NOWE TECHNOLOGIE

Regulacja sztucznej inteligencji – co czeka przedsiębiorców?

Wiarygodność sztucznej inteligencji jest warunkiem wstępnym jej upowszechnienia. W zależności od poziomu ryzyka wyróżnia się systemy SI ryzyka niedopuszczalnego, wysokiego, ograniczonego i minimalnego.

TOMASZ KAMIŃSKI
adwokat, Kancelaria Prawna Krzysztof Rożko i Wspólnicy

Wykorzystanie systemów sztucznej inteligencji stanowi jeden z najważniejszych czynników odpowiedzialnych za dynamicznie postępujące w ostatnich latach przemiany w życiu społecznym oraz gospodarczym. Rozwiązania algorytmiczne posiadające cechy sztucznej inteligencji (SI) pozwalają na: usprawnienie procesów dokonywania skomplikowanych prognoz, zwiększenie efektywności procesów, optymalizację kosztów, personalizację świadczonych usług. To wszystko umożliwia osiągnięcie korzyści w różnych obszarach istotnych dla funkcjonowania społeczeństw.

Co jest charakterystyczne dla modelu gospodarki opartej na wiedzy, coraz powszechniej algorytmy stosowane są w celu zwiększenia efektywności procesów realizowanych przez podmioty gospodarcze. Przykładowo, systemy oparte na sztucznej inteligencji pozwalają na usprawnienie procesów rekrutacyjnych, wspierają ocenę zdolności kredytowej, wspomagają ocenę ryzyka szkody, czy umożliwiają prowadzenie spersonalizowanych kampanii reklamowych.

Z drugiej strony ze stosowaniem rozwiązań bazujących na SI wiąże się szereg ryzyk, wśród których najczęściej wymienia się: brak przejrzystości podejmowania decyzji (problem tzw. black box), dyskryminacja, ingerencja w prawo do prywatności czy wykorzystanie w celach przestępczych. Niepewność co do rozwoju systemów sztucznej inteligencji, w tym relacje nadziei oraz obaw związanych z ich wykorzystaniem, najlepiej chyba oddaje opinia wyrażona przez prof. Stephena Hawkinga, który stwierdził, że „sztuczna inteligencja będzie albo najlepszą albo najgorszą rzeczą, jaka spotka ludzkość".

Ważne wyzwanie

Bez wątpienia problematyka regulacji systemów SI stanowi jedno z największych wyzwań, jakie stoją przed instytucjami odpowiedzialnymi za stanowienie prawa. Obecnie w różnych jurysdykcjach równolegle prowadzone są prace związane z wprowadzeniem regulacji dotyczących działania sztucznej inteligencji, które w nieodległej przyszłości będą wyznaczać ramy prawne wykorzystania algorytmów.

Wspólnym mianownikiem podejmowanych prób uregulowania systemów SI są dylematy, z jakimi już na wstępnym etapie prac muszą mierzyć się instytucje odpowiedzialne za przygotowanie propozycji stosowanych ram prawnych. Bez wątpienia największym wyzwaniem związanym z regulowaniem systemów sztucznej inteligencji jest stworzenie takich ram prawnych, które z jednej strony będą wspierały wykorzystanie innowacyjnych rozwiązań, przyczyniając się tym samym do wzrostu gospodarczego, konkurencyjności oraz zwiększenia jakości usług publicznych, z drugiej zaś będą zapewniały bezpieczeństwo systemów SI oraz ochronę praw podstawowych.

U podstaw toczących się w Unii Europejskiej prac nad stworzeniem ram prawnych sztucznej inteligencji leży założenie o podwójnym celu, jaki powinna spełniać taka regulacja. Podkreśla się zarówno konieczność promowania stosowania sztucznej inteligencji, jak i potrzebę zajęcia się zagrożeniami związanymi z niektórymi zastosowaniami nowej technologii. Źródłem takiego podejścia jest uznanie, że wiarygodność sztucznej inteligencji jest warunkiem wstępnym jej upowszechnienia.

Tak sformułowane cele podejścia do sztucznej inteligencji mają zapewniać korzyści płynące z zastosowania nowej technologii dla obywateli państw członkowskich, przedsiębiorstw, interesu publicznego, jak i środowiska. Ramy prawne sztucznej inteligencji w Unii Europejskiej mają wpisywać się w szerszą politykę dotyczącą sztucznej inteligencji, ukierunkowaną na osiągniecie tzw. ekosystemu doskonałości oraz zaufania.

Nakreśliwszy cel, jakim jest stworzenie ekosystemu doskonałości oraz zaufania, w odniesieniu do działania systemów SI, podjęto w UE decyzję o zainicjowaniu trzech toczących się równolegle procesów legislacyjnych, które obejmują:

- wniosek w sprawie przyjęcia aktu w sprawie sztucznej inteligencji (ang. Artificial Intelligence Act, AIA), który ma ustanawiać zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania sztucznej inteligencji w UE – projekt został opublikowany 21 kwietnia 2021 r.;
- ustanowienie reguł dotyczących odpowiedzialności cywilnej w celu dostosowania przepisów dotyczących odpowiedzialności do ery cyfrowej i sztucznej inteligencji – 10 stycznia 2022 r. zakończył się okres konsultacji publicznych;
- przegląd aktów sektorowych z zakresu bezpieczeństwa.

Zakłada się, że powyższe inicjatywy legislacyjne powinny mieć komplementarny charakter oraz że będą przyjmowane etapami.

Główne założenia projektu

W ramach prac analitycznych nad opracowaniem założeń unijnego aktu prawnego w sprawie sztucznej inteligencji rozważano różne koncepcje nowej regulacji. Ostatecznie wybrano wariant polegający na przyjęciu horyzontalnego (a zatem znajdującego zastosowanie w różnych sektorach) instrumentu legislacyjnego, uwzględniającego proporcjonalne podejście oparte na analizie ryzyka, uzupełnianego przez branżowe kodeksy postępowania dotyczące systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem.

Projekt zakłada wyodrębnienie czterech kategorii systemów SI, co opiera się na analizie ryzyka, jakie stwarza wykorzystanie danego rodzaju systemu. W zależności od poziomu ryzyka wyróżnia się systemy SI ryzyka niedopuszczalnego, wysokiego, ograniczonego i minimalnego. O ile zakwalifikowanie danej praktyki w zakresie sztucznej inteligencji do kategorii niedopuszczalnego ryzyka oznacza zakaz stosowania danego systemu, o tyle w odniesieniu do pozostałych kategorii systemów przypisanie do danej kategorii ryzyka łączy się ze zróżnicowaniem poziomu wymogów w odniesieniu do projektowania, opracowania, wprowadzania do obrotu czy wykorzystywania systemu.

Zgodnie z zaproponowanym podziałem ryzyko niedopuszczalne dotyczyć ma np.: wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który stosuje techniki podprogowe będące poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną.

Kolejną kategorią ryzyka wskazaną w rozporządzeniu jest ryzyko wysokie, w skład którego wchodzą systemy stanowiące znaczne zagrożenie dla zdrowia i bezpieczeństwa lub praw podstawowych Unii Europejskiej. Systemy wysokiego ryzyka dzielą się na dwie grupy – do pierwszej należeć mają przede wszystkim systemy SI będące elementami produktu przeznaczonego do użycia jako związane z bezpieczeństwem lub produkty objęte innymi przepisami harmonizacyjnymi UE, podlegające ocenie zgodności ex ante przeprowadzanej przez osoby trzecie. W skład drugiej grupy wchodzić zaś mają samodzielne systemy SI mające wpływ głównie na prawa podstawowe, których rodzaje zostały wyraźnie wymienione w załączniku III do projektu AIA. Określony w załączniku III wykaz systemów SI wysokiego ryzyka określa ograniczoną liczbę systemów SI, które zważywszy na dotychczas ujawnione ryzyko, zakwalifikowane zostały do systemów SI wysokiego ryzyka. Do tej kategorii zostały zaliczone m.in. systemy SI przeznaczone do stosowania w celu zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym" i „post factum", systemy SI przeznaczone do stosowania jako związane z bezpieczeństwem elementy procesów zarządzania i obsługi ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło i energię elektryczną czy systemy sztucznej inteligencji przeznaczone do wykorzystania w celu rekrutacji lub wyboru osób fizycznych.

> Rozwiązania algorytmiczne posiadające cechy sztucznej inteligencji (SI) pozwalają np. na usprawnienie procesów dokonywania skomplikowanych prognoz

Aby zapewnić możliwość szybkiego uzupełniania wykazu zastosowań SI, określonych w załączniku nr 3 do projektu AIA, Komisja Europejska została wyposażona w kompetencję do rozszerzenia tego katalogu, w określonych obszarach, w oparciu o wskazane w projekcie rozporządzenia kryteria oraz metodykę oceny ryzyka, co oznacza, że podmioty rozwijające systemy SI powinny na bieżąco obserwować aktywność Komisji Europejskiej w zakresie poszerzania katalogu systemów SI wysokiego ryzyka oraz starać się dokonywać wstępnej oceny, a przez to antycypować, czy rozwijane przez nich systemy mogą być w przyszłości zakwalifikowane jako systemy wysokiego ryzyka.

Rozliczalność systemów

Postanowienia projektu AIA dotyczące systemów SI wysokiego ryzyka ukierunkowane są przede wszystkim na zapewnienie tzw. rozliczalności (accountability) takich systemów, co oznacza zapewnienie możliwości przypisania odpowiedzialności za skutki ich działania. Powyższe wiąże się z wymogami przejrzystości (transparency) oraz wyjaśnialności (explainability) systemów SI.

Realizacji powyższych założeń służyć mają liczne wymogi określone w projekcie AIA, odnoszące się do systemów SI wysokiego ryzyka. Obejmują one m.in. konieczność wdrożenia i utrzymania systemów zarządzania ryzykiem, zapewnienie jakości danych treningowych, walidacyjnych i testowych, prowadzenie dokumentacji technicznej systemu, umożliwienie automatycznego rejestrowania zdarzeń, projektowanie i opracowywanie systemów w sposób zapewniający wystarczającą przejrzystość ich działania, zapewnienie w okresie wykorzystywania systemu SI nadzoru osoby fizycznej, jak również obowiązek projektowania i opracowania systemów, aby osiągały odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa. Projekt AIA nie określa zamkniętego katalogu sposobów, jak powyższe wymogi mają być realizowane. Wybór określonych metod pozwalających na zapewnienie zgodności systemów z wymogami projektowanej regulacji dostosowany ma być do specyfiki oraz ryzyka generowanego przez dany system. Naturalnie ciężar, a zatem także odpowiedzialność za dobór odpowiednich metod spoczywać mają na podmiotach obowiązanych. Taka metoda regulacji zwiastuje w niedalekiej przyszłości powstawanie rozlicznych norm ISO, kodeksów dobrych praktyk oraz publikacje różnych stanowisk nadzorczych, które będą wspierały podmioty rozwijające systemy SI w zapewnieniu zgodności z wymogami AIA.

> Stosowaniem rozwiązań bazujących na SI wiąże się wiele ryzyk, wśród których najczęściej wymienia się np. brak przejrzystości podejmowania decyzji

Niezwykle dynamiczny rozwój systemów SI stanowi ogromne wyzwanie dla instytucji odpowiedzialnych za stanowienie prawa. W istocie, podmioty takie stają w obliczu dylematów niemalże filozoficznych, dotyczących m.in. takich kwestii, jak relacje między człowiekiem a technologią, czy konieczności ważenia takich wartości, jak bezpieczeństwo oraz prawa podstawowe z jednej strony, a innowacyjność oraz rozwój technologii (która w założeniu również powinna służyć ludzkości) z drugiej.

Istotną kwestią jest również to, że interwencja legislacyjna dotycząca systemów SI nie może być wyłącznie reaktywna, tj. nie może, tak jak to ma miejsce zazwyczaj w stosowaniu prawa, stanowić wyłącznie odpowiedzi na zmiany społeczno-gospodarcze, które już nastąpiły. Z uwagi na dynamikę zmian technologicznych doniosłość wpływu systemów SI na zmiany społeczno-gospodarcze, charakter możliwych ryzyk związanych z wykorzystaniem systemów SI, a także uwzględniając fakt, że wiele ryzyk nie jest obecnie znanych, ani nawet możliwych do przewidzenia, prace legislacyjne dot. stworzenia ram prawnych dla systemów SI wykorzystywane są jako jeden z ważnych elementów realizacji polityk rozwoju sztucznej inteligencji. Dlatego również regulacjom tym stawia się podwójny cel, tj. zarówno ochronę bezpieczeństwa i praw podstawowych oraz wspieranie rozwoju oraz innowacyjności.

Niewątpliwie przed podmiotami projektującymi, rozwijającymi oraz wdrażającymi systemy SI wysokiego ryzyka stać będzie nie lada wyzwanie, natury operacyjnej, organizacyjnej, a także finansowej, związane z koniecznością dostosowania do wymogów prawnych dedykowanych wykorzystywaniu systemów SI. Czas pokaże, czy legislatorom udało się znaleźć odpowiedni balans pomiędzy zarządzaniem ryzykiem związanym ze zastosowaniem sztucznej inteligencji a wspieraniem innowacji technologicznych. /©℗