PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 118 (2316), 17 CZERWCA 2021 © PISM

BIULETYN

Unijny projekt regulacji sztucznej inteligencji

Stefania Kolarz, Oskar Szydłowski

Propozycja prawnego uregulowania sztucznej inteligencji (AI) na unijnym rynku ma przede wszystkim chronić prawa podstawowe i wartości UE. Jako pierwsza tego rodzaju regulacja na świecie ma szansę stać się wyznacznikiem standardów. Nowe wymogi mogą jednak w praktyce utrudnić dostęp podmiotów zagranicznych do rynku wewnętrznego oraz zmniejszyć konkurencyjność unijnych przedsiębiorców.

21 kwietnia br. Komisja Europejska (KE) zaproponowała rozporządzenie, które jest pierwszym na świecie projektem kompleksowego uregulowania AI. Dotychczas pojedyncze przepisy były przyjmowane jedynie na poziomie krajowym (np. definicja utworu wygenerowanego komputerowo w przepisach brytyjskich lub wymóg prawa niemieckiego, by w pojeździe autonomicznym był obecny kierowca). Państwa UE częściej korzystały z dokumentów politycznych, np. strategii dotyczącej AI (m.in. Francja, Estonia, Polska, Niemcy). Dzięki tej inicjatywie Unia ma więc szansę po raz kolejny – po rozporządzeniu o ochronie danych osobowych (RODO) – wyznaczyć światowe standardy normatywne.

Główne założenia projektu. Propozycja ma na celu zapewnienie przestrzegania etyki, poszanowania bezpieczeństwa, unijnych wartości i praw podstawowych w tworzeniu AI. Pewność prawa ma sprzyjać inwestycjom i rozwojowi AI w UE, wzmacniać unijną konkurencyjność i chronić suwerenność cyfrową Wspólnoty.

Projekt przewiduje zharmonizowane zasady rozwijania, wprowadzania do obrotu i stosowania AI w Unii. Opiera się na podziale systemów AI na obarczone ryzykiem różnego stopnia: nieakceptowalnym, wysokim, niskim i minimalnym. Do pierwszej kategorii – zakazanej – kwalifikuje m.in. systemy wykorzystujące techniki podprogowe wpływające na zachowanie osoby w sposób, który powoduje lub może spowodować krzywdę jej lub innym, albo dokonujące oceny wiarygodności społecznej (*social scoring*). Projekt najszerzej reguluje systemy AI wysokiego ryzyka, stosowane np. w transporcie, do oceny wniosków kredytowych lub decyzji o przyznaniu świadczeń socjalnych. Będą one musiały spełnić szereg wymogów, m.in. odpowiedniego testowania, oceny zgodności ze standardami UE, rejestracji w unijnej bazie danych i informacji dla użytkowników. Te obowiązki będą dotyczyć producentów i dostawców systemów AI niezależnie od tego, czy mają siedzibę w Unii, czy poza nią, i użytkowników w Unii. W przypadku pozostałych systemów AI (np. chatbotów) propozycja przewiduje przede wszystkim obowiązek informowania użytkowników, że wchodzą w interakcję z AI.

Za nieprzestrzeganie przepisów będzie grozić wyższa kara niż w przypadku RODO – do 6% całkowitego rocznego światowego obrotu. W państwach członkowskich za wykonywanie rozporządzenia będą odpowiedzialne organy wskazane przez władze krajowe, które na szczeblu unijnym będą tworzyć z Europejskim Inspektorem Danych Osobowych (EIDO) Europejską Radę Sztucznej Inteligencji (ERSI) pod przewodnictwem Komisji. Jej zadaniem będzie doradzanie KE i koordynacja działań organów państw członkowskich.

Regulacja w praktyce. Projekt rozporządzenia jest popierany przez EIDO, który nalega na bardziej rygorystyczne podejście. Choć za szeroką regulacją opowiadają się np. Niemcy, wiele państw członkowskich obawia się spowolnienia rozwoju technologicznego. Na forum UE za ograniczeniem regulacji AI do niezbędnego minimum i korzystaniem z niewiążących instrumentów opowiedziało się 14 państw, w tym Polska.

Propozycja w obecnej formie zawiera wiele wyłączeń i nieprecyzyjnych definicji. Przykładowo, zakaz biometrycznej identyfikacji w czasie rzeczywistym dotyczy jedynie organów ścigania w przestrzeni publicznej – nie obejmie więc przestrzeni prywatnej, innych organów publicznych lub podmiotów prywatnych. Ponadto nie będzie obowiązywał w przypadku użycia systemu do

przeciwdziałania terroryzmowi czy zagrożeniu życia lub bezpieczeństwa osób, co pozostawia duże możliwości interpretacji.

Kategoryzacja ryzyka została przygotowana przez KE bez podania jednoznacznych kryteriów. Wśród sposobów oceny ryzyka jest np. ocena na podstawie możliwości zastosowania. Daje to szerokie pole do interpretacji – ponieważ modele można dostosować do dowolnych zastosowań, oceniający będą w stanie uzasadnić ocenianie każdego modelu. Tworzy to niestabilne warunki do rozwoju AI, gdyż kategorie ryzyka mogą zostać dowolnie aktualizowane. Jako system wysokiego ryzyka sklasyfikowano np. algorytmy czarnej skrzynki (*black box*), które funkcjonują w szczególny sposób – model jest w nich konstruowany po dostarczeniu danych, bez wkładu ludzkiego. W zwykłych modelach precyzuje się algorytm, według którego model ma się uczyć, a w przypadku czarnych skrzynek model samodzielnie decyduje, jak dobierać zmienne, ustalać wagi, które dane pominąć itd. Nie pozwala to określić, które zmienne, w jaki sposób i dlaczego zostały wykorzystane. Charakteryzują się one wysoką skutecznością (dopasowaniem), jednak nie spełniają wymogów analizy ryzyka. Ich faktyczne wykluczenie jest istotnym ograniczeniem innowacyjności w UE.

Choć propozycja regulacji zawiera twierdzenie o prymacie człowieka nad technologią, nie uwzględnia perspektywy użytkowników. W szczególności pominięto rozwiązania gwarantujące jednostkom podejmowanie skutecznych działań prawnych, m.in. specjalnego mechanizmu ubiegania się o odszkodowanie w wyniku nieuprawnionej czy nieprzewidzianej działalności systemu AI.

Międzynarodowy wymiar regulacji. Propozycja KE jest obecnie najdalej idącym planem regulacji AI. Wpisuje się jednak w trendy widoczne w innych krajach, kładąc nacisk na analizę ryzyka i zagrożeń związanych z AI oraz przygotowywanie planów na wypadek ich wystąpienia. Ze względu na rosnące i zmieniające się w czasie ryzyko systemy AI powinny być niezależnie testowane w czasie rzeczywistym, podczas ich funkcjonowania i później. Takie podejście można zaobserwować w lokalnych regulacjach, np. w USA – w Wirginii i Kalifornii. Punkty wspólne mogą stanowić podstawę do negocjowania regulacji w formacie transatlantyckim. Mało prawdopodobna jest jednak akceptacja przez USA unijnej definicji wysokiego ryzyka czy rozbudowanego systemu monitorowania technologii. Współpraca transatlantycka mogłaby korzystać z już wypracowanych praktyk, np. wzajemnego uznawania przepisów i dopuszczania podmiotów do obu rynków. O chęci kooperacji świadczy pozytywny odbiór unijnego projektu wyrażony przez Jake'a Sullivana, doradcę Joe Bidena ds. bezpieczeństwa narodowego.

Amerykańskie firmy technologiczne, w tym Google i Microsoft, zapowiedziały kwestionowanie propozycji na drodze sądowej. Systemy AI tych firm w dużym stopniu zostały dostosowane („wytrenowane") na podstawie danych obywateli UE, są też bezpośrednio wykorzystywane w usługach oferowanych na rynku unijnym. Oznacza to, że regulacja wymusi na tych firmach wdrożenie wszystkich mechanizmów analizy ryzyka. Nie będzie ponadto możliwe ominięcie regulacji dzięki wydzieleniu systemów AI do osobnej spółki działającej poza rynkiem UE, bo ona też będzie objęta przepisami. W konsekwencji niektóre usługi mogą nie być oferowane w UE lub powstaną modele AI przeznaczone na ten rynek. Barierę wejścia będą mogły pokonać jedynie większe firmy. Dodatkowe obowiązki unijnych podmiotów mogą utrudnić ich rozwój oraz ekspansję na rynki zagraniczne – istotna część zasobów zostanie przeznaczona na spełnienie nowych wymogów, podobnie jak w przypadku RODO. Niektóre zastosowania AI, np. wykorzystujące biometrykę, będą całkowicie zakazane, czego rezultatem – dopóki podobne przepisy nie będą funkcjonować globalnie – stanie się oddanie w tym obszarze pola firmom amerykańskim i chińskim.

Wnioski i perspektywy. Unijne rozporządzenie jako pierwsza kompleksowa regulacja AI na świecie może podzielić sukces RODO. KE zakłada jego elastyczność i dostosowanie do potencjalnego rozwoju AI bez konieczności regularnego nowelizowania. Rozporządzenie może przyczynić się jednak do spowolnienia tempa rozwoju AI oraz zmniejszenia konkurencyjności unijnych przedsiębiorców. Mimo przewidzianej w projekcie pomocy państw członkowskich dla małych i średnich firm (m.in. pierwszeństwo w dostępie do specjalnych środowisk testowania, ułatwienia uzyskiwania informacji o nowych przepisach, niższe koszty oceny zgodności) może w praktyce utrudnić przedsiębiorcom, w tym polskim, dostęp do wspólnego rynku.

Proponowana regulacja jest potrzebna z punktu widzenia ochrony praw człowieka, ale powinna być dostosowana do realnych możliwości egzekwowania przestrzegania jej postanowień. By zmaksymalizować jej skuteczność, nie poświęcając własnych przewag konkurencyjnych, w trakcie konsultacji wewnętrznych w UE Komisja powinna zachęcać zagranicznych partnerów (np. USA) do przyjęcia podobnych standardów, w tym ochrony praw człowieka, m.in. na forum WTO czy OECD. Na poziomie wewnętrznym dodatkowym wsparciem dla firm zarejestrowanych w UE mogłoby być utworzenie nowych programów finansowania badań nad AI ze środków unijnych.