Nowy projekt Rozporządzenia w sprawie AI (sztucznej inteligencji) z 11 listopada 2022 r. – kluczowe założenia

Według danych Eurostat w 2020 r. jedynie 0,7% przedsiębiorstw w UE zatrudniających co najmniej 10 osób korzystało z aplikacji AI, a usługa czatu, w której chatbot lub wirtualny agent generował odpowiedzi w języku naturalnym dla klientów, była wykorzystywana w 2% przedsiębiorstw. Taki sam odsetek przedsiębiorstw, 2%, wykorzystywał roboty usługowe, które charakteryzują się pewnym stopniem autonomii, na przykład do wykonywania zadań porządkowych, niebezpiecznych lub powtarzalnych, takich jak sprzątanie substancji trujących, sortowanie przedmiotów w magazynie, pomaganie klientom w zakupach lub w punktach płatniczych itp.[1]

Brak regulacji w zakresie wytwarzania, oferowania i użytkowania systemów AI stwarza stan znacznej niepewności dla wszystkich uczestników rynku, zwłaszcza w odniesieniu do najbardziej zaawansowanych systemów. W kwietniu 2021 r. Komisja Europejska zaprezentowała swój pakiet AI, w którym znalazł się m.in. wniosek dotyczący nowego projektu rozporządzenia ustanawiającego zharmonizowane zasady dotyczące sztucznej inteligencji (Akt o sztucznej inteligencji). W ciągu minionego roku dwukrotnie dostrzeżono potrzebę zaktualizowania i dostosowania proponowanych przepisów, by lepiej odzwierciedlały specyfikę zaawansowanych systemów AI i zapewniały większe bezpieczeństwo ich użytkownikom.

Nowa wersja projektu Aktu o sztucznej inteligencji z dnia 11 listopada 2022 r. wprowadza pewne zmiany w stosunku do dwóch poprzednich wersji. Definicja systemu sztucznej inteligencji przyjęta w uprzedniej wersji aktu została jedynie lekko zmodyfikowana. W nowym brzmieniu uwzględnia ona elementy autonomii, jaką posiada AI[2].

Przyjęto, iż systemem sztucznej inteligencji jest system, który został zaprojektowany do działania z elementami autonomii i który na podstawie danych i informacji dostarczonych z zewnątrz - przez człowieka i/lub maszynę, wnioskuje, w jaki sposób osiągnąć cele określone przez człowieka. System ma przy tym wykorzystywać uczenie maszynowe (machine learning) i/lub podejścia oparte na logice i wiedzy.

"system sztucznej inteligencji (system AI) oznacza system, który został zaprojektowany do działania z elementami autonomii i który na podstawie danych i informacji dostarczonych przez maszynę i/lub człowieka, wnioskuje, w jaki sposób osiągnąć określony zestaw celów, wykorzystując uczenie maszynowe i/lub podejścia oparte na logice i wiedzy, oraz wytwarza generowane przez system dane wyjściowe, takie jak treści (generatywne systemy AI), przewidywania, zalecenia lub decyzje, wpływające na środowisko, z którym system AI wchodzi w interakcje."

Katalog podmiotów objętych przepisami obecnej wersji rozporządzenia, nie uległ zmianie w stosunku do poprzedniej wersji tego aktu. Aktualna propozycja zachowała nowe kategorie podmiotów wprowadzone w uprzedniej wersji, wobec których rozporządzenie będzie miało zastosowanie. Są to:[3]

- importerzy i dystrybutorzy systemów AI;
- producenci produktów wprowadzających na rynek lub do użytku system AI wraz ze swoim produktem i pod własną nazwą lub znakiem towarowym;
- upoważnieni przedstawiciele dostawców, którzy mają siedzibę w Unii Europejskiej.

SOŁTYSIŃSKI KAWECKI SZLĘZAK

[1] *Uhttps://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210413-1*
[2] *Art. 3 (1) Projektu Rozporządzenia, https://artificialintelligenceact.eu/wp-content/uploads/2022/11/AIA-CZ-Draft-General-Approach-11-Nov-22.pdf*
[3] *Artykuł 2 (1) (d) – (f), Projektu rozporządzenia.*

Wyłączenia

Projekt zawiera również pewne wyłączenia[4], które można podzielić na kilka zasadniczych kategorii. Przepisy rozporządzenia nie będą miały zastosowania wobec:

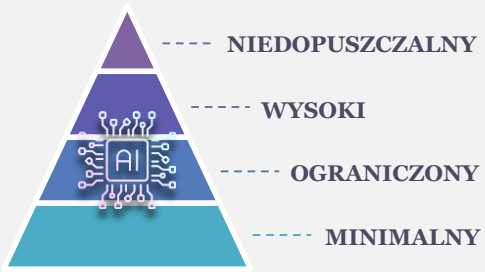
Systemów AI, przeznaczonych do celów nie objętych zakresem prawa Unii, zwłaszcza działań dotyczących celów wojskowych, obronnych lub bezpieczeństwa narodowego, niezależnie od rodzaju podmiotu prowadzącego te działania.

Systemów AI opracowanych i wprowadzonych do użytku wyłącznie w celu prowadzenia badań naukowych i rozwoju (R&D).

Organów publicznych w państwie trzecim oraz organizacji międzynarodowych, jeżeli wykorzystują systemy AI w ramach umów międzynarodowych dotyczących współpracy w zakresie egzekwowania prawa i współpracy sądowej z Unią lub z co najmniej jednym państwem członkowskim.

Użytkowników będących osobami fizycznymi korzystającymi z systemów AI w ramach czysto osobistej działalności nieprofesjonalnej, z pewnymi wyłączeniami.

Kluczowa jest także zmiana w zakresie parametrów klasyfikacji systemów do poszczególnych grup ryzyka: niedopuszczalnego, wysokiego, ograniczonego i minimalnego.



Systemy AI wysokiego ryzyka

W praktyce dyskusje i kontrowersje budzą kryteria klasyfikacji systemów AI, zwłaszcza systemów wysokiego ryzyka. Wg danych Eurobarometru[5] nieco ponad połowa Europejczyków (51%) uważa, że w celu zapewnienia etycznego stosowania systemów AI konieczna jest interwencja polityki publicznej w tym zakresie. Aż 80% respondentów uważa, że powinni być informowani, gdy usługa cyfrowa lub aplikacja mobilna z której korzystają wykorzystuje AI.

W obecnym kształcie projekt przewiduje, iż systemem AI o najwyższym stopniu ryzyka jest system, który:

- jest produktem objętym właściwymi unijnymi przepisami, jeżeli wymaga się od niego przeprowadzenia oceny zgodności w celu wprowadzenia do obrotu lub oddania do użytku[6].
- został wymieniony w załączniku III do rozporządzenia, chyba, że rezultaty działania tego systemu są czysto pomocnicze w odniesieniu do odpowiedniego działania lub decyzji, która ma być podjęta, i nie jest prawdopodobne, by prowadziły do znacznego zagrożenia dla zdrowia, bezpieczeństwa lub praw podstawowych[7]. Są to m.in.:

[4] *Artykuł 2 ust. 3, 6 i 7 projektu rozporządzenia.*
[5] *https://ec.europa.eu/commission/presscorner/detail/es/ip_20_383*
[6] *Art. 6 ust. 1 projektu rozporządzenia.*
[7] *Art. 6 ust. 3 projektu rozporządzenia.*

- systemy zdalnej identyfikacji biometrycznej,
- systemy kontroli dostępu osób fizycznych do instytucji, programów edukacyjnych czy szkoleniowych,
- systemy przeznaczone do stosowania w celu rekrutacji lub selekcji osób fizycznych i.a. do zamieszczania ukierunkowanych ogłoszeń o pracę, analizowania i filtrowania podań o pracę oraz do oceny kandydatów,
- systemy przeznaczane do oceny zdolności kredytowej osób fizycznych lub ustalenia ich punktacji kredytowej (z pewnymi wyjątkami),
- systemy przeznaczone do wykorzystania przez organy ścigania lub w ich imieniu do oceny wiarygodności dowodów w trakcie dochodzenia lub ścigania przestępstw,
- systemy przeznaczone do stosowania do oceny ryzyka wobec osób fizycznych oraz ustalania cen ubezpieczeń na życie i ubezpieczeń zdrowotnych (z wyjątkiem systemów AI wprowadzanych do użytku przez dostawców będących mikroprzedsiębiorstwami i małymi przedsiębiorstwami).

Dodatkowe wymogi bezpieczeństwa

Z perspektywy uczestników rynku poza skutecznością (efektywnością) rozwiązań technologicznych, szczególnie istotny jest aspekt bezpieczeństwa. Z tych względów przewidziano, iż nawet systemy AI ogólnego przeznaczenia, które mogą być stosowane jako systemy wysokiego ryzyka lub jako elementy tych systemów powinny spełniać dodatkowe wymogi w zakresie bezpieczeństwa. Przede wszystkim powinny one[8]:

- posiadać system zarządzania ryzykiem[9];
- spełniać wymogi w zakresie zarządzania danymi[10];
- posiadać odpowiednią dokumentację techniczną[11] i instrukcję użytkowania[12];
- odpowiedni poziom dokładności, odporności i bezpieczeństwa cybernetycznego, oraz zachowywać się spójnie pod tymi względami w całym cyklu życia[13].

Poza aspektem technicznym, nacisk położono również na kwestie etyczne i te związane z ochroną prywatności użytkowników systemów AI. Projekt przewiduje, iż zakazane są m.in.[14]:

- systemy AI stosujące techniki podprogowe poza świadomością użytkownika, których celem lub skutkiem jest istotne zniekształcenia jego zachowania w sposób, który może spowodować u niego (lub innej osoby) szkody fizyczne lub psychiczne;
- systemy AI wykorzystujące podatność określonej grupy osób ze względu na ich wiek (np. dzieci lub osób starszych), niepełnosprawność lub sytuację społeczną lub ekonomiczną, by istotnie zniekształcić zachowania takiej osoby w sposób, który może powodować u niej (lub u innej osoby) szkody fizyczne lub psychiczne;
- systemy AI do oceny lub klasyfikacji osób fizycznych w określonym czasie na podstawie ich zachowań społecznych lub znanych/przewidywanych cech osobowych lub osobowościowych, które prowadzą do ich szkodliwego lub niekorzystnego traktowania (dyskryminacja) ;
- systemy identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej przez organy ścigania lub w ich imieniu do celów egzekwowania prawa, chyba, że jest to absolutnie niezbędne np. w celu ułatwienia poszukiwania konkretnych potencjalnych ofiar przestępstw, wykrycia lub identyfikacji osoby fizycznej w celu prowadzenia dochodzenia karnego, czy zapobiegania konkretnemu i znaczącemu zagrożeniu dla infrastruktury krytycznej, życia, zdrowia lub bezpieczeństwa lub zapobieganie atakom terrorystycznym.

SOŁTYSIŃSKI KAWECKI SZLĘZAK

[8] *Art. 4b (1) projektu Rozporządzenia*
[9] *Art. 9 projektu Rozporządzenia.*
[10] *Artykuł 10 projektu Rozporządzenia.*
[11] *Artykuł 11 Rozporządzenia.*
[12] *Art. 13 projektu Rozporządzenia.*
[13] *Artykuł 15 projektu Rozporządzenia.*
[14] *Artykuł 5 projektu Rozporządzenia.*

Biorąc pod uwagę duża liczbę użytych pojęć generalnych i zwrotów nieostrych, takich jak „*istotne zniekształcenie*”, „*znaczne zagrożenie*” czy „*absolutnie niezbędne*”, w praktyce z pewnością pojawią się wątpliwości co do prawidłowej interpretacji poszczególnych pojęć zastosowanych w rozporządzeniu. Obecnie brak jest jeszcze wystarczającej praktyki organów i orzecznictwa w tym obszarze (na poziomie krajowym i unijnym). Wydaje się jednak, iż podobnie jak w innych przypadkach, interpretacja będzie dokonywana z uwzględnieniem przyjętych przez ustawodawcę celów rozporządzenia i funkcji, jakie AI ma pełnić w wymiarze społecznym i gospodarczym.

Odpowiedzialność – dotkliwe sankcje finansowe

Ze względu na istnienie ryzyka wystąpienia szkody – materialnej lub niematerialnej – w zależności od okoliczności i zastosowania danego systemu AI, w celach prewencyjnych w projekcie przewidziano znaczące kary finansowe za nieprzestrzeganie jego przepisów. Przykładowo, złamanie któregokolwiek z zakazów, o których mowa w art. 5 projektu rozporządzenia (tj. opisanych powyżej praktyk zakazanych), ma być karane **grzywną administracyjną w wysokości do 30 000 000 EUR lub**, jeżeli sprawcą jest przedsiębiorstwo, **do 6 % jego całkowitego światowego rocznego obrotu za poprzedni rok obrotowy.** W przypadku małych i średnich przedsiębiorstw, w tym przedsiębiorstw rozpoczynających działalność, grzywny te mają wynosić do 3% ich rocznego światowego obrotu za poprzedni rok finansowy[15].

dr hab. Ewa Skrzydło-Tefelska
Starszy Partner, radca prawny
✆ +48 608 420 802
✉ ewa.skrzydlo-tefelska@skslegal.pl

Marta Kowalczuk-Kędzierska
Prawnik
✆ +48 883 391 699
✉ marta.kowalczuk-kedzierska@skslegal.pl

Warszawa
Jasna 26, 00-054 Warszawa
T +48 22 608 70 00
F +48 22 608 70 70
E office@skslegal.pl

Katowice
Wojewódzka 10, 40-026 Katowice
T +48 32 731 59 86
F +48 32 731 59 90
E office.katowice@skslegal.pl

Poznań
Mickiewicza 35, 60-837 Poznań
T +48 61 856 04 20
F +48 61 856 05 67
E office.poznan@skslegal.pl

Wrocław
Plac Solny 16, 50-062 Wrocław
T +48 71 346 77 00
E office.wroclaw@skslegal.pl

www.skslegal.pl

[15] *Artykuł 71 (3) projektu Rozporządzenia.*