Archipelag sztucznej inteligencji", [w:] *Przedwiośnie ery sztucznej inteligencji. Technologia-zarządzanie-prawo*, t. I, red. Edmund Wittbrodt,

Zdzisław Brodecki, Marta Dargas-Draganik. 43-72. Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego, 2024.

Tomaszewski Paweł, „Inteligentne kontrakty jako narzędzie regulacji sztucznej inteligencji", [w:] *Prawo w erze sztucznej inteligencji. Cyfryzacja i autonomizacja życia publicznego*, red. Zdzisław Brodecki, Marta Nowicka. 189-230. Gdynia–Pelplin: Bernardinum, 2022.

Więckowski Zbigniew, Grzegorz Kubalski, „Czy sztuczna inteligencja oraz inne technologie informatyczne pomogą w dostępie do wymiaru sprawiedliwości osobom ze szczególnymi potrzebami?" *Prawo i Więź* nr 4 (2022): 146-165. https://doi.org/10.36128/priw.vi42.546.

Więckowski Zbigniew, Marek Świerczyński, „Analiza ryzyka dokonywana na podstawie konwencji ramowej Rady Europy o sztucznej inteligencji na przykładzie zastosowań w sektorze prawnym" *Prawo i Więź* nr 1 (2025): 409-428. https://doi.org/10.36128/PRIW.VI54.1171.

Wiśniewski Adam, „Sztuczna inteligencja i prawa człowieka w kontekście prawa międzynarodowego"*Prawo i Więź*, nr 4 (2023): 29-52. https://doi.org/10.36128/PRIW.VI47.785.

Wiśniewski Adam, „Wokanda europejska – ETPC", [w:] *Przedwiośnie ery sztucznej inteligencji. Technologia-zarządzanie-prawo*, t. I, red. Edmund Wittbrodt, Zdzisław Brodecki, Marta Dargas-Draganik. 280-288. Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego, 2024.