

PIOTR BURCZANIUK

Tworzenie prawa sztucznej inteligencji – wyzwania i perspektywy

Artificial Intelligence Lawmaking: Challenges and Prospects

Abstract

The discussion around artificial intelligence (AI) is currently leading the political, journalistic, technical and legal debate. This interest should come as no surprise, given that this technology is likely to underpin the ongoing process of the so-called “fourth industrial revolution”, and lead us towards strategic economic and social change. In this debate, however, theoretical and legal considerations touching on the very process of the creation of artificial intelligence law have not received a cross-cutting discussion. This paper attempts to fill this gap, building research areas for further comprehensive expansion. The topic of AI lawmaking is discussed here from three perspectives. First, vertically, by presenting the directions of legislative work carried out by the legislators of diverse subjects; second, horizontally, by analyzing the areas and issues that appear to be of regulatory relevance due to the use or imminent implementation of AI-based systems in them; and finally, third, by presenting the regulatory methods and types of legal norms that are or should be subject to legislative use in the area of IS law. These considerations have made it possible to outline the directions and foreseeable effects to which this use will lead.

KEYWORDS: artificial intelligence, AI, law-making, Artificial Intelligence

SŁOWA KLUCZOWE: sztuczna inteligencja, SI, tworzenie prawa, Akt w sprawie sztucznej inteligencji

PIOTR BURCZANIUK, doktor nauk prawnych, Uniwersytet Kardynała Stefana Wyszyńskiego, ORCID – 0000-0002-6685-8769,
e-mail: p.burczaniuk@uksw.edu.pl

1 | Wstęp

Podjęcie rozważań obejmujących zagadnienie tworzenia prawa obszaru sztucznej inteligencji (zwanej dalej też „AI”) jest zadaniem złożonym i skomplikowanym, głównie z uwagi na wieloaspektowość, co ma związek zarówno z koniecznością multigałęziowego spojrzenia badawczego, wynikającego z implikacji rozwiązań opartych o AI w obszarach regulacyjnych przyporządkowanych klasycznie do różnych gałęzi prawa, jak i podejścia multidyscyplinarnego, związanego z koniecznością odwołania się do dorobku nauk pozaprawnych, w szczególności informatycznych, ekonomicznych i socjologicznych. Pomimo zarysowanych wyzwań podjęcie analizy tego zagadnienia wydaje się szczególnie istotne z uwagi na dwa zasadnicze czynniki. Po pierwsze, opisywanego w naukach ekonomicznych, trwającego aktualnie procesu określanego nazwą „czwartej rewolucji przemysłowej” (tzw. Przemysł 4.0), utożsamianego z nowym systemem funkcjonowania organizacji produkcji, opartej o tzw. łańcuch wartości, łączący stosowanie lub używanie systemów cyber-fizycznych, internetu rzeczy i przetwarzania chmurowego^[1]. To okres swoistego przenikania się i bezpośredniego łączenia świata realnego i wirtualnego. Zjawisko to wywołuje nie tylko istotne przeobrażenia gospodarcze, ale ma i będzie mieć fundamentalne znaczenie społeczne, pozostając przez to w oczywistym zainteresowaniu nauk prawnych, dążących do realizacji podstawowej, organizacyjno-regulacyjnej funkcji prawa. Po drugie, pomimo licznych opracowań oraz trwającej debaty publicystycznej, politycznej, technicznej a zwłaszcza prawnej, poświęconej zjawisku AI, nie poruszono do tej pory, w sposób przekrojowy i kompleksowy, teoretycznoprawnych rozważań dotyczących zagadnienia kreacji norm prawnych tego obszaru.

Biorąc powyższe pod uwagę, podjęcie problematyki kreacji norm prawnych obszaru AI wymaga spojrzenia trójaspektowego. Po pierwsze, wertykalnego, rozumianego jako analiza kierunków prac legislacyjnych z perspektywy zróżnicowanych podmiotowo poziomów regulacyjnych, obejmujących zarówno kreację norm obowiązujących powszechnie, jak i związanych z tworzeniem tzw. prawa miękkiego. Po drugie, horyzontalnego, wymagającego analizy obszarów i zagadnień, które w debacie doktrynalnej i publicystycznej, a wreszcie w prowadzonych działaniach

¹ Por. Mario Hermann, Tobias Pentek, Boris Otto, „Working Paper No. 01/2015 Design Principles for Industrie 4.0 Scenarios” *A Literature Review*, (2016). <https://ieeexplore.ieee.org/document/7427673>.

prawodawczych, jawią się jako istotne regulacyjnie. Wreszcie po trzeciej, dokonać należy zestawienia wniosków z wyżej wymienionych analiz, celem ich odniesienia do metod regulacyjnych i rodzajów norm prawnych, które są lub powinny być przedmiotem legislacyjnego użycia. Zarys kierunków i przewidywalnych skutków tego użycia zostanie zasygnalizowane we wnioskach końcowych.

Wskazane powyżej hipotezy badawcze wpływają na wybór metody prowadzenia dalszych rozważań koncentrując się na analizie dogmatycznej tekstów prawnych, w tym ich projektów, a także tekstów prawniczych.

2 | Ujęcie wertykalne

Przechodząc do analizy prowadzonych aktualnie prac legislacyjnych obszaru AI, biorąc za kryterium rodzaj podmiotów za te prace odpowiedzialnych, wyraźnie wskazać należy, iż początek działań prawodawczych w tym zakresie dały różnego rodzaju akty prawa miękkiego, pochodzące zarówno od podmiotów zaangażowanych w tworzenie rozwiązań opartych o AI (samoregulacja), jak i organizacji typu non-profit, zajmujących się problematyką nowych technologii, czy też wreszcie organizacji międzynarodowych, podejmujących przedmiotową tematykę z uwagi na zakres własnych celów działania.

W ramach aktów samoregulacyjnych obejmujących AI na plan pierwszy wysuwają się tzw. kodeksy etyczne, określające zasady i wartości moralne, do przestrzegania których zobowiązuje się dany podmiot podczas projektowania, rozwoju i stosowania AI (np. kodeksy etyczne Google^[2], Microsoft^[3], IBM^[4] czy Facebook^[5]). Organizacjom pozarządowym zawdzięczamy z kolei tzw. standardy odpowiedzialności, określające zasady dotyczące przejrzystości, odpowiedzialności za decyzje AI, monitorowania skutków działania AI oraz postępowania w przypadku szkód lub nieprawidłowości

² *Google AI Principles*. <https://ai.google/responsibility/principles/>.

³ *Responsible AI principles from Microsoft*. <https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1:primaryr6>.

⁴ *Everyday Ethics for Artificial Intelligence IBM 2014-2022*. <https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf>.

⁵ *Facebook's five pillars of Responsible AI, June 22, 2021*. <https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/>.

(np. Deklaracja Montrealska na rzecz Odpowiedzialnego Rozwoju Sztucznej Inteligencji^[6]). Działania organizacji międzynarodowych rozpatrywać należy natomiast dwukierunkowo: po pierwsze, w kontekście kreowanych przez nie zaleceń lub wytycznych, zbliżonych zakresowo do kodeksów etycznych, regulujących zasady uczciwości, przejrzystości, odpowiedzialności, równości i poszanowania praw człowieka (np. Rada Europy – Europejska Karta Etyczna w sprawie wykorzystania systemów sztucznej inteligencji w systemach prawnych, grudzień 2018 r.^[7]; Unia Europejska – Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, kwiecień 2019 r.^[8]; OECD – Zalecenie Rady w sprawie sztucznej inteligencji, maj 2019 r.^[9]); po drugie, w ramach procesu standaryzacji i certyfikacji, koncentrując się na określaniu wymogów technicznych lub organizacyjnych związanych z tworzeniem (w tym m.in. testowanie, ocena bezpieczeństwa, standaryzacja interfejsów i komunikacji, wymagania jakości i niezawodności) lub wykorzystywaniem AI (wdrażanie i integracja zarządzania ryzykiem związanym z AI np. norma ISO/IEC23894:2023 z lutego 2023 r.^[10]).

Opisany model regulacji miękkiej, opartej głównie na implementacji norm etycznych niezbędnych do oceny systemów AI z perspektywy naruszenia praw podstawowych, reguł dyskryminacyjnych, jakości i bezpieczeństwa danych i ich transparentności czy też zasad kontroli nad systemami AI, bez wątplenia stworzył podwaliny do obserwowanych aktualnie trendów regulacyjnych zmierzających do kreacji normy imperatywnych

⁶ The Montreal Declaration for a Responsible Development of Artificial Intelligence. Tłumaczenie własne, <https://recherche.umontreal.ca/english/strategic-initiatives/montreal-declaration-for-a-responsible-ai/>. Deklaracja ogłoszona 3 listopada 2017 r. na zakończenie Forum Społecznie Odpowiedzialnego Rozwoju Sztucznej Inteligencji, które odbyło się w Palais des congrès de Montréal. Deklaracja ma na celu wywołanie debaty publicznej i zachęcenie do postępowego i inkluzywnego podejścia do rozwoju sztucznej inteligencji

⁷ European Commission for the Efficiency Of Justice (CEPEJ). Tłumaczenie własne. <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

⁸ <https://op.europa.eu/pl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.

⁹ Recommendation of the Council on Artificial Intelligence. Tłumaczenie własne, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

¹⁰ Information technology – Artificial intelligence – Guidance on risk management (Technologia informacyjna – Sztuczna inteligencja – Wytyczne dotyczące zarządzania ryzykiem). Tłumaczenie własne. <https://www.iso.org/standard/77304.html>.

lub semiimperatywnych pochodzących od organów upoważnionych do kreacji źródeł prawa krajowego bądź ponadpaństwowego.

W tym kontekście, kierując się w stronę aktów prawnych o charakterze powszechnie obowiązującym, zwrócić należy uwagę, iż – poza nielicznymi przykładami – prace nad nimi nie wyszły aktualnie poza sferę koncepcyjną. W tym zakresie, w sposób oczywisty z perspektywy europejskiego uczestnika obrotu prawnego, na plan pierwszy wysuwają się działania regulacyjne obszaru AI podejmowane przez Unię Europejską i Radę Europy.

21 maja 2024 r. Rada Europejska, po ponad 3 latach pracy, zatwierdziła projekt tzw. Aktu w sprawie sztucznej inteligencji^[11] (zwanego dalej też „AI Act”), który wszedł w życie 1 sierpnia 2024, stając się rzeczywistością prawną Unii Europejskiej. Jak wskazuje motyw 1 tego aktu normatywnego, podstawowym jego celem jest „poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych, w szczególności w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania sztucznej inteligencji zgodnie z wartościami Unii”. Akt ten opiera się konstrukcyjnie na trzech wymogach stawianych AI, zasygnalizowanych wcześniej w wytycznych UE z 2019 r., dotyczących: po pierwsze, jej zgodności z prawem obowiązującym (ze szczególną rolą ochrony prywatności, w tym danych osobowych); po drugie, zgodności z zasadami etycznymi; po trzecie, solidności technicznej i społecznej. Spełnienie tych wymogów ma zapewnić wykonanie celu nadrzędnego jakim jest oparcie AI na wartościach i prawach podstawowych, na czele z godnością ludzką i ochroną prywatności.

Od strony podmiotowej projekt AI Act zakłada kompleksowe i szerokie oddziaływanie, odrywając zakres jego zastosowania od siedziby dostawcy bądź twórcy AI. W ten sposób AI Act będzie wiązał zarówno dostawców systemów sztucznej inteligencji, niezależnie od tego, czy mają oni siedzibę w Unii, czy w państwie trzecim, oraz użytkowników systemów sztucznej inteligencji mających siedzibę w Unii, jaki i dostawców i użytkowników systemów sztucznej inteligencji, którzy mają siedzibę w państwie trzecim w takim zakresie, w jakim wyniki działania tych systemów są wykorzystywane w Unii oraz instytucje, urzędy, organy i agencje Unii, gdy działają one jako dostawca lub użytkownik systemu AI (szczegółowy zakres

¹¹ Pełny tytuł: rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze unii. Dalsze rozważania dotyczą wersji projektu z dnia 6 grudnia 2022 r. w oficjalnym polskim tłumaczeniu. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CONSIL:ST_15698_2022_INIT.

zastosowania określa projektowany art. 2). Przedmiotowo, analogicznie jak rozporządzenie RODO^[12], AI Act został ukształtowany w oparciu o zasadę ryzyka, kwalifikując systemy AI w zależności właśnie od ryzyka, jakie mogą generować dla praw i wolności podmiotów, które będą korzystały z tej technologii, w szczególności ich użytkowników. W tym kontekście projekt zakłada wprowadzenie czterech poziomów ryzyk AI:

1. niedopuszczalnego (tytuł II rozdział 1 AI Act), realizujących zakazane praktyki, których enumeratywną listę zawiera art. 5 projektu, obejmujących: stosowanie technik podprogowych (manipulacyjnych); wykorzystywanie dowolnych słabości określonej grupy osób; dokonywanie oceny lub klasyfikacji osób fizycznych prowadzonej przez określony czas wywołujących określone skutki; wykorzystywania w przestrzeni publicznej przez organy ścigania lub w ich imieniu, systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” do celów egzekwowania prawa;
2. wysokiego (tytuł III rozdział 2 i 3 AI Act), sklasyfikowane w załączniku do rozporządzenia, wobec których zakłada się konieczność spełnienia ustanowionych w nim wymogów, w szczególności w zakresie zarządzania ryzykiem, wykorzystywania i zarządzania danymi, rejestrowania zdarzeń, udostępniania informacji użytkownikom, nadzoru przez człowieka czy też dokładności, solidności i cyberbezpieczeństwa. Co istotne, poza wprowadzeniem w/w wymogów na same systemy, zakłada się nałożenie określonych obowiązków zarówno na ich dostawców, importerów, dystrybutorów, jak i samych użytkowników. Wobec tych systemów zorganizowany zostanie system oceny ich zgodności i certyfikacji oraz unijna baza danych zawierająca informacje o tych systemach i ich operatorach;
3. ogólnego, utożsamione z tzw. systemami ogólnego przeznaczenia (niebędącymi systemami wysokiego ryzyka), wobec których wprowadzone zostaną określone obowiązki wobec ich dostawców, czy też w zakresie posiadania deklaracji zgodności UE;
4. braku ryzyka, pozostałe systemy AI bez nałożonych wymogów.

¹² 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 (Dz.U.UE.L.2016.119.1).

Początkowo, w debacie nad AI Act podkreślano, iż wskazane założenie klasyfikacyjne nakierowane jest na kompleksowe objęcie AI, bez względu na to w jakim kierunku pójdzie postęp technologiczny. Wydaje się jednak, iż prawodawca unijny zmienił to podejście – prawdopodobnie w uwagi na zakładany brak możliwości jego realizacji – wprowadzając m.in. załączniki enumeratywnie określające wykazy systemów wysokiego ryzyka oraz specjalną procedurę przyspieszonej jego modyfikacji. Na marginesie dodać należy, iż gwarantem funkcjonowania tworzonego przez AI Act systemu, podobnie jak w systemie RODO, mają być wysokie, proporcjonalne i odstraszające kary, określane procentowo od obrotu osiąganego przez podmiot, który dopuścił się naruszenia.

Równoległe do działań legislacyjnych UE, Rada Europy prowadziła prace nad Konwencją w sprawie sztucznej Inteligencji, praw człowieka, demokracji i praworządności, której tzw. „zerowy” projekt datowany na 6 stycznia 2023 r., w lutym 2023 r. opublikował Komitet Rady Europy do spraw Sztucznej Inteligencji, który został ostatecznie przyjęty 17 maja 2024 r. w Strasburgu, podczas dorocznego spotkania ministerialnego Komitetu Ministrów Rady Europy. Jak wskazuje się w doktrynie, zajęcie się problematyką AI przez Radę Europy wynika z założenia, iż niekontrolowany rozwój technologii AI jest zagrożeniem dla podstawowych wartości europejskich skupionych w trzech flarach: ochronie praw człowieka, demokracji i praworządności. Przykład takich zagrożeń stanowią m.in. techniki rozpoznawania twarzy, czy też identyfikacji w czasie rzeczywistym osób na podstawie wizerunków, celem śledzenia i kontrolowania ludzi^[13]. Podobnie jak UE, Rada Europy podkreśla, że celem Konwencji jest stworzenie prawnych (nie tylko etycznych) standardów międzynarodowych systemów AI. Zwraca jednak uwagę swoista przewaga regulacji Rady Europy nad unijnym AI Act, która z uwagi na konwencyjną formę prawną aktu będzie otwarta do podpisu dla państw trzecich, tj. spoza grona jej członków.

Na tle opisanych europejskich prac prawodawczych, wskazać należy, iż w innych porządkach prawnych, w tym w szczególności technologicznie najbardziej rozwiniętych w zakresie tworzenia AI, jak Stany Zjednoczone i Chiny, również podjęto działania regulacyjne nakierowane na generatywną AI, przy czym przebiegają one w odmiennych kierunkach.

¹³ Por. Marek Świerczyński, Zbigniew Więckowski, „Ramy prawne dla sztucznej inteligencji w świetle najnowszych prac Rady Europy”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński (Warszawa: Wolters Kluwer, 2021), 301.

W Stanach Zjednoczonych 1 stycznia 2021 r. weszła w życie ustawa o krajowej inicjatywie w zakresie sztucznej inteligencji z 2020 r. (NAIIA), będącej *de facto* dokumentem programowym dla Gabinetu Stanów Zjednoczonych, mającym na celu „przyspieszenie badań i zastosowań sztucznej inteligencji dla dobrobytu gospodarczego i bezpieczeństwa narodowego, którego misją jest zapewnienie ciągłego przywództwa USA w badaniach i rozwoju sztucznej inteligencji, przewodzenie świata w rozwoju i wykorzystaniu godnej zaufania sztucznej inteligencji w sektorze publicznym i prywatnym oraz przygotowanie obecnej i przyszłej siły roboczej USA do integracji systemów sztucznej inteligencji we wszystkich sektorach gospodarki i społeczeństwa”^[14]. Śledząc debatę polityczną w USA, wyraźnie zauważa się priorytet przyznawany rozwojowi technologii AI, nad kwestiami jego bezpieczeństwa. Dopiero pojawienie się technologii chatbot-CzatGTP zapoczątkowało dyskusję programową, prowadzoną głównie z pozycji Departamentu Handlu US, zmierzającą do zebrania opinii na temat ewentualnego zakresu regulacyjnego, który zapewniłby, że systemy AI będą działać legalnie, skutecznie, etycznie, bezpiecznie i w sposób godny zaufania^[15]. Mimo wszystko, w podejściu tym zwraca uwagę absolutny priorytet przyznawany prawu własności jako podstawowej wartości, która służyć ma postępowi i rozwojowi ekonomicznemu, co zapowiada w przyszłości istotną kolizję tego systemu z europejskim, opartym o zasadę bezpieczeństwa.

W Chinach opublikowany 11 kwietnia 2023 r. projekt ustawy w sprawie środków regulujących świadczenie usług generatywnej sztucznej inteligencji zakłada, że podmioty używające AI (rozumianej jako technologia generująca tekst, obraz, wideo, program i inne treści na podstawie algorytmów i modeli), będą odpowiedzialne za wyniki działania swoich systemów, wymagając m.in., aby dane wykorzystywane do szkolenia ich algorytmów spełniały surowe wymagania bezpieczeństwa (w tym nie naruszając praw własności intelektualnej innych osób). Przy czym wymogi tego bezpieczeństwa zakładają m.in., iż:

treści generowane przez sztuczną inteligencję będą musiały „odzwierciedlać kluczowe wartości socjalistyczne i nie mogą zawierać elementów wywrotowych”. Zakazane będzie m.in. propagowanie treści uznawanych

¹⁴ *Artificial Intelligence Initiative Portal (Portal Inicjatywy Sztucznej Inteligencji)*. Tłumaczenie własne. <https://www.ai.gov/>.

¹⁵ Por. David Shepardson, Diane Bartz, „US begins study of possible rules to regulate AI like ChatGPT”, Reuters, (2023), <https://www.reuters.com/technology/us-begins-study-possible-rules-regulate-ai-like-chatgpt-2023-04-11/>.

przez chińskie władze za „terrorystyczne lub ekstremistyczne”, „nienawiści etnicznej” oraz innych treści „mogących zakłócić porządek ekonomiczny i społeczny”. Oznacza to, że treści generowane przez sztuczną inteligencję będą musiały być zgodne z wytycznymi chińskiej cenzury^[16].

Co więcej, każdy produkt AI przed wejściem na rynek będzie musiał uzyskać pozytywną ocenę bezpieczeństwa krajowego departamentu ds. regulacji Internetu.

Z kolei w Polsce, analizując zakres działań legislacyjnych, wyraźnie zauważa się brak aktywności zmierzających do kreacji aktów prawa powszechnie obowiązującego dotyczącego AI, co prawdopodobnie wynika z założenia związanego z oczekiwaniem na ukończenie prac prowadzonych w Unii Europejskiej i Radzie Europy, celem ewentualnej synchronizacji regulacji krajowych z obowiązującym bezpośrednio AI Act bądź też Konwencją. Nie oznacza to jednak braku wszelkiej aktywności w zakresie regulacyjnym sztucznej inteligencji. Uwagę zwracają tu prace koncepcyjne prowadzone są na poziomie grup roboczych, na czele z Grupą roboczą ds. sztucznej inteligencji (GRAI), która poprzez prace swoich podgrup, koncentruje się na różnych aspektach AI w zidentyfikowanych obszarach problemowych^[17].

3 | Ujęcie horyzontalne

Przechodząc do kolejnej części niniejszych rozważań, nakierowanych na analizę kierunków prowadzonych w ujęciu przedmiotowym prac legislacyjnych z obszaru AI, podkreślić należy, iż stanowi on aktualnie zbiór otwarty. Jest to bezpośrednio następstwo nieustannego rozwoju technologii AI, a przez to ciągłego odkrywania potencjalnych nowych zakresów jej zastosowania. W konsekwencji więc, prowadzenie dalszych rozważań należy prowadzić z perspektywy trzech segmentów tematycznych. Pierwszego dotyczącego bezpośrednio samej sztucznej inteligencji, analizowanej jako

¹⁶ Tak Hubert Kozieł, „Sztuczna inteligencja musi być komunistyczna. Tak chcą Chiny” *Rzeczpospolita* (2023). <https://cyfrowa.rp.pl/globalne-interesy/art-38293371-sztuczna-inteligencja-musi-byc-komunistyczna-tak-chca-chiny>.

¹⁷ Strona internetowa Grupy roboczej ds. sztucznej inteligencji (GRAI). <https://www.gov.pl/web/ai/grupa-robocza-ds-ai>.

swoisty byt prawny, koncentrując się na takich ogólnych zagadnieniach AI, jak jej definicja i korelacja do zasad prawnych, w tym w szczególności praw podstawowych. Drugi wiąże się z regulacjami prawnymi AI związanymi z zastosowaniem tzw. „słabej AI” (opartej o uczenie maszynowe, w którym system informatyczny różni się od innych tym, że jest w stanie wykonywać operacje zastrzeżone dotychczas wyłącznie dla umysłu ludzkiego) w określonych, zidentyfikowanych już technologicznie obszarach. Trzeci, najbardziej nieo określony, wiążący się z próbą dość futurystycznej kreacji zagadnień i problemów prawnych związanych z potencjalnymi zagrożeniami, które może ona stwarzać z racji swojego przewidywanego rozwoju w kierunku tzw. „silnej AI” (posiadającej wszystkie atrybuty ludzkiego mózgu, będąc jednocześnie zdolną do przetwarzania zasobów danych nieosiągalnych dla człowieka – aktualnie technologicznie niedostępnej) bądź też wkroczenia „słabej AI” w obszary, w których aktualnie jej zastosowanie technologicznie jest niemożliwe. Oczywiście z racji ogólności rozwiązań objętych obszarem pierwszym ewentualne jego zmiany będą przekładać się w sposób logiczny na zakres regulacyjny norm objętych obszarem drugim bądź kreowanych dla obszaru trzeciego, co wyraźnie wskazuje na wyzwania stojące w najbliższym czasie przed legislatorami różnych poziomów prawodawczych.

Kierując się w stronę pierwszej grupy zagadnień, wyraźnie uwydatnia się znaczenie przyjęcia prawnej definicji sztucznej inteligencji, co stanowić będzie punkt wyjścia dla wszelkich prac legislacyjnych nad AI, umożliwiając prowadzenie dalszych rozważań, w szczególności w zakresie jej korelacji z prawami podstawowymi, głównie prawem do prywatności. Ten segment regulacyjny jest aktualnie przedmiotem wskazanych powyżej prac prawodawczych prowadzonych przez UE oraz Radę Europy.

Dotykając problematyki definicji AI, wskazać należy, że pierwotnie jej kształtowaniem zajmowały się nauki informatyczne, rozumiejąc ją jako „system komputerowy zdolny do wykonywania zadań, które w zwykłych okolicznościach wymagają ludzkiej inteligencji”^[18]. Co ważne, definicja ta pozostaje na poziomie „słabej AI”, co kierunkowo powielono w art. 3 ust. 1 AI Act, zgodnie z którym system sztucznej inteligencji to

system, który zaprojektowano do działania w sposób częściowo autonomiczny i który, w oparciu o dane i informacje dostarczone maszynowo lub przez człowieka, wnioskuje w jaki sposób osiągnąć zadany zestaw

¹⁸ Tak Jeremy Achin, *Datarobot AI Experience 2017*. Tłumaczenie własne. <https://www.youtube.com/watch?v=ZChA63CpX5o>.

celów – z wykorzystaniem technologii uczenia się maszyn lub metod opartych na logice i wiedzy, i który generuje wyniki, takie jak treści (generatywne systemy sztucznej inteligencji), przewidywania, zalecenia lub decyzje, wpływające na środowiska, z którymi system ten wchodzi w interakcję.

Pomimo więc zakładanego przez prawodawcę europejskiego dążenia do zmaksymalizowania indyferentności technologicznej tej definicji, zapewniającej neutralność rozwojową AI, widać wyraźnie, że jej osiągnięcie, w perspektywie rozwoju „silnej AI”, może być w praktyce trudne do osiągnięcia. Doprowadzi to więc prawdopodobnie do konieczności cyklicznej jej aktualizacji, co z kolei będzie wymagało nieustannej jej analizy w zakresie zgodności z prawami podstawowymi, na co zresztą zwrócił już uwagę prawodawca europejski odwołując się w załącznikach objętych AI Act do określonego rodzaju technologii.

Przechodząc do drugiego segmentu, zauważyć należy, iż został on pozostawiony aktualnie działaniom prawodawcy krajowego, choć prawdopodobnie wraz z zamykaniem działań regulacyjnych nad pierwszym segmentem będzie stopniowo przejmowany przez prawodawcę ponadpaństwowego, w szczególności EU, w związku z jego istotnym przełożeniem na rynek wewnętrzny. Zakresowo, segment ten odznacza się znacznym poziomem identyfikowalności obszarów regulacyjnych AI, nad którymi trwają aktualnie debaty prawne lub bezpośrednie działania legislacyjne w wielu krajach, nie tylko europejskich. Analizując te prace, wskazać należy, iż obejmują one takie obszary jak:

1. prawo cywilne – dotyczące badania osobowości prawnej AI, zasad odpowiedzialności za jej działania^[19], ale także jej wykorzystania w postępowaniu cywilnym^[20];

¹⁹ 20 października 2020 r. Parlament Europejski przyjął rezolucję z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję, zakładająca rozróżnienie odpowiedzialności ze względu na rodzaj AI: systemy wysokiego ryzyka (zasadę ryzyka), inne systemy (zasada winy z odwróconym ciężarem dowodu). 28 września 2022 r. Komisja Europejska przyjęła z kolei propozycję dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję, w której nie powielono propozycji PE, lecz wyłącznie odniesiono się do ustanowienia szerszej ochrony ofiar systemów SI poprzez ułatwienie dochodzenia roszczeń o odszkodowanie (wprowadzenie zasad dowodowych, w tym zasad ujawniania dowodów przez dostawców AI), a także wspieranie sektora sztucznej inteligencji.

²⁰ Por. Ewa Płocha, „O pojęciu sztucznej inteligencji i możliwościach jej zastosowania w postępowaniu cywilnym” *Prawo w działaniu*, nr 44 (2020): 273-291.

2. własność intelektualna – dotyczy praw autorskich do utworów oraz praw własności przemysłowej do wynalazków wytworzonych przez AI lub z jej pomocą;
3. prawo karne, w szczególności kryminalistyki, której rozwój zostanie zdeterminowany systemami AI, od strony negatywnej, w związku z koniecznością neutralizacji nowych sposobów dokonywania przestępstw, od strony pozytywnej dostarczając nowych narzędzi do walki z przestępczością^[21], z jednoczesnym zwróceniem uwagi na zakres zgodności tych narzędzi z prawami człowieka. Odrębnym zagadnieniem pozostaje również wykorzystanie AI w postępowaniu karnym;
4. obsługa prawna – dotyczy zarówno sprawowania wymiaru sprawiedliwości (od wykorzystywania AI usprawniającego działalność tradycyjnych sądów po tzw. elektroniczne – zautomatyzowane sądy oparte decyzyjnie o AI^[22]) oraz obsługi prawnej (od problematyki wykorzystania różnych poziomów LegalTechu po automatyzację tej obsługi opartej o generatywne wykonywanie przez AI umów objętych jej kodem^[23]);
5. zdrowie – dotyczy zasad dostępu i przetwarzania danych medycznych, jakości danych medycznych oraz testowania i implementacji AI w tym obszarze oraz określenia zasad współpracy przy jej korzystaniu z personelem medycznym i pacjentami;
6. energetyka – dotyczy prognozowania, optymalizacji zasobów, działań i operacji na sieci, predictive maintenance (PdM)^[24], a także automatyzacji procesów w zakresie pomiarów, rachunków i ogólnej dystrybucji;

²¹ Por. Marcin Wielec, Ewa Płocha, „Sztuczna inteligencja jako narzędzie pracy biegłego w procesie karnym”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński (Warszawa: Wolters Kluwer, 2021), 193.

²² Por. Maria Dymitruk, Jacek Gołaczyński, „Elektroniczny sąd a sztuczna inteligencja w prawie polskim”, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, Dariusz Szostek (Warszawa: C.H. Beck, 2019), 47.

²³ Por. Dariusz Szostek, „IBAC (IoT, Blockchain, AI i Cyberbezpieczeństwo) – samoregulacja kodów czy kontrola uprzednia?”, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, Dariusz Szostek (Warszawa: C.H. Beck, 2019), 44.

²⁴ Tzn. procesu zapobiegania awariom sprzętu i przestojom poprzez łączenie zasobów przedsiębiorstwa obsługujących IoT, stosowanie zaawansowanych analiz do dostarczanych przez nie danych w czasie rzeczywistym oraz wykorzystywanie wyników postrzeżeń do tworzenia procedur konserwacji.

7. rolnictwo i ochrona środowiska – dotyczy wykorzystania narzędzi AI w badaniach z tego obszaru oraz ich wykorzystania przez rolników;
8. transport i mobilność – dotyczy wdrożenia AI w przedsiębiorstwach działających w branży transportowo-logistycznej i w obszarach związanych z mobilnością (m.in. w zakresie inteligentnych systemów transportu zbiorowego^[25]);
9. finanse i bankowość – dotyczy wykorzystania AI w tym obszarze (głównie z uwzględnieniem zasady proporcjonalności) oraz efektywnych rozwiązań dla podmiotów publicznych odpowiedzialnych za nadzór nad instytucjami regulowanymi, a także ich dostawcami;
10. edukacja – dotyczy umiejętności cyfrowych, nakierowanych na rozwijanie kompetencji związanych z tworzeniem oraz korzystaniem z technologii AI;
11. praca i polityka społeczna – dotyczy konsekwencji społecznych AI zarówno na rynku pracy (związanych z nierównościami i naturą pracy)^[26], jak i zmian w relacjach społecznych, w szczególności tzw. generacji Alfa^[27];
12. wojskowość – dotyczy zakresu wykorzystania i nadzoru nad autonomicznymi systemami uzbrojenia przenoszącymi proces decyzyjny z człowieka na system AI.

Zupełnie wyodrębnionym zakresowo obszarem pozostaje zagadnienie jurysdykcji i wyboru prawa z uwagi na eksterytorialność cyberprzestrzeni.

²⁵ Por. Łukasz Goździaszek, „Zasady wyboru i wdrażania aplikacji i usług inteligentnych systemów transportowych (ITS)”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński (Warszawa: Wolters Kluwer, 2021), 115-124.

²⁶ Por. Agata Frankowska, Bartosz Pawlik, „Przegląd osiągnięć publikowanych w zakresie sztucznej inteligencji na świecie – analiza bibliometryczna”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński (Warszawa: Wolters Kluwer, 2021), 155.

²⁷ Tak Ada Florentyna Pawlak, *Doświadczenia telefikcyjne i relacje paraspoleczne generacji Alfa*, XV Konferencja Bezpieczeństwo w Internecie – Solidarność Cyfrowa, ALK, 11 maja 2023 r.

4 | Metody regulacyjne AI

Biorąc pod uwagę analizowany powyżej wertykalnie i horyzontalnie problem regulacji prawnej obszaru AI, trzeba wyraźnie wskazać, że skutkuje on możliwością wykorzystania każdej z trzech klasycznych metod regulacyjnych tzn. metody prywatnoprawnej, karnoprawnej, administracyjnoprawnej i ewentualnie podejścia zintegrowanego, łączącego te metody. Oczywiście wybór danej metody jest silnie uzależniony od wyznaczonego na poziomie politycznym kierunku działania. Obserwacja debaty publicznej prowadzonej w USA i Europie, czy też decyzji władz Chin, pokazuje, że kierunek ten, w przypadku AI, może być zupełnie przeciwstawny, co przekłada się na wybór odmiennej metody regulacyjnej.

Metoda prywatnoprawna ma zasadniczo na celu zapewnienie elastyczności i samoregulacji w sektorach, gdzie interwencja państwa może lub powinna być ograniczona. Metoda ta opiera się na zasadzie autonomii woli stron, które w swobodnym procesie negocjacyjnym ustalają warunki i zasady swojego działania, oczywiście z poszanowaniem szerokich granic norm objętych gałęzią prawa cywilnego. Metoda ta oparta jest więc na procesie samoregulacji przybierającym postać umowy, regulaminu, standardu branżowego lub innej formy porozumienia. W przypadku stosowania AI metoda ta może więc teoretycznie obejmować m.in. tworzenie umów licencyjnych lub umów dostarczania usług, określających prawa i obowiązki dotyczące korzystania z systemów AI, odpowiedzialności za jej działania, ochronę danych i inne kwestie związane z ich stosowaniem. Wydaje się, iż tą metodą regulacyjną podążają USA, zaś UE, porzuciła ją wraz z projektem AI Act.

Metoda karnoprawna ma na celu eliminację przez państwo określonej grupy czynów uznawanych przez nie za społecznie szkodliwe, poprzez określenie ich rodzajów, ustalenie zasad odpowiedzialności oraz sankcji i sposobów jej wymierzenia. W kontekście AI metoda karnoprawna może mieć zastosowanie w swoisty sposób jako konkurencja metody prywatnoprawnej, dotykając dualistycznych albo fundamentalnych zagrożeń związanych z funkcjonowaniem AI, na czele z ochroną prywatności w tym danych osobowych bądź sektorowo, związanych z zastosowaniem AI w branżach wrażliwych np. medycynie czy też rynku finansowym. Aktualnie rozwiązania prawne dotyczące AI, wykorzystujące tą metodę, nie zostały przedstawione.

Metoda administracyjnoprawna „oparta jest na zasadzie władztwa organu administracji publicznej i podporządkowania mu innych podmiotów,

adresatów normy prawnej. Nadrzędna pozycja organu wynika z powierzenia mu kompetencji załatwiania spraw”^[28]. W kontekście AI, analizując zakres postulowanych rozwiązań m.in. w debacie europejskiej, stwierdzić należy, że większość z nich jest możliwa do osiągnięcia właśnie tą metodą. Co istotne, w ramach metody administracyjnoprawnej wyróżnić można dwa jej rodzaje, tzn. tradycyjny model polski (oparty o normy bezpośrednio obowiązujące, które nakładają obowiązki publicznoprawne na podmiot uregulowany, za przestrzeganie których odpowiada wyznaczony organ państwowy; i normy pośrednio obowiązujące, wymagające aktu administracyjnego określającego prawa i obowiązki) oraz model unijny, który poza rozwiązaniami właściwymi modelowi polskiemu, zakłada możliwość m.in. obowiązku wprowadzania określonych rozwiązań ładu wewnętrznego w podmiotach prywatnoprawnych, np. polityk zgodności oraz dopuszczenia istnienia prywatnych podmiotów certyfikujących, podlegających nadzorowi publicznemu (*de facto* zastępujących organy państwowe), upoważnionych do potwierdzania posiadania określonych zdolności przez podmiot prywatne w postaci np. certyfikatu (*de facto* zastępującego decyzję organu)^[29]. Analizując AI Act można bez wątpliwości stwierdzić, że prawodawca unijny implementuje w tej regulacji metodę administracyjnoprawną, którą *de facto* zwiążę, po przyjęciu tych przepisów, prawodawców i systemy prawne państw członkowskich, co doprowadzi też do modyfikacji sposobu jej rozumienia i stosowania w tych państwach.

Zwrócić należy też uwagę na podejście zintegrowane, zakładające stosowanie zróżnicowanych, wielogłęziowych metod regulacyjnych, które przy wielowymiarowości problematyki AI może okazać się istotnym w praktyce legislacyjnej sposobem regulowania AI na poziomie poszczególnych państw.

²⁸ Tak Stanisław. Prutis, „Metody regulacji prawnej stosunków społecznych a uwarunkowania prawne mediacyjnych (ugodowych) form rozstrzygnięcia sporów”, [w:] Państwo, gospodarka, prawo. Księga dedykowana Profesorowi Cezaremu Kosikowskiemu z okazji jubileuszu pracy naukowej na Wydziale Prawa Uniwersytetu w Białymstoku, red. Anna. Piszcz, Marcin Olszak, Maciej. Etel (Białystok: Temida2, 2015), 29-53.

²⁹ Por. Mariusz Maciejewski, „Nadzór publiczny nad sztuczną inteligencją jako gwarancja realizacji praw i zasad cyfrowych w cyfrowej dekadzie”, XV Konferencja Bezpieczeństwo w Internecie – Solidarność Cyfrowa, ALK, 11 maja 2023 r.

5 | Wnioski

Podsumowując powyższe rozważania, wskazać należy, iż wykazują one zasadniczo wyłącznie reaktywne podejście legislatorów różnych poziomów prawodawczych przy tworzeniu regulacji prawnych zarysowanych obszarów. Analizowani prawodawcy (zarówno krajowi, jak i ponadpaństwowi) dostosowują normy prawne do już istniejących i nieustannie rozwijanych rozwiązań technicznych, próbując odpowiedzieć na problemy prawne, które wywołuje ich stosowanie. Doprowadza to do sytuacji faktycznego ograniczenia możliwości działania sprawczego kształtującego przyszły rynek. „W dyskusji nad prawnymi aspektami sztucznej inteligencji mniej uwagi poświęcone jest natomiast próbie poszukiwania kierunku zmian dla całego systemu prawnego w taki sposób, aby normy prawne służyły do proaktywnego kształtowania branży, która dopiero powstaje”^[30]. Jak się wydaje, futurystyczny aktualnie segment obszaru trzeciego, związany z potencjalnym powstaniem tzw. „silnej AI”, nie tylko stwarza możliwość, ale wręcz nakłada na legislatorów obowiązek kompleksowego i uprzedniego podejścia – swoistego spojrzenia „do przodu” – zakładającego proaktywne wyznaczenie kierunków rozwoju AI.

Wyznaczenie takich kierunków na poziomie uniwersalnym, który jest fundamentalny z perspektywy globalizacji technologii AI, bazującej na rozproszonych geograficznie danych, może być w praktyce jednak niemożliwe. Patrząc bowiem na trwającą debatę polityczną w USA, Europie czy też Chinach, prowadzącą do wyboru wskazanych wcześniej, odmiennych kierunków regulacyjnych AI, już w najbliższym czasie nastąpi jej zasadnicze prawne zróżnicowanie na tych trzech kluczowych rynkach.

Patrząc z perspektywy polskiej, jako państwa członkowskiego UE, która realnie pozbawiona jest możliwości wytwórczych AI, przy prezentowanym podejściu zostaniemy, wraz z resztą Europy, faktycznie „skazani” na technologię amerykańską (przy wykluczeniu z przyczyn bezpieczeństwa technologii chińskiej), która tworzona jest w modelu, dla którego bezpieczeństwo jest tylko jednym (nie jedynym) elementem podejmowania decyzji biznesowych jej rozwoju. Doprowadzi to niestety do bezpośredniej „próby sił”, prowadzonej głównie w wymiarze prawnym, pomiędzy

³⁰ Tak Marcin Rojszczak, „Prawne aspekty systemów sztucznej inteligencji – zarys problemu”, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. Kinga Flaga-Gieruszyńska, Jacek Gołączyński, Dariusz Szostek (Warszawa: C.H. Beck, 2019), 2.

twórcami i dostawcami amerykańskiej technologii AI a UE, reprezentującą europejskiego użytkownika. Doświadczenia nabyte podczas poprzedniego zbliżonego dyskursu, prowadzonego pomiędzy twórcami, dostawcami serwisów społecznościowych i komunikatorów internetowych a UE na tle regulacji RODO, nie do końca przekonują, czy spojrzenie na rozwój technologii przez pryzmat wyłączenie praw podstawowych (w tym prawa do prywatności) będzie tym, które w wymiarze faktycznym odniesie sukces. Pozwala to też stawiać pytania o faktyczny koszt, zwłaszcza dla europejskiego rozwoju gospodarczego, jaki przyniesie takie podejście. Wprost zadać należy pytanie: która strona zostanie dostawcą, a która importer tej technologii? Wydaje się, że warto uwzględnić te konsekwencje, prowadząc dalszą debatę nad kształtem regulacji AI.

Bibliografia

- Dymitruk Maria, Jacek Gołaczyński, „Elektroniczny sąd a sztuczna inteligencja w prawie polskim”, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, Dariusz Szostek. 47-56, Warszawa: C.H. Beck, 2019.
- Frankowska Agata, Bartosz Pawlik, „Przegląd osiągnięć publikowanych w zakresie sztucznej inteligencji na świecie – analiza bibliometryczna”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński. 155-168. Warszawa: Wolters Kluwer, 2021.
- Goździaszek Łukasz, „Zasady wyboru i wdrażania aplikacji i usług inteligentnych systemów transportowych (ITS)”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński. 115-124. Warszawa: Wolters Kluwer, 2021.
- Hermann Mario, Tobias Pentek, Boris Otto, „Working Paper No. 01/2015 Design Principles for Industrie 4.0 Scenarios” *A Literature Review*, (2016). <https://ieeexplore.ieee.org/document/7427673>.
- Kozieł Hubert, „Sztuczna inteligencja musi być komunistyczna. Tak chcą Chiny” *Rzeczpospolita*, (2023). <https://cyfrowa.rp.pl/globalne-interesy/art-38293371-sztuczna-inteligencja-musi-byc-komunistyczna-tak-chca-chiny>.
- Płocha Ewa, „O pojęciu sztucznej inteligencji i możliwościach jej zastosowania w postępowaniu cywilnym” *Prawo w działaniu*, nr 44 (2020): 273-291.

- Prutis Stanisław, „Metody regulacji prawnej stosunków społecznych a uwarunkowania prawne mediacyjnych (ugodowych) form rozstrzygania sporów”, [w:] *Państwo, gospodarka, prawo. Księga dedykowana Profesorowi Cezaremu Kosikowskiemu z okazji jubileuszu pracy naukowej na Wydziale Prawa Uniwersytetu w Białymstoku*, red. Anna. Piszcz, Marcin Olszak, Maciej Eteł. 29-53. Białystok: Temida2, 2015.
- Rojszczak Marcin, „Prawne aspekty systemów sztucznej inteligencji – zarys problem”, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, Dariusz Szostek. 1 -22. Warszawa: C.H. Beck, 2019.
- Shepardson David, Diane Bartz, „US begins study of possible rules to regulate AI like ChatGPT” *Reuters*, (2023). <https://www.reuters.com/technology/us-begins-study-possible-rules-regulate-ai-like-chatgpt-2023-04-11/>.
- Szostek Dariusz, „IBAC (IoT, Blockchain, AI i Cyberbezpieczeństwo) – samoregulacja kodów czy kontrola uprzednia?”, [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. Kinga Flaga-Gieruszyńska, Jacek Gołaczyński, Dariusz Szostek. 39-46, Warszawa: C.H. Beck, 2019.
- Świerczyński Marek, Zbigniew Więckowski, „Ramy prawne dla sztucznej inteligencji w świetle najnowszych pac Rady Europy”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński. 301-326. Warszawa: Wolters Kluwer, 2021.
- Wielec Marcin, Ewa Płocha, „Sztuczna inteligencja jako narzędzie pracy biegłego w procesie karnym”, [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. Bogdan Fischer, Adam Pązik, Marek Świerczyński. 193-210. Warszawa: Wolters Kluwer, 2021.

