

Analiza aktu w sprawie sztucznej inteligencji na tle dynamicznego rozwoju AI

Krzysztof Kiszluk

1. Wprowadzenie

Sztuczna inteligencja (AI – z ang. *artificial intelligence*), niegdyś domena naukowej spekulacji, stała się w ostatnich latach kluczowym elementem technologicznego postępu. W ciągu ostatniej dekady AI przeszła dynamiczny rozwój i przeniknęła do wielu sfer naszego życia, od przemysłu i produkcji, poprzez transport i logistykę aż po rynki kapitałowe i usługi konsumenckie. Wzrost mocy obliczeniowej, postęp w dziedzinie uczenia maszynowego (w szczególności głębokiego uczenia) oraz dostępność ogromnych zbiorów danych przyczyniły się do przyspieszenia tego procesu. W rezultacie AI zyskała zdolność wykonywania zadań, które jeszcze niedawno były uważane za dostępne wyłącznie dla ludzkiego umysłu – od tworzenia obrazów, muzyki i filmów krótkometrażowych, poprzez prowadzenie konwersacji aż po przygotowywanie skomplikowanych analiz i prognoz. Trudno nadażyć za tempem rozwoju sztucznej inteligencji – gdyby zatrzymać go nagle w miejscu na obecnym etapie, to jeszcze lata zajęłoby nam odkrycie wszystkich zastosowań tej technologii. Rozwój ów natomiast nie zwalnia, ale przyspiesza – prawdopodobnie

w tempie wykładniczym¹, co oznaczałoby, że wszystko, co wydarzy się w najbliższym czasie w związku z AI, będzie większym przełomem niż wszelkie osiągnięcia w tej dziedzinie z ostatnich kilkudziesięciu lat. Na potwierdzenie tej tezy przywołać można najnowsze doniesienia ze świata nauki, zgodnie z którymi chat GPT4 przeszedł test Turinga² (mający dowodzić opanowania przez maszynę umiejętności myślenia w sposób podobny do ludzkiego). Co więcej, przeprowadzono po raz pierwszy test moralności Turinga, podczas którego 299 badanych nieświadomie oceniło, że zdolność chatu GPT4 do rozwiązywania kwestii moralnych jest już na poziomie wyższym niż ludzka³. W badaniu odrębnie oceniane były cechy takie jak cnota, inteligencja i wiarygodność – w każdym z tych wymiarów AI wypadła lepiej od ludzi.

2. Sztuczna inteligencja a polscy przedsiębiorcy

Rewolucja dotycząca sztucznej inteligencji nie ominęła także polskich przedsiębiorców. W 2023 r. polskie przedstawicielstwo międzynarodowego koncernu EY przeprowadziło badania, które miały na celu ocenę obecnego stanu wdrożenia systemów AI w polskich przedsiębiorstwach⁴. Badanie przeprowadzono na próbie 501 przedsiębiorców.

¹ W 1965 r. sformułowano tzw. prawo Moore'a, które było wynikiem obserwacji, że liczba tranzystorów w układzie scalonym podwaja się w niemal równych odcinkach czasowych. Prawo to używane jest do określenia postępu w różnych dziedzinach technologii. Badania prowadzone nad możliwościami sztucznej inteligencji wskazują, że jej rozwój podlega prawu Moore'a – zob. <https://www.ml-science.com/exponential-growth> (dostęp: 20.07.2024).

² B.K. Bergen, C.R. Jones, *People Cannot Distinguish GPT-4 from a Human in a Turing Test*, arXiv:2405.08007, 2024.

³ E. Aharoni i in., *Attributions toward Artificial Agents in a Modified Moral Turing Test*, „Scientific Reports” 2024, nr 14.

⁴ *Jak polskie firmy wdrażają AI?*, Raport EY Polska, 2023.

39% ankietowanych stanowiły przedsiębiorstwa duże (250 lub więcej pracowników lub ponad 50 mln euro obrotu), a pozostałe 61% – średnie (50–250 pracowników lub obrót od 10 do 50 mln euro). W wyniku przeprowadzonych badań opublikowano raport, z którego wynika m.in., że:

1. rozwiązania oparte na narzędziach sztucznej inteligencji wdrożyło 20% ankietowanych przedsiębiorców, a kolejne 40% było w trakcie procesu wdrażania;
2. aż 8 na 10 badanych wyraziło gotowość do wdrożenia narzędzi opartych na AI;
3. do podstawowych motywów skłaniających do wdrożenia systemów AI należą:
 - a) usprawnienie/automatyzacja procesów wewnętrznych,
 - b) chęć wprowadzenia nowej usługi,
 - c) możliwość lepszego dotarcia do klientów;
4. do głównych obszarów, w których przedsiębiorcy wdrażają narzędzia oparte na AI, należą:
 - a) obsługa klienta,
 - b) sprzedaż,
 - c) produkcja,
 - d) marketing i analiza rynku,
 - e) IT/cyberbezpieczeństwo;
5. 8 na 10 przedsiębiorców, którzy wdrożyli systemy AI, stwierdziło, że osiągnęło z tego tytułu zamierzone korzyści.

Z danych wynika, że sztuczna inteligencja staje się kluczowym elementem strategii rozwoju wielu firm. Wysoki poziom gotowości do wdrożeń oraz pozytywne doświadczenia z dotychczasowych implementacji wskazują, że AI może znacząco wpłynąć na efektywność operacyjną i innowacyjność przedsiębiorstw. Warto zauważyć, że obszary takie jak obsługa klienta i marketing są szczególnie podatne na automatyzację przy pomocy sztucznej inteligencji, co może prowadzić do lepszego zaspokajania potrzeb klientów oraz zwiększenia konkurencyjności na rynku.

3. Akt ws. sztucznej inteligencji

Im bardziej sztuczna inteligencja się rozwija, tym większe budzi obawy i wątpliwości oraz tym szersze stwarza możliwości do nadużyć. W literaturze jako największe zagrożenia związane z wykorzystaniem AI na szeroką skalę wskazuje się m.in.⁵ cyberprzestępczość, rozpowszechnianie dezinformacji (np. w postaci deepfake'ów), dyskrecjonalność sztucznej inteligencji w podejmowaniu decyzji, wzrost bezrobocia oraz możliwość utworzenia – na wzór chińskiego „systemu zaufania społecznego”⁶ – systemów kontroli społecznej. Unijny ustawodawca nie pozostał obojętny na te obawy i już w 2021 r. rozpoczął prace nad uregulowaniem funkcjonowania AI. Ich efektem było przyjęcie przez Parlament Europejski dnia 13 marca 2024 r. rozporządzenia o skrótowej nazwie „akt w sprawie sztucznej inteligencji”⁷. Za jeden z jego podstawowych celów uznano

promowanie upowszechniania zorientowanej na człowieka i godnej zaufania sztucznej inteligencji przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie

⁵ Zob. np. D. Prokopowicz, *Opportunities and Threats to the Development of Artificial Intelligence Applications and the Need for Normative Regulation of this Development*, „International Journal of Legal Studies” 2023, nr 2(14), s. 95–129; R. Tadeusiewicz, *Automatyzacja i sztuczna inteligencja jako źródła prawdziwych i wyimaginowanych zagrożeń*, [w:] B. Galwas, P. Kozłowski, K. Prandecki (red.), *Czy świat należy urządzić inaczej. Schyłek i początek*, Warszawa 2019.

⁶ Zob. np. Bartoszewicz, M., *Chiński System Zaufania Społecznego*, „Przegląd Geopolityczny” 2020, nr 32, s. 58–67.

⁷ 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 dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), Dz.U. L, 2024/1689, 12.7.2024.

praw podstawowych Unii Europejskiej, w tym demokracji, praworządności i ochrony środowiska, ochrony przed szkodliwymi skutkami systemów AI w Unii, a także wspierania innowacji⁸.

Regulacja ta jeszcze przed wejściem w życie określona została mianem przełomowej na skalę światową. Jej przełomowość ma wynikać nie tylko z faktu, że są to pierwsze na świecie przepisy regulujące kompleksowo zagadnienia związane z wykorzystaniem sztucznej inteligencji, ale także z przyjętego w akcie tzw. *risk-based approach*. Rozporządzenie wyróżnia bowiem cztery kategorie systemów sztucznej inteligencji w oparciu o kryterium potencjalnych szkód, jakie mogą zostać wyrządzone w związku z ich wykorzystaniem. Te cztery kategorie to: oprogramowanie wysokiego ryzyka, technologie ograniczonego i minimalnego ryzyka oraz systemy nieakceptowalne, które będą w Unii Europejskiej zakazane.

Do ostatniej z tych kategorii będą należeć, zgodnie z art. 5 rozporządzenia, m.in. systemy:

- wykorzystujące techniki przekazu podprogowego i celowe techniki manipulacyjne lub wprowadzające w błąd, czego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub grupy osób w sposób wyrządzający lub mogący wyrządzić poważną szkodę;
- wykorzystujące słabości osoby fizycznej lub określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną;
- przewidujące prawdopodobieństwo popełnienia przez osobę przestępstwa wyłącznie na podstawie jej profilowania, oceny cech osobowości;
- służące kategoryzacji biometrycznej celem wywnioskowania rasy, poglądów politycznych, orientacji seksualnej itp.;
- służące tworzeniu punktacji społecznej.

⁸ Motyw 1 aktu w sprawie sztucznej inteligencji.

Co do pozostałych kategorii – w zależności od stopnia ryzyka – nakładane będą na przedsiębiorców odpowiednie obowiązki. Nie będzie to jednak jedyny czynnik determinujący charakter tych obowiązków. Istotną kwestią wydaje się tutaj także rola, jaką przedsiębiorca pełni względem danego systemu AI. Wyróżnia się więc następujące podmioty: dostawców systemów AI, podmioty stosujące AI, importerów i dystrybutorów systemów AI, producentów produktów powiązanych z AI⁹. Systemy minimalnego ryzyka (w tym większość aplikacji AI dostępnych obecnie na jednolitym rynku UE, takich jak gry wideo z obsługą AI i filtry antyspamowe) nie są regulowane.

Systemy sztucznej inteligencji o ograniczonym ryzyku podlegać będą obowiązkom w zakresie transparentności: dostawcy i podmioty stosujące muszą zapewnić, że użytkownicy końcowi są świadomi, że wchodzi w interakcję ze sztuczną inteligencją (np. z chatbotem).

Systemy AI wysokiego ryzyka to m.in. te, które działają w obszarach¹⁰:

- identyfikacji i kategoryzacji biometrycznej osób fizycznych;
- zarządzania infrastrukturą krytyczną i jej eksploatacji;
- kształcenia i szkolenia zawodowego;
- zatrudniania pracowników i zarządzania nimi;
- ścigania przestępstw;
- zarządzania migracją, azylem i kontrolą graniczną;
- sprawowania wymiaru sprawiedliwości i procesów demokratycznych.

Obowiązki z nimi związane będą nakładane przede wszystkim na dostawców. Należać do nich będzie¹¹:

- ustanowienie, wdrożenie, prowadzenie dokumentacji i obsługa systemu zarządzania ryzykiem;

⁹ Art. 2 aktu w sprawie sztucznej inteligencji.

¹⁰ Załącznik III do aktu w sprawie sztucznej inteligencji – *Systemy AI wysokiego ryzyka, o których mowa w art. 6 ust. 2.*

¹¹ Art. 16–22 aktu w sprawie sztucznej inteligencji.

- ustanowienie właściwych praktyk zarządzania bazami danych wykorzystywanymi do trenowania systemów AI;
- prowadzenie dokumentacji technicznej systemów AI;
- zapewnienie automatycznego rejestrowania wszelkich zdarzeń istotnych dla identyfikacji sytuacji ryzykownych;
- informowanie podmiotów stosujących o tych zdarzeniach;
- zapewnienie nadzoru osób fizycznych nad systemem AI;
- współpraca z właściwymi organami;
- (w przypadku, gdy dostawca ma miejsce zamieszkania lub siedzibę poza UE) ustanowienie przedstawiciela mającego miejsce zamieszkania lub siedzibę w UE.

Podmioty stosujące systemy AI wysokiego ryzyka obowiązane będą m.in. do¹²:

- podjęcia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia, aby systemy takie były wykorzystywane zgodnie z dołączoną do nich instrukcją obsługi;
- zapewnienia nadzoru osób fizycznych;
- monitorowania działania systemu AI wysokiego ryzyka w oparciu o instrukcję obsługi i informowania dostawców oraz organu nadzoru o zaistniałym w związku z tym działaniem ryzykiem.

Ustawa odnosi się również do modeli AI ogólnego przeznaczenia (GPAI)¹³. Dostawcy modeli AI ogólnego przeznaczenia, które nie stwarzają ryzyka systemowego, będą podlegać ograniczonym wymogom

¹² Art. 26 aktu w sprawie sztucznej inteligencji.

¹³ Definiowanych w art. 3 pkt. 63. aktu w sprawie sztucznej inteligencji w sposób następujący: „model AI, w tym model AI trenowany dużą ilością danych z wykorzystaniem nadzoru własnego na dużą skalę, który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model ten jest wprowadzany do obrotu, i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla – z wyłączeniem modeli AI, które są wykorzystywane na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu”. W celu uzyskania szerszej informacji na

dotyczącym przejrzystości. Dostawcy GPAI stwarzających ryzyko systemowe będą dodatkowo zobowiązani m.in. do przeprowadzania odpowiednich testów modelu w celu zidentyfikowania ryzyka czy rejestrowania i zgłaszania informacji dotyczących poważnych incydentów i ewentualnych środków naprawczych służących zaradzeniu im¹⁴.

Za naruszenia przepisów rozporządzenia dotyczącego sztucznej inteligencji przewidziano grzywny, które będą ustalane jako procent całkowitego rocznego obrotu przedsiębiorstwa z poprzedniego roku obrotowego lub jako kwota z góry określona, w zależności od tego, która z tych wartości będzie wyższa.

W celu zapewnienia właściwego egzekwowania przepisów utworzono na poziomie unijnym następujące organy:

1. Urząd ds. Sztucznej Inteligencji w ramach Komisji Europejskiej, odpowiedzialny za egzekwowanie wspólnych zasad w całej UE¹⁵;
2. Radę ds. AI z przedstawicielami państw członkowskich, doradzącą Komisji i państwom członkowskim w spójnym i skutecznym stosowaniu ustawy o AI¹⁶;
3. forum doradcze dla zainteresowanych stron, dostarczające specjalistycznej wiedzy technicznej Radzie ds. AI¹⁷;
4. panel naukowy składający się z niezależnych ekspertów, wspierający działania związane z egzekwowaniem przepisów¹⁸.

temat GPAI zob. *General Purpose AI and the AI Act*, <https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf> (dostęp: 20.07.2024); M. Gahntz, C. Pershan, *Artificial Intelligence Act – How the EU Can Take on the Challenge Posed by General-Purpose AI System*, <https://foundation.mozilla.org/en/blog/how-the-eu-can-take-on-general-purpose-ai-in-the-ai-act/> (dostęp: 20.07.2024).

¹⁴ Art. 55 aktu w sprawie sztucznej inteligencji.

¹⁵ Art. 64 aktu w sprawie sztucznej inteligencji.

¹⁶ Art. 65–66 aktu w sprawie sztucznej inteligencji.

¹⁷ Art. 67 aktu w sprawie sztucznej inteligencji.

¹⁸ Art. 68 aktu w sprawie sztucznej inteligencji.

Rozporządzenie zobowiązuje także państwa członkowskie do utworzenia organu nadzoru rynku i organu notyfikującego i pozostawia w tym zakresie pewną swobodę m.in. co do tego, czy utworzone zostaną nowe organy, czy kompetencje wynikające z rozporządzenia zostaną przekazane organom już istniejącym. W związku z tym Ministerstwo Cyfryzacji przeprowadziło prekonsultacje¹⁹, w których zadano m.in. następujące pytania:

1. Czy w związku z wdrożeniem Aktu powinien powstać w polskim porządku prawnym zupełnie nowy, przeznaczony temu obszarowi organ nadzoru rynku, czy też może tę funkcję powinny pełnić obecnie istniejące organy lub organ?
2. Czy w związku z wdrożeniem Aktu funkcja organu notyfikującego powinna być pełniona przez obecnie istniejący podmiot lub podmioty publiczne, czy też przez nowy, powołany w tym celu podmiot?
3. Czy w związku z wdrożeniem Aktu funkcję organu nadzoru rynku oraz organu notyfikującego powinny być realizowane przez tę samą instytucję, czy też poprzez niezależne od siebie organy na zasadzie współpracy opartej na podziale zadań?

W prekonsultacjach wzięło udział 50 podmiotów. Większość z nich opowiedziało się za powołaniem nowego organu nadzoru rynku AI. Do jego zadań należałoby rozpatrywanie wniosków dotyczących zezwolenia na oddanie do użytku systemów sztucznej inteligencji wysokiego ryzyka oraz rozstrzyganie skarg osób poddanych działaniom systemów AI. Instytucja przyjmowałaby również zgłoszenia dotyczące poważnych incydentów oraz współpracowała z Komisją, forum doradczym oraz Radą ds. AI. Uczestnicy prekonsultacji byli natomiast podzieleni w kwestii podmiotu mającego pełnić funkcję organu notyfikującego.

¹⁹ *Przyszłość AI w Polsce – wyniki prekonsultacji wdrożenia aktu o sztucznej inteligencji*, <https://www.gov.pl/web/cyfryzacja/przyszlosc-ai-w-polsce--wyniki-prekonsultacji-wdrozenia-aktu-o-sztucznej-inteligencji> (dostęp: 20.07.2024).

4. Ocena regulacji

W literaturze nie od dziś podkreśla się konieczność uregulowania pozycji prawnej sztucznej inteligencji ze względu na potencjalne zagrożenia, jakie AI za sobą niesie, oraz konieczność przeciwdziałania próbom nieetycznego jej wykorzystania. W tym kontekście uchwalenie aktu w sprawie sztucznej inteligencji niewątpliwie stanowi istotny krok naprzód. Rozporządzenie to ma na celu wprowadzenie spójnych regulacji w obszarze AI w Unii Europejskiej, co jest istotne m.in. z perspektywy ochrony bezpieczeństwa oraz praw podstawowych, ale służyć będzie także zapewnieniu właściwego rozwoju rynku wewnętrznego UE. O ile trudno oceniać akt prawny jeszcze przed całkowitym jego wdrożeniem, o tyle nie sposób nie zwrócić uwagi na innowacyjne podejście zaprezentowane w akcie ws. sztucznej inteligencji oraz nowatorski charakter tej regulacji. W doktrynie pozytywnie ocenia się przede wszystkim zastosowanie *risk-based approach*, które umożliwia dostosowanie regulacji do specyfiki różnych systemów AI, co może przyczynić się do bardziej efektywnego zarządzania ryzykiem²⁰. Krytykowane z kolei są w głównej mierze zbyt ogólne sformułowania niektórych przepisów (przede wszystkim tych dotyczących klasyfikacji systemów), które mogą prowadzić do niejasności i trudności w ich stosowaniu²¹.

5. Podsumowanie

Sztuczna inteligencja niewątpliwie stanowi jeden z kluczowych elementów współczesnego rozwoju technologicznego. Dynamiczny postęp

²⁰ R. Bieda i in., *O etycznych, prawnych i społecznych konsekwencjach stosowania systemów sztucznej inteligencji w państwach członkowskich Unii Europejskiej. Uwagi na tle projektu rozporządzenia w sprawie sztucznej inteligencji*, „Przegląd Sejmowy” 2023, nr 6(179), s. 66–67.

²¹ Ibidem, s. 74–75.

w dziedzinie uczenia maszynowego, tworzenia algorytmów i budowania sieci neuronowych oraz rosnące możliwości w zakresie wykorzystania dużych baz danych determinują coraz szersze zastosowanie i wzrastający wpływ AI na najróżniejsze sfery naszego życia. Przywołane w opracowaniu badania jednoznacznie wskazują, że rewolucja dotycząca sztucznej inteligencji nie omija także sektora gospodarczego. Polscy przedsiębiorcy są otwarci na wdrażanie narzędzi opartych o AI – wysoka gotowość do implementacji oraz pozytywne doświadczenia z dotychczasowych wdrożeń sugerują, że AI może znacząco wpłynąć na efektywność operacyjną firm.

Rozwój sztucznej inteligencji niesie za sobą jednak szereg zagrożeń, takich jak rozprzestrzenianie dezinformacji, cyberprzestępczość czy ryzyko naruszeń prywatności. Konieczne jest więc uregulowanie tego zjawiska w celu ochrony przed jego potencjalnymi szkodliwymi skutkami. Istotny krok w kierunku ochrony wartości zagrożonych nieetycznym wykorzystaniem sztucznej inteligencji stawia ustawodawca unijny poprzez uchwalenie rozporządzenia – aktu ws. sztucznej inteligencji – mającego na celu ustanowienie standardów prawnych w zakresie tworzenia narzędzi opartych o AI oraz posługiwania się nimi. Pozytywnie należy ocenić nowatorskie podejście regulacyjne oraz kompleksowy charakter rozporządzenia. Biorąc jednak pod uwagę rozległość regulowanej materii oraz nadzwyczajne tempo rozwoju sztucznej inteligencji, a także niejednoznaczność niektórych postanowień aktu ws. sztucznej inteligencji, można przypuszczać, że nie będzie on stanowił wystarczająco skutecznego narzędzia ochrony przed niedopuszczalnymi praktykami związanymi z wykorzystaniem AI, a w najbliższym czasie zajdzie konieczność dostosowania obowiązujących przepisów w tym zakresie lub ustanowienia nowych.