DOI: 10.34616/151615

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 4, 60–80

Łukasz Sobczyk*
ORCID: 0009-0002-3819-4691

Zgodność algorytmów i samouczących się systemów z wybranymi aspektami prawa Unii Europejskiej

Streszczenie

Artykuł podejmuje problem zapewnienia zgodności algorytmów i systemów samouczących się – szeroko rozumianych jako systemy sztucznej inteligencji (AI) – z prawem Unii Europejskiej. Autor wskazuje, że taka zgodność wymaga podejścia multidyscyplinarnego, łączącego perspektywy prawne, etyczne i techniczne, zakorzenionego w koncepcji godnej zaufania AI – zasadzie coraz częściej uznawanej przez unijnych ustawodawców oraz międzynarodowe organy normalizacyjne. Opracowanie podkreśla znaczenie dogmatyki prawa oraz wykładni dynamicznej jako narzędzi pozwalających prawu nadążać za dynamicznym rozwojem technologii AI. Artykuł proponuje ponadto opracowanie nowoczesnej metodologii audytu, dostosowanej do specyficznych cech systemów AI, mającej na celu ocenę, czy spełniają one prawne i etyczne standardy zaufania. Biorąc pod uwagę zdolność AI do przetwarzania ogromnych i zróżnicowanych zbiorów danych, artykuł analizuje związane z tym ryzyka wystąpienia błędów oraz naruszeń praw podstawowych. Przedmiotem analizy są wybrane akty prawne – w tym ogólne rozporządzenie o ochronie danych (RODO), Akt o sztucznej inteligencji (AI Act), Rozporządzenie w sprawie maszyn oraz Dyrektywa NIS 2 – a także norma ISO 42001, przedstawiona jako istotny instrument współregulacyjny. Zwrócono uwagę na zbieżność wymagań przewidzianych w tych ramach regulacyjnych. Artykuł kończy się praktycznymi uwagami dotyczącymi projektowania systemów AI, wskazując na analogie do procesów inżynierii oprogramowania oraz prezentuje model audytu oparty na dostępie do informacji, przejrzystości i wyjaśnialności algorytmów. Takie podejście umożliwia wiarygodną ocenę zgodności systemów AI z obowiązującymi standardami prawnymi i etycznymi.

Słowa kluczowe

algorytmy, sztuczna inteligencja, zgodność sztucznej inteligencji z prawem, audyt zgodności systemów AI, zarządzanie ryzykiem w systemach AI, ochrona danych osobowych, cyberbezpieczeństwo, normy międzynarodowe, przejrzystość, wyjaśnialność, interpretowalność, etyczność, uczciwość, odpowiedzialność, wykładnia dynamiczna, wykładnia funkcjonalna, definicja sztucznej inteligencji

---

* Autor jest absolwentem Politechniki Śląskiej w Gliwicach, Wydziału Automatyki, Elektroniki i Informatyki, na kierunku informatyka, oraz Uniwersytetu Śląskiego w Katowicach, Wydziału Prawa i Administracji, na kierunku prawo. Obecnie odbywa aplikację radcowską przy Okręgowej Izbie Radców Prawnych w Katowicach.

Wstęp

Niniejszy artykuł przedstawia wnioski wynikające z analizy zagadnienia zgodności algorytmów i systemów samouczących się z wybranymi regulacjami prawnymi Unii Europejskiej (UE), podkreślając przy tym jednocześnie znaczenie norm stworzonych przez międzynarodowe organizacje normalizujące jako elementów o charakterze współregulującym.

Zauważyć należy, że zastosowanie algorytmów i systemów samouczących się jako elementów tworzących systemy sztucznej inteligencji (AI) ma istotny wpływ zarówno na sektor technologiczny, jak i szerzej na krajobraz społeczno-gospodarczy. AI dzięki zdolności do analizy dużych zbiorów danych o zróżnicowanym formacie, możliwości adaptacji, możliwości autonomicznej optymalizacji działań otwiera nowe możliwości w wielu dziedzinach, jednocześnie rodząc pytania dotyczące regulacji prawnych i wyzwań etycznych.

Analizę zgodności AI z prawem UE należy w pierwszej kolejności odnieść do standardów międzynarodowych, takich jak te tworzone przez Organizację Współpracy Gospodarczej i Rozwoju[1] (ang. OECD) czy Międzynarodową Organizację Normalizacyjną[2] (ang. ISO). OECD jako organizacja międzynarodowa tworzy i rekomenduje strategie, regulacje czy polityki oparte na dowodach (ang. *evidence-based*), czyli na podstawie solidnych, empirycznych danych, analiz naukowych oraz wiedzy eksperckiej, które wpływają na regulacje prawne. W Polsce odwołania do standardów OECD są widoczne m.in. w dokumencie „Polityka dla rozwoju sztucznej inteligencji w Polsce" z 2020 r.[3], wskazując na ścisłą współpracę i przyjęcie definicji AI opracowanej przez tę organizację. Również ISO, od momentu swojego powstania, gromadzi wokół siebie ekspertów, których zadaniem jest uzgodnienie najlepszych praktyk związanych z wytwarzaniem produktów czy świadczeniem usług. Stosowanie standardów ISO przez przedsiębiorstwa i uzyskiwanie w tym zakresie certyfikacji stało się obecnie jednym z niezbędnych elementem związanych z funkcjonowaniem przedsiębiorstw na rynku. Na poziomie krajowym utworzenie Komitetu Technicznego ds. Sztucznej Inteligencji (KT) przy Polskim Komitecie Normalizacyjnym w 2023 r.[4] pokazuje rosnące znaczenie standaryzacji. Komitet ten ma na celu opracowanie i kształtowanie

[1] Organisation for Economic Co-operation and Development (OECD), https://www.oecd.org/about/ [dostęp: 18.07.2024].

[2] International Organization for Standardization (ISO), https://www.iso.org/home.html [dostęp: 18.07.2024].

[3] Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020, https://tinyurl.com/5euyhtbv [dostęp: 18.07.2024].

[4] Wiadomości PKN. Normalizacja 12/2023, https://tinyurl.com/2naa6knd [dostęp: 18.07.2024].

w Polsce normalizacji, zapewniającej rozwój godnych zaufania systemów AI, które szanują podstawowe wartości i prawa człowieka. Centralnym elementem strategii KT jest harmonizacja z normami europejskimi, co stanowi punkt wyjścia do skutecznej integracji z rynkiem europejskim i ułatwienie szerszej interoperacyjności.

Warto zauważyć, że prawo UE w zakresie nowych technologii, w tym AI, dynamicznie się rozwija, aby stymulować innowacje przy jednoczesnym zapewnieniu ochrony prawnej i etycznej. Ważne jest zrozumienie wyzwań związanych z ochroną prywatności, odpowiedzialnością, etyką, przejrzystością, własnością intelektualną, bezpieczeństwem, wpływem na rynek pracy, dostępnością oraz nierównościami, współpracą międzynarodową oraz standardami i certyfikacją.

Metodologia badania

Punktami wyjścia do analizy zgodności były takie elementy, jak definicja, taksonomia oraz cechy AI. Posłużyły one do określenia ram (zakresu i kontekstu), w jakich należy przeprowadzić analizę zgodności. Definicja AI pozwala na wstępne określenie tego, czy jakiś system może być kwalifikowany jako system AI i w związku z tym, czy będzie on podlegał regulacjom prawnym. Taksonomia określa rodzaj użytego algorytmu, przez co umożliwia bardziej precyzyjne wyodrębnienie z przepisów prawa (lecz nie tylko) wymagań ze względu na związane z danym algorytmem lub jego zastosowaniem ryzyka. Cechy takie jak uczciwość, przejrzystość, interpretowalność, solidność, prywatność i bezpieczeństwo są istotne prawnie i wpływają na projektowanie, tworzenie i wdrażanie systemów AI, tak aby na końcu zapewnić zgodność z przepisami prawa. Aktualnie definicja legalna AI została wprowadzona przez akt w sprawie sztucznej inteligencji. Definicja ta określa system AI jako „system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne”[5]. Takie podejście jest typo-

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), Tekst mający znaczenie dla EOG, Dz. U. UE L 2024.1689 z dnia 2024.07.12.

we dla definicji operacyjnych[6], które koncentrują się na praktycznym zastosowaniu i wynikach działania określonego terminu lub koncepcji, umożliwiając ich przełożenie na konkretne i mierzalne wskaźniki. To podejście jest również uzasadnione ze względu na przyjęte przez ustawodawcę europejskiego w akcie w sprawie sztucznej inteligencji podejścia opartego na ryzyku (ang. *risk-based approach*). Podejście takie, przyjmowane w stosunku do produktów i usług, które wykorzystują sztuczną inteligencję, skupia się bowiem na regulacji jej zastosowań, a nie na ściśle na samej technologii. I tak ustawodawca europejski przyjmuje jako swój cel i skupia się na ochronie demokracji, praworządności i praw podstawowych przy jednoczesnym zachęcaniu do inwestycji i innowacji.

Badanie zgodności systemów AI z prawem europejskim wymaga również odwołania się do dogmatyki prawa[7], która odgrywa istotną rolę w analizie i interpretacji prawa. Dogmatyka prawa angażuje się w analizę aparatu pojęciowego, systematyzację i rozwiązywanie zagadnień doktrynalnych wykładni i stosowania prawa. W obszarze AI dogmatyka prawa poszerza zakres stosowanych metod o metody empiryczne[8], co pozwala na głębsze zrozumienie dynamiki między prawem a społeczeństwem i wpływu prawa na jego adresatów. Dynamicznie zmieniające się środowisko wymaga elastyczności prawa wprowadzanej przez dogmatykę właśnie. W kontekście niniejszego artykułu analiza wpływu standardów i zaleceń dotyczących AI na ocenę skuteczności prawa była kluczowa w związku z określeniem ram audytu zgodności. Zastosowanie metody empirycznej i analizy danych obejmowało, w zakresie systemów AI, zasady dotyczące projektowania, rozwoju, wdrażania i utrzymywania, cechy charakterystyczne, regulacje prawne oraz ocenę zastosowania definicji legalnej AI w przepisach prawa. Do analizy wykorzystano wykładnię dynamiczną prawa, część wykładni funkcjonalnej, która zapewnia adekwatność norm prawnych do sytuacji społeczno-politycznej i oceny społecznej w czasie interpretacji prawa[9]. Dynamiczna wykładnia pozwala prawu nadążać za zmianami, osiągając cele ustawodawcy szybciej niż poprzez zmiany legislacyjne[10]. Stosowanie dynamicznej interpretacji prawa, szczególnie w kontekście AI, pozwala na uwzględnienie unikalnych cech AI, takich jak autonomia, zdolność uczenia się i adaptacji,

---

[6] Encyklopedia Zarządzania, https://tinyurl.com/mr2cxhmb [dostęp: 18.07.2024].

[7] J. Zajadło, *Leksykon współczesnej teorii i filozofii prawa*, Warszawa 2017, s. 37–39.

[8] *Badanie empiryczne: Definicja, metody i przykłady*, https://tinyurl.com/2p9wn5tf [dostęp: 18.07.2024].

[9] J. Wróblewski, S. Ehrlich (red.), *Teoria państwa i prawa*, cz. VI: *Wykładnia prawa*, Warszawa 1960, s. 23.

[10] *Ibidem*, s. 23–24.

oraz wyzwań etycznych i prawnych związanych z AI. Prawodawstwo UE musi być elastyczne i zdolne do adaptacji do ciągłych zmian technologicznych, aby zapewnić bezpieczeństwo i ochronę praw obywateli.

Audyt zgodności systemów samouczących się

Z punktu widzenia omawianej analizy zgodności istotne jest rozróżnienie między oprogramowaniem komputerowym a systemem komputerowym. Przyjęto, że system komputerowy jest pojęciem szerszym. Analogicznie przyjęto, że system samouczący się składa się z algorytmów, czyli też jest pojęciem szerszym. Algorytmy są częściami, z których zbudowany jest system samouczący się, umożliwiającymi osiągnięcie określonej predykcji (rezultatu działania szerzej) na podstawie dostarczonych danych. W ujęciu historycznym zastosowanie algorytmów należy rozumieć jako zastosowanie statycznych schematów działań prowadzących do poprawnych rozwiązań, w odróżnieniu od ich współczesnego wykorzystania w systemach AI, gdzie algorytmy dynamicznie uczą się na podstawie dostarczonych danych. Model w AI jest wynikiem użycia algorytmu uczenia maszynowego i zestawu danych wejściowych, reprezentującym wiedzę nabytą przez ten model w tym procesie[11]. Proces tworzenia systemów samouczących się powinien opierać się na najlepszych praktykach stosowanych w tworzeniu oprogramowania i systemów komputerowych, a także być weryfikowany w ramach audytu zgodności. Przykładowo, w porównaniu do wcześniejszych rodzajów algorytmów algorytmy AI są trudniej wyjaśnialne, ponieważ reguły ich działania są odkrywane przez takie algorytmy w procesie uczenia, a nie są bezpośrednio ustalane przez jego twórcę[12]. W pewnym uproszczeniu za kluczowe pojęcia związane z wykorzystaniem systemu AI można przyjąć dane, model oraz proces jego rozwoju[13]. Przykładowo dane wejściowe o niskiej jakości mogą prowadzić do błędnych decyzji modelu, co podkreśla znaczenie procesu ich odpowiedniego przygotowania.

Rola i znaczenie AI (w tym algorytmów i systemów samouczących się) w kontekście oddziaływania na technologie, które wpływają na rozmaite aspekty życia, są

[11] M. Świerczyński, Z. Więckowski, *Sztuczna Inteligencja w prawie międzynarodowym*, Warszawa 2021, s. 43.

[12] W. Samek (red.), *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020. Springer*, Cham 2022, s. 13–15.

[13] A. Koshiyama, E. Kazim, P. Treleaven, *Algorithm Auditing: Managing the Legal, Ethical, and Technological Risks of Artificial Intelligence, Machine Learning, and Associated Algorithms*, The IEEE Computer Society, April 2022, s. 42.

coraz większe. Rodzą się zatem pytania dotyczące zgodności z prawem, etyki i solidności takich rozwiązań[14]. W odpowiedzi na te kwestie UE zaproponowała ramy prawne dotyczące godnej zaufania AI[15] (ang. *Trustworthy AI*), podkreślające wspomniane wcześniej poszanowanie prawa, zgodność z zasadami etycznymi i solidność – zarówno z technicznego, jak i ze społecznego punktu widzenia, ponieważ systemy AI mogą wywoływać niezamierzone szkody nawet wówczas, gdy korzysta się z nich w dobrej wierze. Wymagane jest, aby wszystkie te cechy współwystępowały, a konflikty między nimi były rozwiązywane w zależności od sytuacji, co ma prowadzić do wprowadzenia do użytku odpowiedzialnych i zrównoważonych innowacyjnych rozwiązań AI w UE. Etyka jest kluczowym filarem oceny zgodności algorytmów, z naciskiem na ochronę praw człowieka, prywatności i minimalizację ryzyka działań szkodliwych algorytmów.

Algorytmy jako synonim cyfrowej rewolucji będą coraz częściej działać samodzielnie z minimalnym nadzorem człowieka, co dostrzegła OECD.AI Policy Observatory w swojej koncepcji „Big Algo". Zastosowano tutaj metodologię „5V"[16] (pięć kluczowych cech z ang. *velocity*, *volume*, *value*, *variety*, *veracity*) obejmującą prędkość, wielkość, wartość, różnorodność i prawdziwość, które odnoszą się do cech algorytmów, takich jak podejmowanie decyzji w czasie rzeczywistym przy minimalnej interwencji człowieka, wzrost liczby algorytmów i ich wzajemna interakcja, pojawienie się nowych usług, źródeł przychodu i branż, zastosowanie w szeroki zakresie oraz kluczowe aspekty, takie jak wiarygodność, legalność, uczciwość, dokładność i zgodność z przepisami jako cechy krytyczne.

Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji[17] (ang. HLEG AI) opracowała wytyczne dotyczące godnej zaufania AI, które obejmują siedem wymogów[18]: przewodnią rolę człowieka[19], solidność techniczną i bezpieczeństwo, ochronę prywatności, przejrzystość, różnorodność i sprawiedliwość, dobrostan społeczny i środowiskowy oraz odpowiedzialność. Zastosowanie odpowiednich metod oraz wspieranie badań naukowych mają na celu zapewnienie zgodności z tymi wymo-

---

[14] High-Level Expert Group on Artificial Intelligence, *Ethics guidelines for Trustworthy AI*, *passim*.

[15] A. Keller, C. Martins Pereira, M. Lucas Pires, *The European Union's Approach to Artificial Intelligence and the Challenge of Financial Systemic Risk*, [w:] H. Antunes *et al.*, *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Cham 2024, s. 426–428; H. Sheikh, C. Prins, E. Schrijvers, *Mission AI. The New System Technology*, Cham 2023, s. 64–65.

[16] TechTarget, Data Management, 5V's of big data, http://tinyurl.com/23fky6mj [dostęp: 18.07.2024].

[17] P.U. Lima, A. Paiva, *Autonomous and Intelligent Robots: Social, Legal and Ethical Issues*, [w:] H. Antunes *et al.*, *op. cit.*, s. 135–136.

[18] High-Level Expert Group on Artificial Intelligence, *op. cit*., *passim*.

[19] U. Pagallo, *Dismantling Four Myths in AI & EU Law Through Legal Information 'About' Reality*, [w:] H. Antunes *et al.*, *op. cit.*, s. 256–260.

gami. Ważne jest również transparentne informowanie osób zainteresowanych oraz angażowanie ich w cały cykl życia systemu AI. Wspomniana grupa ekspertów przedstawiła listę kontrolną oceny godnej zaufania AI, bazującą na środkach współregulacyjnych, która ma na celu zapewnienie odpowiedniego stosowania przedstawionych wymogów. Zgodność z listą kontrolną nie jest jednak dowodem na zgodność z prawem samym w sobie, a jedynie istotnym wnioskiem (wynika z korelacji zakresu badania na podstawie listy kontrolnej z wymaganiami prawa) z przeprowadzenia audytu zgodności systemu AI, który w dalszej części kompletnego procesu oceny zgodności (np. na podstawie procedury zawartej w akcie w sprawie sztucznej inteligencji) będzie miał istotny wpływ na uzyskanie tym razem wiążącego prawnie potwierdzenia zgodności systemu AI z wymogami prawa UE. Odpowiedzialność za zgodność systemów AI przypisuje się również ramom zarządzania w organizacjach, które powinny ustanowić odpowiednie metody zarządzania eliminujące związane z nimi zagrożenia.

Audyt algorytmów[20] obejmuje cały cykl rozwoju systemu AI, minimalizując ryzyko i zapewniając zgodność z prawem, etyką i solidność. Proces ten, analogiczny do inżynierii oprogramowania, powinien zostać rozbudowany o kluczowe cechy AI, takie jak uczciwość[21], wyjaśnialność[22], solidność[23] i prywatność[24]. Kluczowe cechy odnoszą się do zapewnienia zrozumienia działania algorytmów, odporności na ataki, minimalizacji stronniczości oraz zgodności z zasadami prywatności i RODO. Szczególną rolę w audycie odgrywają dane, będące podstawą budowy modeli AI, co wymaga dalszego omówienia zagadnień etyki danych oraz nadzoru nad nimi. Audyt algorytmów AI jest niezbędny dla zapewnienia, że algorytmy są legalne, etyczne i bezpieczne, co ma znaczenie dla późniejszej odpowiedzialności za ich skutki. Analogicznie do np. audytu finansowego algorytmy AI powinny być poddawane rzetelnym audytom przez certyfikowane podmioty. Wspomniane już kluczowe cechy algorytmów AI muszą być uwzględnione na wszystkich etapach tworzenia i oceny systemów AI. Proces audytu powinien obejmować wszystkie etapy od tworzenia do eksploatacji systemu AI, a jego zakres powinien być dostosowany do specyfiki zastosowania danego systemu AI i związanych z tym ryzyk oraz wynikających z tego łącznie wymagań prawnych[25].

---

[20] E. Magrani, P. Guedes Fernandes da Silva, *The Ethical and Legal Challenges of Recommender Systems Driven by Artificial Intelligence*, [w:] H. Antunes *et al.*, *op. cit.*, s. 157.

[21] W. Samek (red.), *op. cit.*, s. 377–378.

[22] *Ibidem*, s. 378–379.

[23] A. Kucharavy, O. Plancherel, V. Mulder *et al*., *Large Language Models in Cybersecurity. Threats, Exposure and Mitigation*, Cham 2024, s. 181–186.

[24] D. Hirsch, T. Bartley, A. Chandrasekaran et al., *Business Data Ethics. Emerging Models for Governing AI and Advanced Analytics*, Cham 2024, s. 84–86.

[25] H. Sheikh, C. Prins, E. Schrijvers, *op. cit.*, s. 370–372.

W zakresie audytu zgodności poddano analizie podejście zaproponowane przez A. Koshiyame, E. Kazima i P. Treleavena[26], w którym wyróżnili cztery główne procesy audytu: rozwój, ocenę, łagodzenie i zapewnienie zgodności. Obejmują one zarządzanie i implementację[27], które są kluczowe dla kontrolowanego tworzenia modeli algorytmicznych[28]. Modele typu *black-box* i *white-box* różnią się poziomem interpretowalności[29], co ma znaczenie dla audytu[30] i zgodności z przepisami.

Uzupełnieniem przyjętego podejścia do audytu zgodności było również poddanie analizie podejścia zaproponowanego przez R. Akule i I. Garibayego[31]. Zaproponowali oni siedem poziomów audytu, od dostępu do procesu, przez dostęp do modelu typu *black-box*, danych wejściowych, rezultatów – dostęp typu *gray-box*, manipulacji parametrami, celów uczenia, aż po pełny dostęp typu *white-box*. Im wyższy poziom kontroli, tym bardziej szczegółowy i dokładny jest audyt, co jest szczególnie ważne dla systemów AI o wysokim ryzyku. Jest to bardzo praktyczne podejście do oceny działania systemów AI, które z natury wynikającej ze specyfiki algorytmów AI są trudno wyjaśnialne lub nawet niewyjaśnialne.

Podczas audytu należy zwrócić szczególną uwagę na przejrzystość i interpretowalność algorytmu, wydajność, solidność, unikanie uprzedzeń i dyskryminacji, prywatność oraz odpowiedzialność za skutki działania systemu AI. Zidentyfikowane problemy i ryzyka muszą być odpowiednio łagodzone już w trakcie procesu rozwoju takich systemów AI, aby obniżyć ryzyko błędnego działania modelu algorytmicznego. Po zakończonym audycie i wdrożeniu działań łagodzących można stwierdzić, że system AI spełnia wymogi etyczne, regulacyjne i prawne (przy założeniu prawidłowego zebrania wymagań w tym zakresie i ich właściwej implementacji, co audyt tylko stwierdza).

Przypomnieć należy, że spełnienie wymagań w ramach przeprowadzonego audytu nie jest dowodem na zgodność z prawem samym w sobie, a jedynie istotnym wnioskiem z przeprowadzenia audytu zgodności systemu AI.

---

[26] A. Koshiyama, E. Kazim, P. Treleaven, *op. cit.*, s. 42.

[27] A. Shajek, E.A. Hartmann, *New Digital Work. Digital Sovereignty at the Workplace*, Cham 2023, s. 135–147.

[28] T. Winkle, *Product Development within Artificial Intelligence, Ethics and Legal Risk*, Wiesbaden 2022, s. 139–140.

[29] W. Samek (red.), *op. cit.*, s. 387–388.

[30] T. Winkle, *op. cit.*, s. 139–140.

[31] R. Akula, I. Garibay, *Audit and Assurance of AI Algorithms*: *A framework to ensure ethical algorithmic practices in Artificial Intelligence*, https://arxiv.org/abs/2107.14046 [dostęp: 18.07.2024].

Przegląd regulacji prawnych dotyczących systemów AI w Unii Europejskiej

W zakresie regulacji prawnych Parlament Europejski zwrócił uwagę na wpływ technologii AI na społeczeństwo, podkreślając konieczność tworzenia ram prawnych[32], które zapewnią poszanowanie godności ludzkiej[33] i praw zawartych w Karcie praw podstawowych UE[34]. W swojej rezolucji[35] Parlament Europejski stwierdził, również na podstawie wytycznych etycznych dotyczących godnej zaufania sztucznej inteligencji przedstawionych przez grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji, że jednym z istotnych z zagrożeń dla wspomnianych ram prawnych są decyzje i wybory podejmowane przez ludzi, a które są związane z tym, w jakim kierunku będzie zmierzać rozwój AI. Stąd też potrzeba regulacji tego obszaru. Inne istotne zagrożenia związane z AI dotyczą decyzji podejmowanych względem osób wyłącznie na podstawie decyzji czy zaleceń generowanych przez te systemy. Dlatego kluczowe jest przyjęcie wytycznych dotyczących przejrzystości i interpretowalności. Wymienione wytyczne są istotne również dla rynku konsumenckiego UE i obejmują one twórców, podmioty wdrażające oraz konsumentów korzystających z systemów AI. Konsumenci często nie są świadomi, jak algorytmy AI są wykorzystywane w usługach, z których korzystają, co wynika m.in. z braku szczegółowych informacji w regulaminach korzystania tych usług. Zaufanie do dostawców usług i założenie zgodności z przepisami prawa mogą prowadzić do nieświadomości istnienia ryzyk. Profilowanie konsumentów i algorytmiczne podejmowanie decyzji mogą prowadzić do manipulacji i ich wykorzystania w sposób, którego nie są świadomi. Dlatego postulowana zgodność systemów AI z przepisami prawa ma na celu zapewnienie dostępu do adekwatnych informacji na ich temat. Nieprzejrzystość algorytmiczną można w stosunku do konsumenta podzielić na technologiczną i relacyjną. Każda z nich ogranicza zrozumienie i zaufanie do świadczonych usług za strony konsumenta oraz zwiększa przewagę drugiej strony obrotu gospodarczego. Brak poinformowania (czyli tzw. aktywnego uczestniczenia w obrocie gospodarczym)

[32] A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Berlin 2022, s. 140–142.

[33] B. Carsten Stahl, D. Schroeder, R. Rodrigues, *Ethics of Artificial Intelligence. Case Studies and Options for Addressing Ethical Challenges*, Cham 2023, s. 79–80.

[34] Karta praw podstawowych Unii Europejskiej (Dz. U. UE C 303 z 2007 r., s. 1 z późn. zm.).

[35] Rezolucja Parlamentu Europejskiego z dnia 20 stycznia 2021 r. w sprawie sztucznej inteligencji: kwestie wykładni i stosowania prawa międzynarodowego w zakresie, w jakim dotyczy ono UE, w dziedzinie zastosowań cywilnych i wojskowych oraz kwestie kompetencji państwa poza wymiarem sprawiedliwości w sprawach karnych (2020/2013(INI)) (Dz. U. UE C 456 z 2021 r., s. 34).

będzie prowadził do ograniczenia możliwości dochodzenia swoich praw poprzez brak możliwości wykazania nieuczciwego zachowania drugiej stronie, które będzie wynikało z braku wiedzy o stosowanych rozwiązaniach z omawianego zakresu.

Pierwszym aktem prawnym UE, który został podany analizie w kontekście zgodności algorytmów i systemów AI z prawem unijnym, było ogólne rozporządzenie o ochronie danych osobowych (RODO) (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679)[36]. RODO stanowi kompleksową regulację dotyczącą ochrony danych osobowych. Zostało ustanowione w celu zapewnienia ochrony prywatności osób fizycznych w związku z przetwarzaniem ich danych osobowych oraz swobodnego przepływu tych danych. W praktyce oznacza to, że po pierwsze te same przepisy o ochronie danych obowiązują wszystkie przedsiębiorstwa działające w UE, niezależnie od tego, gdzie mają siedzibę. Po drugie, wprowadzone zostały nowe obowiązki dla podmiotów przetwarzających dane osobowe, obejmujące m.in. (w omawianym aspekcie wyjaśnialności i przejrzystości, rozumianym też jako informowanie[37]) zapewnienie, że dane osobowe są przetwarzane w sposób zgodny z prawem i z poszanowaniem praw i wolności osób, których dane dotyczą, a to wszystko razem stanowi ważny krok w kierunku jeszcze lepszej ochrony prywatności. Kluczowe w ramach RODO (w omawianym zakresie) są postanowienia określające podstawę prawną przetwarzania danych oraz postanowienia, które nakładają na administratorów obowiązek informowania osób, w tym o zautomatyzowanym podejmowaniu decyzji. RODO podkreśla ochronę przed decyzjami opartymi wyłącznie na zautomatyzowanym przetwarzaniu danych, które mogą znacząco wpływać na sytuację prawną lub życiową tych osób. Przetwarzanie musi być zgodne z odpowiednimi procedurami matematycznymi i statystycznymi, zapewniać ochronę danych oraz prawa do interwencji człowieka. RODO przyznaje prawo osobom, których dane są przetwarzane, niepodlegania decyzjom opartym wyłącznie na automatycznym przetwarzaniu danych, chyba że jest to niezbędne do wykonania umowy, dozwolone prawem UE lub opiera się na zgodzie osoby. Przewidziana w RODO ocena skutków dla ochrony danych jest kluczowa w ocenie ryzyka naruszenia praw osób, których dane są przetwarzane, szczególnie w kontekście systemów AI. W komunikacie w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oce-

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z 2016 r., s. 1 z późn. zm.).

[37] W. Samek (red.), *op. cit*., s. 388–389.

ny skutków przetwarzania dla ich ochrony Prezesa UODO z 17 czerwca 2019 r.[38] wymieniono rodzaje przetwarzania danych wymagające oceny skutków ochrony danych osobowych, takie jak profilowanie, zautomatyzowane podejmowanie decyzji, przetwarzanie danych wrażliwych i biometrycznych, oraz przetwarzanie danych na dużą skalę. RODO również podkreśla konieczność dokonywania oceny skutków w przypadkach systematycznej oceny czynników osobowych na podstawie profilowania lub przetwarzania szczególnych kategorii danych.

Drugim aktem poddanym analizie ze względu na przedmiot omawianej regulacji będący ściśle związanym z zakresem niniejszego artykułu był akt w sprawie sztucznej inteligencji (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689)[39]. Dotychczas nie było specyficznych przepisów dotyczących AI, a akt ten jest pierwszym tego rodzaju. W większości krajów, w tym w Polsce, przyjmowano głównie akty strategiczne (polityki), skierowane do administracji rządowej. Akt w sprawie sztucznej inteligencji ma na celu promowanie stosowania AI i zajęcie się zagrożeniami związanymi z jej zastosowaniami. Promowanie AI obejmuje m.in. uwzględnienie interesów drobnych dostawców i użytkowników systemów AI, ochronę praw podstawowych zawartych w Karcie praw podstawowych UE, tworzenie piaskownic regulacyjnych, promowanie godnej zaufania AI zgodnej z unijnymi wartościami oraz innowacji opartych na AI. Według UE zagrożenia związane z używaniem AI mogą być zredukowane przez wprowadzenie określonych ram prawnych dotyczących godnej zaufania AI, co zwiększy zaufanie obywateli oraz zachęci przedsiębiorców do jej opracowywania. UE ustawiła cele szczegółowe, takie jak zapewnienie bezpieczeństwa i zgodności systemów AI z prawem oraz unijnymi wartościami, zapewnienie pewności prawa, poprawa zarządzania i skuteczne egzekwowanie przepisów, ułatwienie rozwoju jednolitego rynku zgodnych z prawem, bezpiecznych i wiarygodnych zastosowań AI oraz zapobieganie fragmentacji rynku. W akcie w sprawie sztucznej inteligencji zastosowano podejście oparte na analizie ryzyka[40], które dzieli systemy AI na systemy o niedopuszczalnym, wysokim, niskim lub minimalnym ryzyku. W zależności od poziomu ryzyka systemy AI muszą spełniać odpowiednie wymaga-

[38] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. z 2019 r. poz. 666).

[39] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). Tekst mający znaczenie dla EOG (Dz. U. UE L z 2024 r. poz. 1689).

[40] A. Mantelero, *op. cit.*, s. 13–15.

nia. Zakazane są m.in. techniki podprogowe i manipulacyjne oraz klasyfikacja osób na podstawie ich zachowania społecznego (system *scoringu* obywateli). Systemy AI stwarzające wysokie ryzyko obejmują m.in. biometrię, infrastrukturę krytyczną, edukację, zatrudnienie, dostęp do usług prawnych, ściganie przestępstw, zarządzanie migracją, azylem i kontrolą graniczną oraz wymiar sprawiedliwości. Akt nakłada na dostawców obowiązek zapewnienia zgodności produktów z wymogami oraz przygotowania dokumentacji systemu AI. Przewiduje również obowiązek ustanowienia systemu zarządzania ryzykiem dla systemów wysokiego ryzyka, który towarzyszy systemowi w całym cyklu życia. W akcie w sprawie sztucznej inteligencji uregulowano także kwestie związane z danymi i zarządzaniem danymi, w tym trenowaniem modeli oraz ochroną danych osobowych. Kolejnym wymogiem jest zbudowanie technicznych możliwości automatycznego rejestrowania zdarzeń w systemy AI wysokiego ryzyka. Akt kładzie nacisk na przejrzystość działania systemów AI oraz zapewnienie, że osoby fizyczne są świadome interakcji z systemami AI. Wprowadzono również wymóg dołączenia instrukcji obsługi do systemów AI wysokiego ryzyka, zawierającej informacje na temat cech, możliwości i ograniczeń systemu. Nadzór ze strony człowieka nad systemami AI wysokiego ryzyka jest kluczowy. Akt wymaga, aby systemy AI były projektowane z uwzględnieniem narzędzi interfejsu człowiek–maszyna, umożliwiających skuteczny nadzór i reagowanie na ryzyko. Istotne jest także zapewnienie solidności systemów AI, które powinny osiągać odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa. Procedura oceny zgodności dla systemów AI wysokiego ryzyka obejmuje badanie zgodności z wymogami aktu, analizę dokumentacji technicznej oraz zgodność procesów projektowania, opracowywania i monitorowania systemu. Oceny dokonuje jednostka notyfikowana, która wydaje unijny certyfikat oceny dokumentacji technicznej. Akt nakłada również obowiązek rejestracji systemów AI wysokiego ryzyka w unijnej bazie danych. Systemy niemające certyfikatu i niezarejestrowane nie mogą być wdrożone produkcyjnie. Oprócz systemów wysokiego ryzyka akt reguluje również inne systemy AI, wymagając m.in. informowania osób fizycznych o interakcji z systemami AI oraz oznaczania treści generowanych przez AI[41]. Akt w sprawie sztucznej inteligencji obejmuje także modele AI ogólnego przeznaczenia, wprowadzając wymogi dotyczące transparentności, bezpieczeństwa i odpowiedzialności, w celu przeciwdziałania ryzyku systemowemu, które te modele mogą wprowadzać. Ryzyko systemowe[42]

[41] D. Durães, P. Miguel Freitas, P. Novais, *The Relevance of Deepfakes in the Administration of Criminal Justice*, [w:] H. Antunes *et al.*, *op. cit.*, s. 352–354.

[42] M. Lanz, S. Mijic., *Risks Associated with the Use of Natural Language Generation: Swiss Civil Liability Law Perspective*, [w:] H. Antunes *et al.*, *op. cit.*, s. 325–326.

oznacza ryzyko, które jest charakterystyczne dla modeli AI ogólnego przeznaczenia mających zdolności dużego oddziaływania i ma znaczący wpływ na rynek UE ze względu na zasięg tych modeli lub rzeczywiste lub racjonalnie przewidywalne negatywne skutki dla zdrowia publicznego, porządku publicznego, bezpieczeństwa publicznego, praw podstawowych lub całego społeczeństwa, mogące rozprzestrzenić się na dużą skalę w całym łańcuchu wartości. Dostawcy modeli z ryzykiem systemowym muszą przeprowadzać zaawansowane oceny modeli oraz współpracować z Komisją UE i organami krajowymi.

Trzecim aktem odnoszącym się do omawianych wymagań prawnych w zakresie zapewnienia zgodności był akt w sprawie maszyn (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230)[43]. W treści aktu znaleźć można regulacje odnoszące się do systemów AI. Regulacje te koncentrują się na zapewnieniu jednolitych zasad ochrony zdrowia i bezpieczeństwa, w związku z zagrożeniami, jakie mogą zostać dodatkowo wprowadzane przez systemy AI. Rozporządzenie wskazuje na wzrost liczby zaawansowanych, autonomicznych maszyn, które mogą się uczyć i adaptować, co wymaga dodatkowych zabezpieczeń związanych z nowymi technologiami cyfrowymi. Podejście to opiera się na analizie ryzyka wynikającego z algorytmów i systemów samouczących się, których zastosowanie może prowadzić do zmian w zachowaniu maszyn. Kluczowe jest zapewnienie, że funkcje bezpieczeństwa tych maszyn pozostaną skuteczne. Rozporządzenie przede wszystkim podkreśla znaczenie zgodności z prawem i solidności technologicznej, pozostawiając bezpośrednie odniesienia do etyki z uwagi na jego techniczny charakter. Wymogi dotyczące ochrony zdrowia i bezpieczeństwa muszą być spełniane od etapu projektowania maszyn, przez ich produkcję, aż po wprowadzenie na rynek. Celem jest ochrona zdrowia konsumentów, użytkowników profesjonalnych, zwierząt domowych, mienia oraz środowiska. Dokumentacja techniczna musi zapewniać zgodność maszyny z przepisami, a maszyna musi być oznakowana certyfikatem CE po ocenie zgodności. Rozporządzenie przewiduje szczegółowe procedury oceny zgodności, które mają na celu eliminację zagrożeń lub ich minimalizację poprzez projektowanie maszyn zgodnie z wynikami oceny ryzyka. Systemy AI w maszynach muszą być testowane, aby sprawdzić i zapewnić przewidywalność ich zachowań, a ich specyfikacje włączone do dokumentacji technicznej maszyny. Szczególną uwagę zwraca się na układy sterowania, które muszą zapobiegać sytuacjom zagrożenia, oraz

[43] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylenia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG (Dz. U. UE L 165 z 2023 r., s. 1 z późn. zm.).

na funkcję zatrzymania awaryjnego, która musi być dostępna i skuteczna w każdej chwili, niezależnie od trybu pracy.

Ostatnim analizowanym aktem prawnym jest dyrektywa NIS 2 (dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555)[44], która nowelizuje dyrektywę NIS, mającą na celu budowanie zdolności w zakresie cyberbezpieczeństwa w UE oraz łagodzenie zagrożeń dla systemów informatycznych kluczowych dla świadczenia usług. Przegląd dyrektywy wykazał, że przyczyniła się ona do zmian w podejściu do cyberbezpieczeństwa, tworząc krajowe ramy bezpieczeństwa i wspierając współpracę na poziomie UE. Wraz z postępem cyfrowym zwiększyła się częstotliwość incydentów bezpieczeństwa, co skłoniło UE do rozszerzenia ram współpracy i obowiązków związanych z dyrektywą. Dyrektywa NIS 2 określa minimalne przepisy dla państw członkowskich, mające na celu ograniczenie ryzyka incydentów cyberbezpieczeństwa i zwiększenie bezpieczeństwa obywateli oraz przedsiębiorstw. Nowelizacja obejmuje zmiany podmiotowe, zarządzania i bezpieczeństwa, odpowiedzialności osób kierujących oraz rozszerza współpracę międzynarodową. Rozszerzono zakres stosowania dyrektywy, wprowadzając nowe kategorie podmiotów oraz kryteria wielkości przedsiębiorstwa. W zakresie zarządzania i bezpieczeństwa dyrektywa nakłada większe wymagania dotyczące zarządzania, ujawniania podatności, testowania poziomu cyberbezpieczeństwa oraz stosowania szyfrowania i uwierzytelniania wieloskładnikowego. Podkreśla także analizę ryzyka w łańcuchu dostaw, w tym ryzyka związanego z algorytmami i systemami samouczącymi się. Dyrektywa precyzuje procedury raportowania incydentów oraz odpowiedzialność osób kierujących podmiotami za naruszenie obowiązków. Choć dyrektywa NIS 2 nie reguluje bezpośrednio algorytmów i systemów samouczących się, jej celem jest zwrócenie uwagi na zgodność rozwoju systemów AI z wymogami bezpieczeństwa. Analiza ryzyka powinna uwzględniać ryzyka związane z AI, zgodnie postanowieniem dyrektywy, które wymaga od podmiotów wdrażania odpowiednich środków technicznych, operacyjnych i organizacyjnych dla zarządzania ryzykiem. Dyrektywa NIS 2 zachęca do stosowania europejskich i międzynarodowych norm bezpieczeństwa, takich jak ISO 27001 i ISO 27002. Dyrektywa ta również wskazuje na możliwość integracji technologii poprawiających cyberbezpieczeństwo, takich jak systemy oparte na AI lub uczeniu maszynowym, które powinny być objęte analizą ryzyka.

---

[44] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE L 333 z 2022 r., s. 80).

Regulacje prawne w zakresie systemów AI, zarówno unijne, jak i krajowe, są uzupełniane przez międzynarodowe standardy, takie jak te tworzone przez ISO. Przykładem jest norma ISO/IEC 42001[45], która koncentruje się na zarządzaniu systemami AI i ich zgodności z zasadami godnej zaufania AI. Zgodnie z tą normą organizacje muszą odpowiedzialnie podejść do wykorzystania AI, zapewniając przejrzystość, wyjaśnialność decyzji oraz zarządzanie ryzykiem związanym z ciągłym uczeniem się tych systemów. Normy systemu zarządzania sztuczną inteligencją (SZSI) obejmują ustanowienie, wdrożenie, utrzymanie i doskonalenie systemu zarządzania AI, koncentrując się na specyficznych cechach AI, takich jak zdolność do ciągłego uczenia się. Wprowadzenie SZSI powinno być poprzedzone przede wszystkim prawidłowo przeprowadzoną analizą ryzyka, kontekstu organizacji, jak również oceną potrzeb zainteresowanych stron. System zarządzania AI musi być zintegrowany z procesami organizacji i ogólną strukturą zarządzania. Procesy zarządzania powinny obejmować spełnienie wymagań godnej zaufania AI, takich jak zgodność z prawem, etyka i solidność, przez cały cykl życia systemów AI. Szczególną uwagę należy poświęcić zarządzaniu dostawcami i partnerami, którzy rozwijają systemy AI. Spełnienie wymagań normy SZSI pozwala organizacji wygenerować dowody swojej odpowiedzialności i rozliczalności za działania AI, co jest wymagane przez akty prawa dotyczące AI w zakresie, w jakim zostało to zasygnalizowane wcześniej w niniejszym artykule. Wymagania normy obejmują ustanowienie procesów oceny ryzyka, zarządzania cyklem życia systemów AI, zarządzania danymi, informowania użytkowników oraz oceny wpływu systemów AI na jednostki i społeczeństwo. Organizacje muszą dokumentować te procesy, monitorować je i przeprowadzać okresowe przeglądy, aby dostosować je do zmieniającego się kontekstu organizacji. Cele związane z AI, takie jak wydajność, bezpieczeństwo, etyka i zgodność z prawem, powinny być zdefiniowane dla różnych obszarów i poziomów organizacji. Istotne jest, aby dla wymagań określonych przez normę oraz celów związanych z AI stosować środki zabezpieczające wymienione w załącznikach do normy w sposób i w zakresie tam wskazanym. Wyróżnić można takie środki, jak zarządzanie danymi, cykl życia systemu, ocena wpływu i informowanie użytkowników, które mają na celu ustanowienie kompleksowych ram SZSI, które zapewnią etyczne wykorzystanie AI, zarządzanie ryzykiem i wspieranie innowacji w ustrukturyzowanych ramach.

[45] ISO/IEC 42001:2023, *Information technology – Artificial intelligence – Management system*, https://www.iso.org/standard/81230.html [dostęp: 18.07.2024].

Podsumowanie

Zgodność algorytmów i systemów samouczących się (systemów AI) z prawem UE jest złożonym zagadnieniem, wymagającym sformalizowanego i technicznego podejścia. Chociaż dopiero pojawiła się legalna definicja AI, to używane już wcześniej definicje stworzone przez międzynarodowe organizacje podkreślały zdolność do uczenia się i adaptacji jako różnice odróżniając AI od wcześniejszych systemów. Specyficzność AI, wynikająca z możliwości przetwarzania różnorodnych danych i szerokiego zakresu zastosowań, stwarza ryzyka (rozumiane jako zagrożenia), które mogą naruszać prawa jednostek i społeczeństwa. Z tego powodu zgodność powinna opierać się na aspektach prawnych, etycznych i technicznych. Pojęcie godnej zaufania AI, obejmujące zgodność z prawem, etyczność i solidność, jest kluczowe dla analizy zgodności AI. Systemy AI to także szanse (pozytywne ryzyko), dlatego należy zauważyć, że analizowane akty prawne wspierają rozwój innowacyjności. Ramy prawne wprowadzane przez te akty wyznaczają minimalne wymogi, które mają na celu zminimalizowanie zagrożeń (negatywne ryzyko) i problemów związanych z AI, jednocześnie nie utrudniając nadmiernie rozwoju technologii ani nie zwiększając kosztów.

W analizach odwołano się do dogmatyki prawa i wykorzystania metod empirycznych do badania relacji między prawem a AI. Ważne jest dynamiczne interpretowanie przepisów prawa z uwzględnieniem cech AI, takich jak autonomia, adaptacja i zdolność uczenia się. Kluczowe jest również rozważenie wyzwań etycznych i prawnych, takich jak odpowiedzialność za decyzje AI, ochrona danych osobowych oraz praw autorskich.

Analiza zgodności AI może opierać się na praktykach stosowanych przy ocenie jakości wytwarzania i bezpieczeństwa systemów komputerowych. Ważne jest przeprowadzenie audytu procesu wytwarzania systemów AI, uwzględniającego specyficzne wymagania techniczne i operacyjne. W analizie zgodności algorytmów AI odniesiono się do kilku wybranych aktów prawa UE, takich jak rozporządzenie o ochronie danych, rozporządzenie w sprawie sztucznej inteligencji, rozporządzenie w sprawie maszyn i dyrektywa NIS 2. Na przykładzie tych aktów wykazano występowanie wymagań takich jak przejrzystość, interpretowalność (wyjaśnialność), solidność, etyczność, ochrona praw osób, ocena ryzyka, bezpieczeństwo, raportowanie incydentów, formalna ocena zgodności, a następnie przeanalizowano ich wpływ na analizowane zagadnienie zgodności w ujęciu szerszym, biorącym pod uwagę aspekty praktyczne jego zorganizowania w przedsiębiorstwie przy udziale norm

współregulujących. W artykule podkreślono bardzo wyraźnie znaczenie współregulacji, odwołując się do standardów międzynarodowych, takich jak normy ISO, które wpływają na definicje i procedury przyjmowane przez akty prawne. Omówiona norma ISO 42001 ma kluczowe znaczenie dla zarządzania AI w przedsiębiorstwach, minimalizując ryzyka związane z zastosowaniem AI. Norma ta opisuje sekwencję działań, prowadzących od analizy stanu faktycznego do wprowadzenia udokumentowanych środków, które mogą być źródłem oceny przez audyt. Omawiana norma może pomóc przedsiębiorstwom w odpowiedzialnym tworzeniu, wykorzystywaniu i monitorowaniu systemów AI. Skupia się ona na zarządzaniu specyficznymi ryzykami związanymi z AI, przejrzystością procesów decyzyjnych, etyką oraz ciągłym uczeniem się i adaptacją systemów AI. Dokumentacja procesów, spełnianie wymagań etycznych i prawnych oraz zarządzanie interakcjami z dostawcami są kluczowe dla odpowiedzialności i rozliczalności w zakresie systemów AI.

Bibliografia

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. U. UE L 172 z 2019 r., s. 56).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE L 333, z 2022 r., s. 80).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE L 194 z 2016 r., s. 1).

Karta praw podstawowych Unii Europejskiej (Dz. U. UE C 303 z 2007 r., s. 1 z późn. zm.).

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. z 2019 r. poz. 666).

Rezolucja Parlamentu Europejskiego z dnia 20 stycznia 2021 r. w sprawie sztucznej inteligencji: kwestie wykładni i stosowania prawa międzynarodowego w zakresie, w jakim dotyczy ono UE, w dziedzinie zastosowań cywilnych i wojskowych oraz kwestie kompetencji państwa poza wymiarem sprawiedliwości w sprawach karnych (2020/2013(INI)) (Dz. U. UE C 456 z 2021 r., s. 34).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz. U. UE L 152 z 2022 r., s. 1 z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1230 z dnia 14 czerwca 2023 r. w sprawie maszyn oraz w sprawie uchylenia dyrektywy 2006/42/WE Parlamentu Europejskiego i Rady i dyrektywy Rady 73/361/EWG (Dz. U. UE L 165 z 2023 r., s. 1 z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z 2016 r., s. 1 z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) Tekst mający znaczenie dla EOG (Dz. U. UE L z 2024 r. poz. 1689).

Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" (M.P. z 2021 r. poz. 23).

Literatura

Antunes H. *et al.*, *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Cham 2024.

Banasiński C. (red.), *Cyberbezpieczeństwo: zarys wykładu*, Warszawa 2023.

Bertoni E., Fontana M., Lorenzo G. *et al.*, *Handbook of Computational Social Science for Policy*, Cham 2023.

Bieda R., Okoń Z. (red.), *Metaświat. Prawne i techniczne aspekty przełomowych technologii*, Warszawa 2022.

Brazdil P., N. van Rijn J., Soares C. *et al.*, *Metalearning. Applications to Automated Machine Learning*, wyd. 2, Cham 2022.

Carsten Stahl B., Schroeder D., Rodrigues R., *Ethics of Artificial Intelligence. Case Studies and Options for Addressing Ethical Challenges*, Cham 2023.

Chauvin T., Stawecki T., Winczorek P., *Wstęp do prawoznawstwa*, Warszawa 2019.

Chłopecki A., *Sztuczna inteligencja – szkice prawnicze i futurologiczne*, wyd. 2, Warszawa 2021.

Fischer B., Pązik A., Świerczyński M. (red.), *Prawo sztucznej inteligencji i nowych technologii*, t. 2, Warszawa 2022.

Gołaczyński J. (red.), *Prawo nowych technologii: księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, Warszawa 2022.

Hirsch D., Bartley T., Chandrasekaran A. *et al.*, *Business Data Ethics. Emerging Models for Governing AI and Advanced Analytics*, Cham 2024.

Huawei Technologies Co., Ltd., *Artificial Intelligence Technology*, Singapore 2023.

Kidyba A., Olejniczak A. (red.), *Nowoczesne technologie: szansa czy zagrożenia dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych*, Warszawa 2022.

Koshiyama A., Kazim E., Treleaven P., *Algorithm Auditing: Managing the Legal, Ethical, and Technological Risks of Artificial Intelligence, Machine Learning, and Associated Algorithms*, The IEEE Computer Society, April 2022.

Krasuski A., *Status prawny sztucznego agenta: Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021.

Krups F., *Sztuczna Inteligencja od podstaw*, Gliwice 2023.

Kucharavy A., Plancherel O., Mulder V. *et al.*, *Large Language Models in Cybersecurity. Threats, Exposure and Mitigation*, Cham 2024.

Lai L., Świerczyński M. (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.

Lee K.-F., Chen Q., *Sztuczna inteligencja 2041*, Poznań 2022.

Mantelero A., *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Berlin 2022.

Michalak A., *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021.

Morawski L., *Zasady wykładni prawa*, wyd. 2, Toruń 2010.

Piwowar K., *Technologie, które wykluczają: pomiar, dane, algorytmy*, Warszawa 2022.

Sakowska-Baryła M. (red.), *Sztuczna inteligencja – transfery odpowiedzialności i inne wyzwania ochrony danych osobowych*, Wrocław 2022.

Samek W. (red.), *xxAI – Beyond Explainable AI. International Workshop Held in Conjunction with ICML 2020*, Cham 2022.

Sitniewski P., *Otwarte dane i ponowne wykorzystanie. Przewodnik po zmianach*, Warszawa 2022.

Slama D. (red.), *The Digital Playbook. A Practitioner's Guide to Smart, Connected Products and Solutions with AIoT*, Cham 2023.

Shajek A., Hartmann E.A., *New Digital Work. Digital Sovereignty at the Workplace*, Cham 2023.

Sheikh H., Prins C., Schrijvers E., *Mission AI. The New System Technology*, Cham 2023.

Sobczak J., Chałubińska-Jentkiewicz K., Nowikowska M., *Piractwo w sieci*, Poznań 2022.

Susskind R., *Sądy internetowe i przyszłość wymiaru sprawiedliwości*, Warszawa 2021.

Szostek D. (red.), *LegalTech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym*, Warszawa 2021.

Szpor G., Wiewiórowski W.R., Gryszczyńska A. (red.), *Internet hacking*, Warszawa 2023.

Szpringer W., *Datafikacja: gospodarka oparta na danych: konkurencja a regulacja*, Warszawa 2022.

Szpringer W., *Metawersum: nowe wyzwania dla zarządzania w gospodarce cyfrowej*, Warszawa 2023.

Szpringer W., *Platformizacja gospodarki cyfrowej 5.0: nowe wyzwania dla regulacji*, Warszawa 2022.

Szpringer W., *Platformy cyfrowe i gospodarka współdzielenia: problemy instytucjonalne*, Warszawa 2020.

Szpringer W., *Zarządzanie przez algorytmy: technologia, ekonomia, prawo*, Warszawa 2020.

Szpyt K. (red.), *InsurTech: nowe technologie w branży ubezpieczeń*, Warszawa 2023.

Świerczyński M., Więckowski Z., *Sztuczna inteligencja w prawie międzynarodowym – rekomendacje wybranych rozwiązań*, Warszawa 2021.

Winkle T., *Product Development within Artificial Intelligence, Ethics and Legal Risk.*, Wiesbaden 2022.

Wróblewski J., Ehrlich S. (red.), *Wykładnia prawa*, *Teoria państwa i prawa*, cz. VI, Warszawa 1960.

Zachariasz I., *Prawo w ujęciu strukturalnym. Studium o dychotomicznym podziale prawa na prawo publiczne i prawo prywatne*, Warszawa 2016.

Zajadło J., *Leksykon współczesnej teorii i filozofii prawa*, Warszawa 2017.

Zieliński M., *Wykładnia prawa*, wyd. 6, Warszawa 2012.

Źródła internetowe

Akula R., Garibay I., *Audit and Assurance of AI Algorithms: A framework to ensure ethical algorithmic practices in Artificial Intelligence*, https://arxiv.org/abs/2107.14046 [dostęp: 18.07.2024].

Burton T., *The AI Revolution: The Road to Superintelligence*, http://tinyurl.com/2y5upsaj [dostęp: 18.07.2024].

Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *An EU Strategy on Standardisation – Setting global standards in support of a resilient, green, and digital EU single market*, https://tinyurl.com/mu5z3c6s [dostęp: 18.07.2024].

Cyfrowa dekada Europy: cele cyfrowe na 2030 r., https://tinyurl.com/yck6daen [dostęp: 18.07.2024].

Department for Science, Innovation & Technology UK, *A pro-innovation approach to AI regulation*, https://tinyurl.com/3zwrez4p [dostęp: 18.07.2024].

Encyklopedia PWN, https://encyklopedia.pwn.pl [dostęp: 18.07.2024].

Encyklopedia Zarządzania, https://mfiles.pl [dostęp: 18.07.2024].

ENISA, *Securing Machine Learning Algorithms*, https://tinyurl.com/3ub276ee [dostęp: 18.07.2024].

Ethics guidelines for Trustworthy AI, http://tinyurl.com/cc9xepb3 [dostęp: 18.07.2024].

European Committee for Standardization, https://tinyurl.com/yc7apjp3 [dostęp: 18.07.2024].

European Union Agency for Cybersecurity, https://www.enisa.europa.eu/about-enisa [dostęp: 18.07.2024].

Grochowski M., Jabłonowska A., Lagioia F. *et al.*, *Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory*, https://tinyurl.com/2y5zmjbm [dostęp: 18.07.2024].

International Association of Privacy Professionals (IAPP), *Artificial intelligence*, https://tinyurl.com/apf3tsdj [dostęp: 18.07.2024].

International Organization for Standardization (ISO), https://www.iso.org/home.html [dostęp: 18.07.2024].

ISO Strategy 2030, *Key areas of work*, https://tinyurl.com/ynuyjujt [dostęp: 18.07.2024].

ISO 14001:2015, *Environmental management systems – Requirements with guidance for use*, https://tinyurl.com/y8bpyhwu [dostęp: 18.07.2024].

ISO/IEC 27001:2022, *Information security, cybersecurity, and privacy protection – Information security management systems – Requirements*, https://tinyurl.com/p9937wym [dostęp: 18.07.2024].

ISO/IEC 42001:2023, *Information technology – Artificial intelligence – Management system*, https://tinyurl.com/mr34pd9t [dostęp: 18.07.2024].

Komisja Europejska, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, pt. „Europejska strategia w zakresie danych" Bruksela, dnia 19.02.2020 r. COM(2020) 66 final*, https://tinyurl.com/ft34h9sk [dostęp: 18.07.2024].

Komisja Europejska, *Komunikat Komisji pt. „Kształtowanie cyfrowej przyszłości Europy" COM/2020/67 final*, https://tinyurl.com/29thuure [dostęp: 18.07.2024].

Ochrona danych osobowych, http://tinyurl.com/mr28rasz [dostęp: 18.07.2024].

OECD.AI, *Krajowe polityki i strategie dotyczące sztucznej inteligencji (OECD)*, https://tinyurl.com/3szcc8ay [dostęp: 18.07.2024].

Ochrona danych w UE, http://tinyurl.com/ymvbhx23 [dostęp: 18.07.2024].

Szostek D., Załucki M. (red.), *Internet and new technologies law: perspectives and challenges*, https://tinyurl.com/xzzy8nz2 [dostęp: 18.07.2024].

TechTarget, Data Management, 5V's of big data, http://tinyurl.com/23fky6mj [dostęp: 18.07.2024].

Wielki słownik języka polskiego PAN, https://wsjp.pl [dostęp: 18.07.2023].

Zasady OECD w zakresie SI, https://oecd.ai/en/ai-principles [dostęp: 18.07.2024].

Compliance of algorithms and self-learning systems with selected aspects of European Union law

Abstract

This article addresses the challenge of ensuring that algorithms and self-learning systems – broadly understood as artificial intelligence (AI) systems – comply with European Union law. The author argues that such compliance requires a multidisciplinary approach combining legal, ethical, and technical perspectives, grounded in the concept of trustworthy AI, a principle increasingly recognized by EU legislators and international standardization bodies. The study underscores the role of legal dogmatics and dynamic interpretation in enabling the law to respond to the fast-paced development of AI technologies. It further proposes the development of a modern audit methodology adapted to the specific characteristics of AI systems, aiming to assess whether they meet legal and ethical standards of trustworthiness. Given the capacity of AI to process vast and diverse datasets, the article explores the associated risks of errors and fundamental rights infringements. Selected legal acts – including the GDPR, the AI Act, the Machinery Regulation, and the NIS 2 Directive – are analysed alongside ISO 42001, presented as a relevant co-regulatory instrument. The convergence of requirements across these frameworks is highlighted. The article concludes with practical insights into AI system design, drawing parallels with software engineering processes, and presents an audit model based on information access, transparency, and algorithmic explainability. This approach enables a reliable assessment of AI systems' legal and ethical compliance.

Keywords

algorithms, artificial intelligence, compliance of artificial intelligence with the law, AI systems compliance audit, risk management in AI systems, personal data protection, cybersecurity, international standards, transparency, explainability, interpretability, ethics, fairness, responsibility, dynamic interpretation, functional interpretation, definition of artificial intelligence