KONIECZNY WIERZBICKI
KANCELARIA RADCÓW PRAWNYCH

Kraków, dnia 06 sierpnia 2021 r.

ARTIFICIAL INTELLIGENCE ACT

stanowisko Konieczny Wierzbicki Kancelaria Radców Prawnych sp.p.
w ramach konsultacji publicznych nad projektem rozporządzenia unijnego

I. Uwagi ogólne

- Generalnie przedstawiciele biznesu, których opinie poznaliśmy, są pozytywnie nastawieni do Artificial Intelligence Act i widzą potrzebę uregulowania wykorzystywania systemów AI. Kierunek regulacji jest dobry, ale są potrzebne pewne poprawki, które osłonią biznes przed istotną utratą konkurencyjności na rynku globalnym.

II. Definicja systemu AI:

- Co do zasady, jest to prawidłowe podejście do scharakteryzowania AI na potrzeby regulacji prawnych. Definicja ta nie wydaje się za szeroka (przy założeniu, że są wyszczególnione różne poziomy ryzyka). Trudno na ten moment wyobrazić sobie inne, lepsze podejście.
- Zapewnienie skutecznego i przejrzystego sposobu aktualizacji tej definicji jest kluczowe, gdyż na pewno definicja ta będzie musiała być sukcesywnie aktualizowana. Można też spekulować, że bez aktywnego, dynamicznego podejścia do definiowania systemów AI w pewnym momencie rozwój takich technologii jak: komputery kwantowe, blockchain, cloud, techniki deep learningu – może doprowadzić do sytuacji, w której nie będziemy już w stanie zdefiniować czym jest system AI. W tym zakresie należy także zwrócić uwagę na konieczność odpowiedniego zapisu o vacatio legis, które to miałoby zastosowanie do ewentualnych zmian w zakresie wykazu technik i podejść charakteryzujących systemy AI. Skoro bowiem wykaz ten ma kluczowe znaczenie dla ogólnego zakresu zastosowania rozporządzenia, nie ma wątpliwości, że rynek powinien mieć zagwarantowany odpowiednio długi czas na dostosowanie prowadzonej działalności do wymogów rozporządzenia.
- Być może definicja ta powinna jednak w pewnym zakresie nie tylko odnosić się do stosowanych technik, ale i do celów (kierunków działań) jakie są wyznaczane algorytmom. Z jednej strony, niewątpliwie cele (kierunki działań) powinien ustalać wyłącznie człowiek. Będzie to chroniło przed zbyt daleko idącą „autonomizacją" określania celów przez sam algorytm (przykład: algorytm rekomendujący terapię u chorego na chorobę zakaźną nie może dojść do konkluzji, że rozwiązaniem jest uśmiercenie pacjenta). Z drugiej strony, definicja AI powinna uwzględniać sytuację, w której algorytm niedopuszczalny do stosowania w danym celu (np. do social scoringu), będzie mógł być stosowany do innego celu (np. wykrywania chorób).
- W kontekście otwartej definicji systemów AI, istotną kwestią może być ryzyko dywergencji w zakresie praktycznego stosowania regulacji w poszczególnych Państwach Członkowskich UE, wynikające z różnej praktyki organów krajowych, jak i

okazjonalnych prób pośredniej implementacji dodatkowych regulacji w zakresie AI w krajowym ustawodawstwie. Problem ten może dotknąć w szczególności branży finansowej, która to w dużej mierze prowadzi działalność w oparciu o regulacje o charakterze pozaustawowym, takich jak np. rekomendacje czy wytyczne organów nadzoru. Przydatne mogą okazać się mechanizmy weryfikacji stanu prawnego w poszczególnych Państwach Członkowskich UE dla utrzymania jednolitości i spójności regulacyjnej.

III. Odpowiedzialność za systemy AI:

- Do rozważenia pozostaje doprecyzowanie kwestii odpowiedzialności i obowiązków, szczególnie w przypadku złożonych systemów AI składających się z różnego rodzaju bibliotek i rozwiązań tworzonych przez odrębne podmioty. Innymi słowy, dany system AI oferowany użytkownikowi końcowemu może by zbudowany z kilku różnych (pod)systemów opartych o AI, może być konglomeratem wielu pomniejszych systemów AI. Dla usprawnienia kontraktowania między dostawcami różnych systemów AI składających się na produkt finalny dla użytkownika, regulacja unijna powinna zapewniać transparentne reguły rozkładu ryzyk i odpowiedzialności między tymi dostawcami (możliwość tworzenia „łańcuchów" odpowiedzialności, jak np. ma to miejsce w przypadku instytucji powierzenia i podpowierzenia przetwarzania danych osobowych na gruncie GDPR). Można ponadto rozważyć wprowadzenie regulacji, które pozwolą dostawcy systemu AI wyegzekwować od dostawców pomniejszych systemów AI informacje w zakresie jakości danych, zasad/warunków trenowania AI przed dostawcę pomniejszego sytemu AI, itd. – tak by dostawca produktu finalnego do użytkownika mógł przekazać użytkownikowi kompletne informacje dotyczące zakresu, sposobu użycia AI, danych na których algorytm operuje, ryzyk szkód, itd.
- Wbrew pozorom użytkownicy systemów AI mają bardzo duży wpływ na ich pracę (np. poprzez zasilanie algorytmu machine learningowego nowymi danymi). Do rozważenia pozostaje zatem kwestia rozłożenia obowiązków pomiędzy użytkowników a dostawców systemów AI w tym zakresie (może to zostać pośrednio zaadresowane w aspekcie obowiązków informacyjnych wobec użytkowników systemów AI).

IV. Jakość danych:

- być może jeszcze dodatkowego podkreślenia wymaga kwestia zapewnienia akuratności (accuracy) danych jakimi zasilany jest algorytm. Dane dotyczące np. uśrednionych warunków pogodowych w Stanach Zjednoczonych mogą nie być odpowiednie/adekwatne do zastosowania w systemie AI adresowanym do użytkownika z Polski (gdzie uśrednione warunki pogodowe mogą być zupełnie inne). Wobec powyższego, być może należałoby położyć większy akcent na potrzebę testowania algorytmów, w szczególności testowanie w warunkach rzeczywistych.
- nie ma możliwości zapewnienia by dane i ich zbiory były bezbłędne. Konieczne jest zatem urealnienie tych wymagań. Możliwe jest jedynie dążenie do minimalizacji ilości błędów. Pożądane wydaje się doprecyzowanie w projekcie Artificial Intelligence Act, jak należy rozumieć w praktyce pojęcie bezbłędności danych – czy jako oprogramowanie w 100% wolne od błędów, czy np. w 99%.
- Istotne wydaje się zapewnienie mechanizmów i/lub określenie standardów pozwalających na skuteczną weryfikację i ocenę systemów AI przez jednostki notyfikowane. Na ten moment można przypuszczać, że w praktyce weryfikacja

będzie opierała się o analizę dokumentacji danego systemu AI, dostarczoną przez dostawcę tego systemu, i/lub pewną próbkę danych. Ramy prawne dopuszczające weryfikację systemu AI w oparciu o samą analizę dokumentacji i/lub małą próbkę danych mogą skutkować tym, że wyniki weryfikacji nie będą reprezentatywne/miarodajne.

V. Obowiązki informacyjne:

- Być może zakres obowiązków informacyjnych wobec osób, które to korzystają z systemów AI powinien zostać uszczegółowiony. Obowiązkom tym być może powinna być nadana większa waga, tak by każdy kto styka się z AI miał tego pełną świadomość (nie tylko co do samego faktu użycia AI, ale zakresu, sposobu i danych na których algorytm operuje).
- Użytkownik powinien otrzymać możliwie dokładną informację jakie szkody może sobie wyrządzić korzystając / godząc się na korzystanie z danego systemu AI (istotne zwłaszcza w przypadku systemów AI wysokiego ryzyka). Sugestia ta może w praktyce skutkować zalewem użytkowników komunikatami analogicznymi do informowania o polityce „cookies" czy zasadach przetwarzania danych osobowych, tym niemniej immanentne ryzyka związane z systemami AI (np. *algorithmic bias* – przechył algorytmiczny) mogą przeważać nad nieudogodnieniami generowanymi dla użytkowników.

VI. Obowiązki związane z AI wysokiego ryzyka:

- Do rozważenia pozostaje odejście od wymogu wytłumaczalności algorytmu, na rzecz testowania celem dopuszczenia algorytmu do użycia. Wraz z rosnącym rozwojem technologii sztucznej inteligencji zapewnienie wymogu wytłumaczalności algorytmu będzie coraz trudniejsze. Tymczasem należycie przetestowane systemy AI nie powinny stanowić podwyższonego zagrożenia, nawet jeśli nie będzie możliwe w pełni wytłumaczenie decyzji podjętych przez taki algorytm AI. Przykładem dla podejścia tego rodzaju może stanowić branża farmaceutyczna, gdzie dopuszczone do stosowania zostają należycie przetestowane produkty lecznicze, nawet jeśli ich dokładny mechanizm działania nie jest do końca poznany.
- Generalnie zwiększenie nacisku na testowanie algorytmów AI powinno usprawnić proces komercjalizacji systemów AI i zracjonalizować koszty prac badawczo-rozwojowych nad produktami implementującymi algorytmy AI.
- W przypadku zapewnienia możliwości modyfikowania kategorii systemów AI wysokiego ryzyka w drodze aktów delegowanych, należy zwrócić uwagę na konieczność odpowiedniego zapisu o vacatio legis, które miałoby zastosowanie do ewentualnych zmian w tym zakresie. Uznanie danego systemu za sztuczną inteligencję wysokiego ryzyka ma kluczowe znaczenie dla zakresu obowiązków obciążających dostawcę takiego systemu. Tym samym rynek powinien mieć zagwarantowany odpowiednio długi czas na dostosowanie prowadzonej działalności do wymogów charakterystycznych dla systemów AI wysokiego ryzyka.

VII. Klasyfikacja AI ze względu na ryzyko:

- Być może potrzebne jest utworzenie nowej kategorii systemów AI umiejscowionej pomiędzy systemami AI wysokiego ryzyka a systemami AI niskiego ryzyka, np. systemy AI średniego ryzyka. Trudno bowiem zakwalifikować do tej samej kategorii systemy, które potencjalnie zagrażają życiu i zdrowiu oraz systemy, które wiążą się

jedynie z potencjalną stronniczością algorytmu mającą wpływ na zakres dostępu do usług (np. system oceny zdolności kredytowej).

- Niektóre systemy AI zakwalifikowane do kategorii wysokiego ryzyka z takim ryzykiem nie będą związane, a z drugiej strony inne systemy kwalifikowane jako systemy AI niskiego ryzyka już z takim ryzykiem mogą się wiązać. Zakres AI wysokiego ryzyka być może powinien zostać zrewidowany (również w kontekście ewentualnego wyodrębnienia systemu AI średniego ryzyka).