# Jak inteligentne jest prawo regulujące sztuczną inteligencję? Próba analizy AI Act na podstawie jej ugruntowania w przestrzeni komercyjnego użycia

*Kamil Palacz*[1]

Celem niniejszego opracowania jest przybliżenie regulacji prawnych zagadnienia sztucznej inteligencji (*artificial intelligence*), przykładów jej zastosowania oraz ryzyka, jakie ze sobą niesie. W niniejszym artykule poruszono także temat AI Act, przeanalizowano kwestię sztucznej inteligencji w ujęciu prawa kontynentalnego oraz common law, a także podjęto próbę odpowiedzi na pytanie, czy legislacja AI na naszym aktualnym poziomie wiedzy jest legislacją trafną.

## Uwagi wstępne

Sztuczna inteligencja jest technologią inspirującą ludzi, od kiedy ten koncept po raz pierwszy pojawił się w przemówieniu *J. McCarthy'ego* na konferencji w Dartmouth Collage w 1956 r.[2]. Po prawie 70 latach, gdy sztuczna inteligencja jest nam bliższa niż była kiedykolwiek, nie milkną echa konieczności prawnego uregulowania tej kwestii.

To, w jaki sposób patrzymy na sztuczną inteligencję, jest różny. Kiedyś popularne było spojrzenie na nią jak na inną istotę żywą. Zagubioną w świecie stworzonym przez ludzi dokładnie tak jak w filmie *AI: Artificial Inteligence*. Jednak obecnie patrzymy na nią jak na potencjalne zagrożenie mogące zagrozić cywilizacji – w taki sam sposób, który w książce „Superinteligence: Paths, Dangers, Strategies"[3] przedstawia *N. Bostrom* lub który popularyzuje seria filmów o terminatorze.

Na początku warto przytoczyć definicje AI. Czym więc jest ten koncept, który tak interesuje ludzi? Otóż jak wynika z definicji przytoczonej na stronie Parlamentu Europejskiego: „sztuczna inteligencja (SI) to zdolność maszyn do wykazywania ludzkich umiejętności, takich jak rozumowanie, uczenie się, planowanie i kreatywność. Sztuczna inteligencja umożliwia systemom technicznym postrzeganie ich otoczenia, radzenie sobie z tym, co postrzegają i rozwiązywanie problemów, działając w kierunku osiągnięcia określonego celu. Komputer odbiera dane (już przygotowane lub zebrane za pomocą jego czujników, np. kamery), przetwarza je i reaguje. Systemy SI są w stanie do pewnego stopnia dostosować swoje zachowanie, analizując skutki wcześniejszych działań i działając autonomicznie"[4].

Temat wart jest poruszenia nie tylko ze względu na jego szybki rozwój, ale także fakt, iż w przeciwieństwie do masowej opinii nie jest to już technologia przyszłości, a coś, co zaczyna w coraz większej mierze dotyczyć każdego z nas. By się o tym przekonać, wystarczy odebrać telefon, wiele firm nie może bowiem sobie pozwolić (lub nie chce) na dział Call Center. W efekcie wykorzystują dzisiaj boty, które doradzają klientom i prezentują im najnowsze promocje. Szczątkową wersję tegoż możemy zobaczyć już na wielu portalach. Konsultant, którym w rzeczywistości jest *chatbot*, nie jest wart więcej niż koszty jego kupna i administracji, a jest w stanie odsiać większość prozaicznych i prostych do rozwiązania problemów dnia codziennego. Oczywiście taki *chatbot* musi mieć wbudowaną możliwość kontaktu z prawdziwym człowiekiem, który będzie w stanie rozwiązać bardziej skomplikowane sprawy. Jest to już wielki skok technologiczny w porównaniu do czasu sprzed dekady, kiedy możliwość rozmawiania przez telefon z konsultantem nieposiadającym fizycznego ciała, a jedynie zaprogramowany ciąg wypowiedzi, byłaby fikcją, którą można było zobaczyć jedynie w filmach.

## Zagrożenia użytku AI a AI Act

W takich czasach legislacja taka jak AI Act zdaje się odpowiednio ugruntowana w potrzebach nowoczesnego społeczeństwa. Zwłaszcza (o czym będzie mowa w dalszej części artykułu), że AI oprócz wspaniałych możliwości niesie równie wspaniałe zagrożenia. Zagrożenia, które już dzisiaj, mimo raczkującej wciąż technologii wspomaganej sztuczną inteligencją, sprawiły realne problemy realnym ludziom.

Jak zaznacza ekspert w dziedzinie AI – *G. Mauro* w swoim filmie „EU ARTIFICIAL INTELIGENCE ACT: Why we need it, how it works, what it means"[5] w USA działał program, który jedynie na podstawie danych pacjenta oszacowywał prawdo-

[1] Autor jest studentem czwartego roku kierunku Prawo na Uniwersytecie Wrocławskim oraz aktywnym członkiem studenckiego Koła Naukowego Blok Prawa Komputerowego LegalNet. Piastuje także stanowisko młodszego specjalisty ds. prawnych w kancelarii prawnej HYPERION Gałek i Gałan.

[2] Redakcja portalu Ai.nl, Timeline of AI: a brief history of artificial intelligence it's highlights, https://www.ai.nl/artificial-intelligence/timeline-of-ai-a-brief-history-of-artificial-intelligence-its-highlights (dostęp 14.1.2023 r.).

[3] *N. Bostrom*, Superinteligence: Paths, Dangers, Strategies, Oksford 2014, s. 114–115.

[4] Parlament Europejski, Sztuczna inteligencja: co to jest i jakie ma zastosowania?, https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania (dostęp 14.1.2023 r.).

[5] *G. Mauro*, EU ARTIFICIAL INTELLIGENCE ACT: Why we need it, how it works, what it means, https://www.youtube.com/watch?v=l0h5gjturV4 (dostęp 14.1.2023 r.).

podobieństwo, że dana osoba będzie potrzebować większej liczby badań. Algorytm stojący za tym programem różnicował ludzi. Osoby czarnoskóre oraz Azjaci byli przez ów algorytm dyskryminowane, gdyż ten znacznie rzadziej wskazywał u nich na konieczność przeprowadzenia dodatkowych badań, co wielokrotnie skończyło się śmiercią pacjentów.

W tym samym filmie *G. Mauro* mówi o algorytmie wprowadzonym przez firmę Amazon, który miał różnicować CV kandydatów ubiegających się o pracę. Ten algorytm również różnicował ludzi pod względem ich płci, dyskryminując kobiety. Bierze się to ze zjawiska nazwanego: „skrzywieniem algorytmicznym".

## Skrzywienie algorytmiczne i ryzyko, jakie wprowadza

Zjawisko to zostało opisane przez *A. Obem* w wywiadzie udzielonym dla portalu Papaya.rocks: „do wytrenowania sieci neuronowej, czyli złożonego, uczącego się modelu statystycznego, potrzebna jest odpowiednio duża liczba przykładów, o dużej różnorodności, które pozwolą wykryć najdrobniejsze zależności. Zbyt mały, nie dość różnorodny i nieaktualizowany zbiór danych prowadzi do tego, że system popełnia błędy, tworząc skrzywienie. Badacze z Uniwersytetu w Waszyngtonie celowo »skrzywili« algorytm, którego zadaniem było klasyfikowanie zwierząt na zdjęciach – wilków i psów rasy husky. Dane treningowe obejmowały 20 zdjęć wilków – wszystkie w tle miały śnieg. Co się wydarzyło? Wytrenowany na takich danych algorytm zwierzęta występujące na tle śniegu oznaczał zawsze jako wilki – zwracając uwagę tylko na tło, a nie na cechy charakterystyczne zwierzęcia"[6].

Wobec czego oczywistym krokiem wydaje się konieczność wprowadzenia regulacji, która zapewniłaby poprawną administrację nad tymi algorytmami. Wszystko po to, by sytuacja nie powtórzyła się, zwłaszcza w momencie, w którym sztuczna inteligencja na stałe zawita do naszych domów. Również do gałęzi życia, w których mogłaby – nieodpowiednio administrowana – spowodować więcej zniszczeń.

## Przykłady wykorzystania AI na świecie

Pod koniec 2022 r. agencja Reuters[7] podała, że w Pekinie ma wystartować start-upowa sieć „robo taksówek". Krytycy tego pomysłu postulują o niebezpieczeństwach, jakie niesie za sobą wprowadzenie takiej technologii do użytku publicznego. Stoi za tym BAIDU, chińskie przedsiębiorstwo, które zapowiada, że zwiększy liczbę swoich autonomicznych taksówek do 200 w ciągu trwającego roku.

W tym samym artykule podano, że większość producentów samochodowych wycofała się z tego pomysłu, jednak BAIDU już prowadzi działania na skalę większą niż tylko Chiny. Do miejsc, gdzie owe autonomiczne samochody trafią, zaliczają się Arizona oraz California. Jednak gdy myślimy o autonomicznych samochodach, firmą, która najbardziej wysuwa się na pierwszy plan, jest Tesla.

Swego czasu przedsiębiorstwo założone przez *E. Muska* było najlepszym kandydatem do zaimplementowania tej technologii do naszego świata. Dziś po śledztwie, które przeprowadził amerykański rząd, Tesla utrzymuje, że ich autonomiczne pojazdy wymagają człowieka gotowego na szybką reakcję, w razie gdyby samochód nie reagował samoczynnie na zjawisko występujące na drodze. Tym mocniej w pamięć zapada zdarzenie, które wydarzyło się w trakcie jazdy takiego samochodu Tesli. Ten, by ominąć liść, wykonał manewr, który kosztował życie nieuważnego przechodnia.

W Europie również możemy pochwalić się pewnym postępem w tej dziedzinie. W trakcie konferencji „Cyberspace", która odbyła się na Uniwersytecie Masaryka w Brnie w 2022 r., podczas paralelnego panelu „The world of AI sandboxes, and their use in practice"[8], zastępca dyrektora ds. mobilności autonomicznej oraz badań, rozwoju i innowacji przy Ministerstwie Transportu Republiki Czeskiej – *T. Čížková* wypowiadała się o trudnościach, z jakimi aktualnie mierzą się Czechy w dostosowywaniu infrastruktury drogowej do użytku przez samochody autonomiczne.

Z kolei, jak podaje gazeta *New York Post*, chińscy naukowcy zdołali zaprogramować algorytm, który po wystawieniu na dane ponad 17 000 spraw, „jest w stanie do pewnego stopnia zastąpić prokuratora w procesie podejmowania decyzji"[9] – mówi prof. *S. Yong*, który sprawował pieczę nad tymi badaniami. Wskazuje na jego niebywałą skuteczność sięgającą aż 97%.

W przypadku analizowania AI łatwo o wniosek, że niebezpiecznie zbliżamy się do dystopii. Jednak pamiętajmy, że są to dopiero pierwsze kroki technologii, której wkład w świat zależeć będzie od naszego podejścia do niej. Oczywiste jest, że braki w stworzonym algorytmie sztucznej inteligencji mogą zabić przechodniów lub doprowadzić do skazania niewinnego człowieka. To słusznie budzi w nas niepokój, jednak ta sama technologia używana jest również do rzeczy, które ułatwiają nam życie codzienne, jak chociażby komunikator Alexa lub Siri.

---

[6] *J. Czechowicz*, Sztuczna inteligencja, ale prawdziwa dyskryminacja. Jakie są potencjalne zagrożenia wynikające z AI?, https://papaya.rocks/pl/trendbook/sztuczna-inteligencja-ale-prawdziwa-dyskryminacja-jakie-sa-p (dostęp 14.1.2023 r.).

[7] *K. Krolicki*, Baidu, Pony.ai start driverless robotaxi tests in Beijing, https://www.reuters.com/technology/baidu-gets-license-driverless-robotaxi-tests-beijing-2022-12-30/ (dostęp 14.1.2023 r.).

[8] Uniwersytet Masaryka, 21. Międzynarodowa konferencja Cyberspace 2022, www.cyberspace.muni.cz/programme (dostęp z 14.1.2023 r.).

[9] *H. Sparks*, China's AI attorney prosecutes crimes 'with 97% accuracy', https://nypost.com/2021/12/27/chinas-ai-attorney-prosecutes-crimes-with-97-accuracy/ (dostęp 14.1.2023 r.).

W tej sytuacji warto przypomnieć sobie popularną analogię z nożem. On sam w sobie nie jest zły, używamy go w końcu każdego dnia i choć skaleczenia są jak najbardziej bolesne, wynikają z naszego własnego roztargnienia lub braku umiejętności, nie z jego natury. Nie zmienia to jednak faktu, że to samo narzędzie, w nieodpowiednich rękach może przyczynić się do tragedii.

## AI Act, czyli prawo oparte na ryzyku

W wyżej opisanej rzeczywistości UE zdecydowała się wprowadzić legislację, która miałaby zahamować niektóre niepożądane użycia AI.

AI Act jest aktem, który za swój rdzeń ma wartości, którym hołduje UE i na podstawie wyliczonego prawdopodobieństwa wystąpienia ryzyka pogwałcenia tychże zasad, klasyfikuje pewne gałęzie komercyjnego użycia, które powinny być obwarowane szczególnymi przepisami. Ryzyko podzielono na cztery kategorie.

Nieakceptowalne użycie stanowi pierwszą kategorię, którą wyszczególnia AI Act. Zawiera się w niej użycie AI do m.in. manipulowania ludźmi. Nietrudno sobie wyobrazić, jakie możliwości posiadałoby mikrotargetowanie reklam czy komunikatów przy użyciu analizującej każde kliknięcie sztucznej inteligencji. Zwłaszcza że już teraz pojawiają się badania nad tym, jakie komunikaty działają na poszczególne jednostki najbardziej. Liczni eksperci cytowani na łamach bussinesinsider.com, potwierdzają, że właśnie takie działania i badania przyczyniły się do wygranej *Trumpa* w wyborach prezydenckich w 2016 r.[10].

Kolejnym nieakceptowalnym użyciem technologii AI jest rozpoznawanie twarzy przy użyciu kamer monitoringu miejskiego w czasie rzeczywistym. Jednak tu istnieje wyjątek. Wciąż legalne będzie wykorzystywanie tego sposobu do odnajdywania zagubionych dzieci oraz identyfikowania terrorystów w przestrzeni publicznej.

Użycie o wysokim ryzyku – w tej kategorii mieści się używanie sztucznej inteligencji do oceniania i różnicowania ludzi przy zatrudnianiu oraz przy promocji czy awansu. Jednak warto wspomnieć już teraz, że AI Act wymaga od dostawców takowych algorytmów, aby czuwali nad tym, jak działają ich programy. Wszystko po to, by nie doszło do ich spaczenia, co mogłoby stworzyć podobną sytuację jak z przytaczanym już wcześniej algorytmem wykorzystywanym swego czasu przez platformę Amazon.

Kolejnym użyciem, które zawiera się w kategorii wysokiego ryzyka, jest ocenianie ludzi pod względem przyjęcia na uniwersytet. Również w tym przypadku, jak w poprzednim, AI Act wymaga od dostawców ciągłej administracji po to, by nie dochodziło do nadużyć czy dyskryminacji na tle rasowym, czy płci. Najważniejszym zapisem jest jednak wpisanie do tej kategorii używanie AI dla infrastruktury krytycznej oraz Policji. Można zakładać, że poziom administracji takiego algorytmu będzie zdecydowanie wyższy niż w przypadku oceny ludzi starających się o przyjęcie do pracy oraz że zaufanie do takiego algorytmu będzie mocno ograniczone. Deweloperzy tej technologii są zobligowani do serii testów, które wyeliminują jakąkolwiek stronniczość w ocenianiu danych, na jakie będzie wystawiony algorytm. Tu również pojawia się wymóg obecności człowieka po drugiej stronie algorytmu, który będzie w stanie go „naprawić", jeśli ten zacznie wychylać się ze swoją oceną gdzieś poza ramy przyjęte przez te określone w akcie ramy użycia.

Trzecią i czwartą kategorię stanowią tzw. użycie limitowane oraz minimalne. Oba wykorzystywane są w działaniach, podczas których trudno zrobić krzywdę człowiekowi. Mowa tu m.in. o rozwiązaniach jak *Chatbot* czy filtr spamu. W takiej sytuacji deweloperzy tej technologii zobowiązani są, by każdorazowo powiadamiać użytkownika, że rozmawia ze sztuczną inteligencją. Dodatkowo zalecane jest, by deweloperzy wytworzyli w tej kwestii swój własny kod etyki. Jednak presja na tym wyszczególnionym aspekcie użytkowania sztucznej inteligencji nie jest wysoka.

## Antropocentryzm w AI Act

AI Act nazywany jest legislacją „na próbę", co samo w sobie nie jest złe w żaden sposób. Nie wiemy jeszcze, jakie są granice użycia AI w różnych gałęziach przemysłu, więc AI Act wydaje się naprawdę dobrym aktem prawa, który nada ton późniejszym obostrzeniom oraz bada to, w jaki sposób AI może być użytkowane, by sprawić, żeby życie było lepsze.

Zastanawia jednak fakt podejścia prawodawców do tego przedmiotu regulacji. Jest to akt, który reguluje wykorzystywanie sztucznej inteligencji przez pryzmat człowieka. Bo to do niego odnoszą się wszelkie ewentualne konsekwencje nieplanowanych działań sztucznej inteligencji.

Oczywiste jest, że w regulacji prawnej przede wszystkim chodzi o to, żeby nikomu nie stała się krzywda przez legalne użytkowanie tego typu programów. Jednak wątpliwości może budzić jakość danych zgromadzonych przez legislatorów na podstawie ustawy, której centrum stanowi człowiek.

Jednocześnie zastanawia, dlaczego regulacje nie odnosiły się do konkretnych kwestii związanych ze sztuczną inteligencją. Nie zabroniono tworzyć oprogramowania mogącego spełniać przesłanki kategorii nieakceptowalnej, ale zabroniono jej używać. Może to doprowadzić do sytuacji, gdy przy różnej legislacji oprogramowanie, które w Europie nie może być wykorzystywane, jest w niej jednocześnie produkowane.

[10] *I. Asher Hamilton*, Trump targeting Black voters in 2016 shows Facebook's microtargeting is a danger to democracy, experts say, https://www.businessinsider.com/trump-targeting-black-voters-facebook-2016-deterrence-experts-comment-2020-9 (dostęp 14.1.2023 r.).

## AI w ujęciu prawa kontynentalnego oraz *common law*

Prawo kontynentalne istotnie różni się od *common law*, a różnice te mogą stanowić przeszkodę w przypadku ograniczania rozwoju szkodliwych nowych technologii. Pierwszą i kluczową odmiennością jest tu tempo legislacji. Zdecydowanie wolniej będą tworzyć się akty, na które obywatel może się powołać w starciu sądowym z deweloperami sztucznej inteligencji. Mimo używania wykładni intencjonalnej najczęściej preferowanej przez UE wciąż zdecydowanie szybszy rozwój nowych technologii, w tym AI, może doprowadzić do sytuacji, w której ta technologia będzie używana do łamania pewnych praw, a jednocześnie będzie wciąż legalna.

W systemie *common law* sytuacja ma się zgoła inaczej, jeśli obywatel może przed sądem powołać się na wyrok innego sądu. Wystarczy jeden wyrok skazujący, by to jedno wykorzystanie tej nowej technologii zostało do pewnego stopnia ograniczone, a na pewno, by obywatel mógł bronić swoich praw w efektywniejszy sposób.

## Polityczność kręgosłupa AI oraz czy i jakie prawa mogą na tym ucierpieć

Prawodawcy, jak wszyscy politycy, odpowiadają przed swoim suwerenem, jakim są ludzie. Można zatem zakładać, że takie podejście będzie miało swoje odzwierciedlenie w aktach prawa, które z rąk takich prawodawców wychodzą. Zatem uzasadnioną obawą jest, że prawa, których opis łatwiej zamknąć w prostych słowach, będą determinowały to, na co pozwolimy deweloperom sztucznej inteligencji.

Nikt nie poskarży się, że spowolnienie rozwoju AI narusza jego prawa ekonomiczne, kiedy zobaczy, że źródłem tych ograniczeń jest wolność i bezpieczeństwo każdego Europejczyka. Jednak stanowi to aspekt, nad którym warto się zastanowić. Jeśli prawo będzie tworzone pod medialny wydźwięk, możemy doprowadzić do sytuacji, w której nie będziemy w stanie korzystać z tej technologii w pełni jej potencjału. Ważne jest, by znaleźć złoty środek między ograniczaniem a wytyczaniem optymalnego kursu, który, choć już widoczny w zalążku, powinien być rozwijany w przyszłości dla najlepszej efektywności algorytmów sztucznej inteligencji. Nie możemy również poddawać się emocjom, które od początku towarzyszą tej technologii.

## Czy legislacja na naszym aktualnym poziomie wiedzy jest legislacją trafną?

Na ten moment legislacja oparta na ryzyku w użyciu jest rozsądna. Nie znamy jeszcze wszelkich możliwości sztucznej inteligencji, a jej wszechstronność działa na niekorzyść regulacji mających ją ograniczać. Dlatego dobrze, że powstał akt prawa, który (choć nie jest wolny od wad) normuje najbardziej krytyczne sposoby użytkowania tej technologii.

Oczywiste jest, że pojawią się wkrótce sposoby wykorzystania jej do rzeczy, które – gdybyśmy o nich wiedzieli dziś – byłyby wyłączone z użycia, jednak złą praktyką z perspektywy rozwoju byłoby również ograniczanie jej w sposób nazbyt rozwinięty. Każda technologia ma koniec końców służyć ludziom. A AI Act jest na dobrej drodze, by zapewnić nam przyszłość, w której tymi ludźmi jesteśmy my.

**Słowa kluczowe:** sztuczna inteligencja, AI Act, kategorie AI Act, regulacje prawne sztucznej inteligencji, zastosowanie sztucznej inteligencji.

---

# *How intelligent is the law regulating artificial intelligence? An attempt to analyse the AI Act based on its implementation in the sphere of commercial use*

*The purpose of this study is to present regulations in regard to artificial intelligence, examples of its use and risks it entails. In the present article the author also brings up the subject of the AI Act, analyses the issue of artificial intelligence in the context of civil law and common law, and attempts to answer the question whether AI legislation on our current level of knowledge is accurate legislation.*

**Keywords:** artificial intelligence, AI Act, categories of AI Act, artificial intelligence regulations, application of artificial intelligence.

---