

Warszawa, dnia 31 sierpnia 2021 r.

Pan Janusz Cieszyński
Sekretarz Stanu
w Kancelarii Prezesa Rady Ministrów

Szanowny Panie Ministrze,

Unia Metropolii Polskich im. Pawła Adamowicza przedstawia uwagi do projektu rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}.¹

I. Uwagi ogólne.

1. Ogólna charakterystyka i cel rozporządzenia

Projekt rozporządzenia w sprawie sztucznej inteligencji jest aktem prawnym, który istotnie wpłynie na stopień innowacyjności administracji publicznej. Obecnie coraz więcej systemów teleinformatycznych, aplikacji i produktów ICT wykorzystuje rozwiązania oparte o technologię uczenia maszynowego. Wykorzystywanie tego rodzaju technologii zwiększa efektywność operacji i szybkość ich wykonywania. Mechanizmy sztucznej inteligencji są wykorzystywane w działaniach wewnątrz organizacji, np. do bieżącego zarządzania dokumentacją, jako element zwiększający bezpieczeństwo dostępu do zasobów teleinformatycznych, ale także pomieszczeń. Mechanizmy sztucznej inteligencji są również wykorzystywane w działaniach, które mają na celu zwiększenie bezpieczeństwa i porządku publicznego oraz w kontaktach z mieszkańcami. W szczególności w zakresie efektywności w bieżącej obsłudze mieszkańców. Z pewnością rozwój sztucznej inteligencji w przyszłości wpłynie na możliwość ich wykorzystywania w coraz bardziej zaawansowanych procesach, w tym w procesach tworzenia, jak i stosowania prawa.

W ocenie Unii Metropolii Polskich przyszłe regulacje Unii Europejskiej muszą stanowić wsparcie w rozwoju systemów sztucznej inteligencji oraz wdrożeniu technik w działalności sektora prywatnego i publicznego. Należy wskazać, że większość strategii państw członkowskich Unii Europejskiej podkreśla konieczność wsparcia rodzimego przemysłu i nauki w rozwoju sektora AI oraz jednocześnie akcentuje konieczność wdrażania tej technologii w sektorze publicznym, jako katalizatora dla prac badawczych i biznesowych.²

Nie jest zasadne tworzenie ram prawnych regulujących wykorzystanie sztucznej inteligencji, która w założeniu kładzie nacisk na zakazy wykorzystywania tych narzędzi w określonych obszarach. Świadczy o tym nie tylko układ projektu rozporządzenia oraz treść przepisów normatywnych, ale również motywy

¹ <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206&from=EN>

² Przykładowo Polska Załącznik do uchwały nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. (poz. 23) stanowiąca Załącznik do uchwały nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. (poz. 23) na str. 76 wskazuje, że jednym z celów Polityki jest „Zwiększenie liczby zamówień na AI w sektorze publicznym, w tym administracji rządowej, samorządowej oraz w spółkach Skarbu Państwa i spółkach komunalnych jednostek samorządu terytorialnego, dzięki rozwojowi narzędzi opracowanych przez Program GovTech Polska”

rozporządzenia, które akcentują niebezpieczeństwa wykorzystania tej technologii a dopiero następnie wskazują możliwość wykorzystania tych systemów pod określonymi warunkami.

W zależności od poziomu ryzyka związanego z bezpieczeństwem użytkowników i prawami podstawowymi Komisja proponuje cztery kategorie ryzyka:

- zabronione będą systemy AI o niedopuszczalnym poziomie ryzyka (oceny punktowe obywateli stosowane przez organy publiczne, wykorzystywanie podatności dzieci, stosowanie technik podprogowych i systemów identyfikacji biometrycznej w czasie rzeczywistym w publicznie dostępnej przestrzeni do celów egzekwowania prawa),
- systemy AI o wysokim poziomie ryzyka (związane z infrastrukturą krytyczną, kształceniem lub szkoleniem zawodowym, aktywnością na rynku pracy i wyborem potencjalnych pracowników, podstawowymi usługami prywatnymi i publicznymi, egzekwowaniem przepisów, zarządzaniem migracjami, azylem i kontrolą granic, sprawowaniem wymiaru sprawiedliwości i procesami demokratycznymi),
- AI o ograniczonym stopniu ryzyka (wyraźne ryzyko ingerencji, np. poprzez stosowanie wirtualnych doradców) nałożone zostaną szczególne wymagania dotyczące przejrzystości, a użytkownicy będą musieli mieć świadomość, że wchodzi w interakcję z maszyną,
- wszystkie inne systemy AI obarczone minimalnym poziomem ryzyka (np. oparte na AI gry wideo lub filtry antyspamowe) będą mogły być rozwijane i wykorzystywane zgodnie z obowiązującymi przepisami bez dodatkowych wymogów prawnych.

Uważamy, że za wcześnie jest na określenie tak kategorycznego podziału systemów AI na poziomie aktu jakim jest Rozporządzenie UE. W szczególności podział nie powinien odwoływać się do sektorów, lecz skutków wykorzystania AI. Regulacja, która *a priori* traktuje mechanizmy sztucznej inteligencji (w tym wykorzystujące biometrię) za zakazane albo budzące wątpliwości może doprowadzić do zniechęcenia podmiotów prywatnych jak i publicznych do rozwoju tej technologii. Tego odbioru nie zmienia treść motywu (41), w którym podkreśla się, że *„z faktu, że dany system sztucznej inteligencji został sklasyfikowany jako system wysokiego ryzyka zgodnie z niniejszym rozporządzeniem, nie należy interpretować jako wskazującego na to, że korzystanie z tego systemu jest siłą rzeczy zgodne z prawem na gruncie innych aktów prawa Unii lub prawa krajowego zgodnego z prawem Unii, na przykład w zakresie ochrony danych osobowych, stosowania poligrafów i podobnych narzędzi lub innych systemów służących wykrywaniu stanu emocjonalnego osób fizycznych. Każde takie wykorzystanie należy kontynuować wyłącznie w sposób zgodny z mającymi zastosowanie wymogami wynikającymi z Karty oraz z mającymi zastosowanie aktami prawa wtórnego Unii i prawa krajowego.”*

Układ treści oraz podział logiczny aktu o sztucznej inteligencji nie wspiera rozwoju technik uczenia maszynowego i powinien zostać zmieniony.

Projektowane rozporządzenie powinno stanowić ramy stosowania sztucznej inteligencji, jednak nie wychodzące od zakazów stosowania danego rodzaju systemów lub wskazywania na ryzyko jego stosowania a od określenia zakresu dopuszczalności stosowania sztucznej inteligencji oraz produktów ją wykorzystujących. Zmiana podejścia z „negatywnego” na „pozytywne” jest wskazane, z uwagi na ogólny wydźwięk aktu prawnego oraz sposób jego interpretacji. Należy bowiem wskazać, że podstawą metodą wykładni aktów prawa unii europejskiej jest wykładnia celowościowa. Jest to szczególnie istotne w przypadku zestawienia przepisów aktu o sztucznej inteligencji z celami i przepisami np. ogólnego rozporządzenia o ochronie danych osobowych.

Unia Metropolii Polskich popiera propozycję opinii Komisji Polityki Społecznej, Edukacji, Zatrudnienia, Badań Naukowych i Kultury (SEDEC) Europejskiego Komitetu Regionów sprawie Europejskiego podejścia do sztucznej inteligencji Akt o sztucznej inteligencji ³ w której podkreślono, że przy formułowaniu przepisów prawa w zakresie wykorzystania sztucznej inteligencji zasadne jest przyjęcia podejścia opartego na uczeniu się zamiast wprowadzania przepisów o charakterze sektorowy i podziału określonych technik AI i sposobów jej wykorzystywania jako „zakazanych” lub „sztucznego ryzyka”.

³ <https://cor.europa.eu/PL/our-work/Pages/OpinionTimeline.aspx?oplId=CDR-2682-2021>, nr SEDEC-VII/022 CDR 2682/2021

W ocenie Unii Metropolii Polskich stosowanie sztucznej inteligencji nie może prowadzić do dyskryminacji, wywierania ukrytego wpływu na osoby fizyczne oraz automatycznego (bez braku środka odwoławczego) lub też identyfikacji bez wyraźniej podstawy prawnej lub uzasadnienia. Wskazane wartości mają charakter uniwersalny i ich przestrzeganie nie jest niezależne od miejsca, zakresu oraz obszaru stosowania sztucznej inteligencji.

Ponadto, jak słusznie wskazano ww. projekcie opinii Komisji SEDEC⁴ najważniejszym kryterium określającym AI obciążoną wysokim poziomem ryzyka jest stopień, w jakim człowiek może wpływać na proces decyzyjny, oraz wpływ podejmowania decyzji na prawa i rzeczywiste działanie obywateli i obywateli.

W przypadku pozostawienia podziału systemów - m.in. na systemy wysokiego ryzyka - treść obecnego art. 7 ust. 2 lit a-h powinna zostać przeniesiona do art. 6 jako regulacja rozpoczynająca przepisy merytoryczne rozpoczynające rozdział o systemach wysokiego ryzyka a przesłanki wskazane ww. przepisie powinny stanowić punkt wyjścia dla dalszych regulacji.

2. Przyzwolenie dla podmiotów publicznych dla stosowania AI

W przypadku podmiotów publicznych postulujemy wprowadzenie przepisu wskazującego wprost na możliwość stosowania przez te podmioty sztucznej inteligencji w ramach wykonywania ich zadań publicznych, jeżeli jest to uzasadnione realizacją interesu publicznego lub wynika wprost z przepisów prawa.

W ocenie Unii Metropolii Polskich treść motywu zgodnie, z którym *„Niniejszego rozporządzenia nie należy rozumieć jako ustanawiającego podstawę prawną przetwarzania danych osobowych, w tym w stosownych przypadkach szczególnych kategorii danych osobowych.⁵”* nie jest prawdziwe w szczególności w zakresie działalności sektora publicznego. Ogólne rozporządzenie o ochronie danych osobowych ingeruje w proces przetwarzania danych, wprowadzając ograniczenia dla procesów profilowania i automatycznego wydawania rozstrzygnięć. W przepisach tych wprost odwołuje się do regulacji prawa krajowego lub prawa UE. W przypadku, w którym powstaje regulacja na poziomie europejskim dotycząca działania systemów AI, konieczne jest wskazanie wzajemnych relacji pomiędzy systemem przepisów UE a przepisami prawa krajowego. W przypadku systemów sztucznej inteligencji wykorzystywanych w sektorze publicznym w zdecydowanej większości systemów będzie dochodziło do przetwarzania danych osobowych. Należy wskazać, że będzie się to wiązało z profilowaniem a także, w niektórych przypadkach z automatycznym podejmowaniem decyzji przy użyciu (albo wsparciu) tego rodzaju systemów. Wbrew intencji projektodawcy, te dwie sfery muszą być ze sobą połączone, aby nie doprowadzić do rozbieżności w interpretacji przepisów projektu rozporządzenia i ogólnego rozporządzenia o ochronie danych osobowych (w szczególności w których organami nadzoru na gruncie aktów mogą zostać odrębne organy). W przeciwnym wypadku powstaną istotne wątpliwości prawne związane z oceną, czy możliwe jest stosowanie systemów w administracji publicznej, skoro z jednej strony istnieją zakazy (ograniczenia) z RODO a z drugiej strony system stanowiłby „system podwyższonego ryzyka”, które także cechują się „domyślnym” - choć nie wskazanym w treści aktu zakazem, który dopiero może zostać „przełamany” na skutek dokonania dodatkowych czynności i wymagań, które akt o sztucznej inteligencji ustanawia.

Propozycja regulacji:

„Art. X.

1. Podmioty sektora publicznego mogą wykorzystywać systemy sztucznej inteligencji, jeżeli służą one zwiększeniu efektywności lub jakości realizowanych przez te podmioty zadań albo usług.
2. Przepisy prawa krajowego uprawniające podmioty sektora publicznego do wykorzystywania systemów sztucznej inteligencji, które stwarzają ryzyko szkody dla zdrowia i bezpieczeństwa lub ryzyko niekorzystnego wpływu na prawa podstawowe powinny podlegać ocenie pod kątem proporcjonalności

⁴ Co zostało także wyrażone w Białej Księdze Sztucznej Inteligencji

⁵ Motyw 41 zdanie ostatnie. W treści normatywnej aktu brak jest odpowiedniej regulacji.

celów, które mają realizować krajowe przepisy prawa i z zachowaniem odpowiednich zabezpieczeń praw i wolności osób podlegających operacjom realizowanym przy wykorzystaniu systemów sztucznej inteligencji.

3. *Przepis ten nie narusza obowiązków wynikających z przepisów o ochronie danych osobowych oraz obowiązków związanych z wykorzystywaniem systemów sztucznej inteligencji wysokiego ryzyka.*" (wskazany ust. 2 ma charakter propozycji warunkowej, w przypadku utrzymania w projekcie rozporządzenia obecnego podziału systemów sztucznej inteligencji"

Uzasadnienie: Wydaje się zasadne wprowadzenie wprost przepisów wskazujących na możliwość wykorzystywania systemów sztucznej inteligencji pod warunkiem jednak, że zwiększy: efektywność lub jakość realizacji zadania publicznego, lub sposób wypełnienia obowiązku prawnego albo świadczenia usług. Regulacja ta nie będzie stanowiła wyraźnej podstawy prawnej z art. 6 ust. 1 lit. a, c lub b - gdyż powinna ona wynikać z przepisu prawa krajowego/ lub wyraźnego przepisu prawa UE - jeżeli one stanowią podstawę działania podmiotu publicznego.

Ważne jest, aby wskazać wyraźną podstawę dla możliwości wykorzystania systemów sztucznej inteligencji dla podmiotów publicznych, które np. w polskim systemie prawnym muszą działać na podstawie i w ramach przepisów prawa.

II. Uwagi szczegółowe

1. Projekt rozporządzenia wprowadza definicję sztucznej inteligencji (dalej „AI”), przez którą rozumie się programowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję. Definicję tą uzupełnia wskazanie technik i podejścia z zakresu sztucznej inteligencji wymienione w załączniku nr III do projektu rozporządzenia. Zostały wśród nich wymienione:

- a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;
- b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne),
- c) bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe; podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.

Wskazana definicja jest bardzo szeroka. Obejmuje swoim zakresem systemy kwalifikowane obecnie jak deep learning, jak oraz systemy ekspertowe i może prowadzić do pejoratywnego odbioru stosowania wskazanych metod. W konsekwencji może dojść do prób obchodzenia (poprzez zmianę nazewnictwa oraz zmianę opisu stosowanych metod) projektu rozporządzenia.

Ponadto, wskazanie w definicji konieczności stosowania „co najmniej jednej” wydaje się wadliwa. Wykaz technik i podejść wskazany w Załączniku nr 1 powinien mieć charakter wspierający (albo jego treść powinna zostać przeniesiona do motywów projektu rozporządzenia).

2. Do stosowania rozporządzenia zobowiązane są: **organy publiczne** agencje lub inne podmioty.

W ocenie Unii Metropolii Polskich projekt rozporządzenia w sprawie wykorzystania sztucznej inteligencji powinien zawierać definicję podmiotu sektora publicznego i podmiotu publicznego zamiast wieloznacznych zwrotów tj. organ publiczny, agencja. W tym celu należy zastosować definicje podmiotu publicznego analogiczną jak w przypadku rozporządzenia eIDAS.⁶

Zgodnie z tym aktem „podmiot sektora publicznego” oznacza organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez jeden lub kilka takich organów lub jeden lub kilka takich podmiotów prawa publicznego, lub jednostkę prywatną, której co najmniej jeden z tych organów, podmiotów lub jedno z takich stowarzyszeń udzieliły upoważnienia do świadczenia usług

⁶ Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).

publicznych, gdy działa ona na podstawie takiego upoważnienia. Natomiast w zakresie podmiotu prawa publicznego rozporządzenie eIDAS odwołuje się do podmiotu zdefiniowanego w art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE (15) (tzw. dyrektywa zamówieniowa).

Wskazane rozwiązanie zapewni spójność regulacji UE dotyczących jednolitego rynku cyfrowego, gdyż tego rodzaju zdefiniowanie podmiotów publicznych ma miejsce w wielu regulujących sprawę cyfrowe (poza ww. rozporządzenia eIDAS) innych aktach tak o charakterze dyrektyw jak i rozporządzeń.

Dodatkowo należy wskazać, że z uwagi na fakt, iż ww. definicję funkcjonują już w obrocie prawnym zmniejszy się niepewność rozumienia przepisów nowego aktu. Wskazać tu można na problem m.in. pojęcia „agencja”, które może oznaczać tak agencje UE jak i podmioty na szczeblu krajowym – które jednakże mają różne cechy i cele działania w poszczególnych krajach, często nie związane z realizacją np. zadań publicznych.

Konsekwencją przyjętej definicji będzie konieczność wyodrębnienia w słowniku przyszłego rozporządzenia nowych kategorii tj. osoby prawne i osoby fizyczne oraz agencje Unii Europejskiej.

3. Zgodnie z motywem 9 projektu rozporządzenia „Do celów niniejszego rozporządzenia pojęcie **przestrzeni publicznej** należy rozumieć jako odnoszące się do każdego miejsca fizycznego, które jest dostępne dla ogółu osób, niezależnie od tego, czy dane miejsce jest własnością prywatną czy publiczną. Pojęcie to nie obejmuje zatem miejsc, które mają charakter prywatny i zazwyczaj nie są ogólnodostępne dla osób trzecich, w tym organów ścigania, chyba że osoby te wyraźnie zaproszono lub upoważniono do wejścia na dany teren; do takich miejsc zalicza się domy, prywatne kluby, biura, magazyny i fabryki. Przestrzenie internetowe również nie są objęte niniejszym rozporządzeniem, ponieważ nie są to przestrzenie fizyczne. Sam fakt, że mogą obowiązywać jednak pewne warunki dostępu do danej przestrzeni, takie jak bilety wstępu lub ograniczenia wiekowe, nie oznacza, że przestrzeń ta nie jest dostępna publicznie w rozumieniu niniejszego rozporządzenia. W związku z tym oprócz przestrzeni publicznych, takich jak ulice, odpowiednie części budynków rządowych i większość infrastruktury transportowej, publicznie dostępne są zazwyczaj również przestrzenie takie jak kina, teatry, sklepy i centra handlowe. To, czy dana przestrzeń jest dostępna publicznie, powinno być jednak ustalane indywidualnie w każdym przypadku, z uwzględnieniem specyfiki danej sytuacji.”

Z drugiej strony sama definicja „**przestrzeni publicznej**” zawarta art. 3 pkt 39 projektu rozporządzenia jest bardzo skrótowa i wskazuje się, że oznacza ona każde fizyczne miejsce dostępne publicznie, niezależnie od tego, czy mają zastosowanie określone warunki dostępu.

Należy wskazać, iż przyjęcie ww. przepisy (i interpretacji zawartej ww. motywie) może nieść ze sobą konsekwencje dla polskiego systemu prawnego. Zwracamy uwagę, że pojęcie to występuje już w polskich przepisach prawa np. w art. 9a ustawy z dnia Art. 9a z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2020 r. poz. 713) „Gmina w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej może stosować środki techniczne umożliwiające rejestrację obrazu (monitoring) w obszarze przestrzeni publicznej, za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy lub jednostek organizacyjnych gminy, a także na terenie wokół takich nieruchomości i obiektów budowlanych, jeżeli jest to konieczne do zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej.”

W ślad za komentatorami ww. przepisu⁷ należy przyjmować, że obszar przestrzeni publicznej, o którym mowa w ww. przepisach samorządowych ustaw ustrojowych, przy okazji regulowania zagadnienia monitoringu, należy rozumieć tak, jak zdefiniowane to zostało w art. 2 pkt 6 ustawy o planowaniu i zagospodarowaniu przestrzennym. Zgodnie z tym przepisem „obszar przestrzeni publicznej” – należy rozumieć jako obszar o szczególnym znaczeniu dla zaspokojenia potrzeb mieszkańców, poprawy jakości ich życia i sprzyjający nawiązywaniu kontaktów społecznych ze względu na jego położenie oraz cechy funkcjonalno-przestrzenne, określony w studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy.

⁷ M. Sakowska-Baryła, Rozdział V. Dopuszczalność stosowania monitoringu przez jednostki samorządu terytorialnego, w: Monitoring zgodny z RODO. Praktyczny poradnik z wzorami dla sektora publicznego i prywatnego red. dr Aneta Sieradzka, Monika Wieczorek, wyd. C.H. Beck, 2020 r.

W przyszłości mogą się pojawić wykładnia wskazująca, że dla potrzeb stosowania AI ww. definicja ma charakter autonomiczny, także względem polskich regulacji np. wskazanej w art. 9a. O ile w świetle prawa unii europejskiej tego rodzaju sytuacja jest dopuszczalna, o tyle wydaje się, że w polskiej praktyce będzie miała ona charakter dysfunkcyjny. Trudno rozdzielić stosowanie np. art. 9a statuującego podstawę prawną do prowadzenia monitoringu dla samorządu, prowadzonego w szczególności „w celu zachowania porządku publicznego i bezpieczeństwa obywateli” od możliwości stosowania monitoringu wykorzystującego technologię AI.

W ocenie Unii Metropolii Polskich zwrot zawarty m.in. w ustawie o samorządzie gminnym zawiera się w definicji wskazanej w projekcie rozporządzenia. Wymaga to jednakże potwierdzenia przez administrację rządową już na etapie prac nad projektem ustawy. Ewentualnie należy dodać przepis, że pojęcie przestrzeni publicznej może podlegać zdefiniowaniu na poziomie przepisów prawa krajowego.

4. Projektowane rozporządzenie zawiera w art. 5 ust. 1 lit. d zakaz stosowania w przestrzeni publicznej „Wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:

- (i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;
- (ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;
- (iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa.”

Odnosnie uznania systemów monitoringu za systemy wysokiego ryzyka, należy wskazać, że wykorzystywanie danych biometrycznych może być wykorzystywane właśnie w celu ochrony danych osobowych i ich podstawowych wolności. System taki wykorzystuje dane biometryczne w celu identyfikacji (wizerunku) osoby w celu subanonimizacji jej twarzy np. dla operatora monitoringu, który może kontrolować sytuację a jednocześnie nie widzi konkretnych osób. Dopiero następnie, w przypadku wystąpienia sytuacji niepożądanego systemu umożliwia identyfikacji twarzy dla późniejszych celów np. ścigania przestępstw. Tego rodzaju system, w świetle motywy 38 i 39 działa w czasie rzeczywistym. Tego rodzaju przykład pokazuje, że *a priori* kwalifikacja systemów monitoringu wykorzystanych biometrię nie jest rozwiązaniem optymalnym.

W przypadku utrzymania tego podziału należy wprowadzić regulację, która pozwoli w sposób szybki przeprowadzić uproszczoną analizę celu wykorzystania systemu, której celem byłoby zwolnienie tego rodzaju systemów z pozostałych obowiązków, które muszą spełnić systemy wysokiego ryzyka.

5. Do systemów wysokiego ryzyka zostały także zaliczone „systemy sztucznej inteligencji przeznaczone do wykorzystania przez organy publiczne lub w imieniu organów publicznych w celu oceny kwalifikowalności osób fizycznych do świadczeń i usług publicznych, jak również w celu przyznawania, ograniczania, unieważniania lub żądania zwrotu takich świadczeń i usług.”

W ocenie Unii Metropolii Polskich ww. systemy nie powinny być *a priori* określane jako systemy wysokiego ryzyka. Należy odróżnić system wykorzystujący mechanizmy AI, którego celem jest wsparcie prac analitycznych dla instytucji, którego wynik może mieć wpływ jedynie pośrednio na inne osoby, gdyż uzyskiwane przy pomocy tego systemu informacje mogą stanowić podstawę dla polityk, strategii lub konkretnych działań administracji od systemu działającego autonomicznie lub półautonomicznie, który w oparciu o określone kryteria przydziela lub odmawia przydzielania świadczenia. W przypadku tego rodzaju systemów powinny istnieć mechanizmy kontroli. Mechanizmy te są wymagane w większości krajów członkowskich Unii Europejskiej i są wypracowane w ich dorobku porządku prawnego.

W przypadku polskiego systemu prawnego na gruncie konstytucji i ugruntowanego orzecznictwa Trybunału Konstytucyjnego wymagany jest obowiązek kontroli (zasadniczo) w administracyjnym toku instancji, a następnie sądowno-administracyjnej.⁸ Podkreśla się przy tym, że kontrola ta musi być realna i efektywna.

⁸ Należy wskazać, w wyroku pełnego składu z 13 marca 2013 r., sygn. K 25/10 (OTK ZU nr 3/A/2013, poz. 27, cz. III, pkt 3.4.10 uzasadnienia), w którym Trybunał, podsumowując swoje dotychczasowe orzecznictwo, stwierdził, że: "Zakres stosowania pojęcia

Niesie to ze sobą konieczność zapewnienia aby system sztucznej inteligencji albo pozwalał na ingerencje (korygowanie wyników działania sztucznej inteligencji) albo zapewniał wyjaśnianie działań dla takiego systemu. W tym kontekście, w ocenie Unii Metropolii Polskich podstawowym celem regulacji prawa UE powinno być wprowadzenie wymogu dla systemów aby możliwe byłoby spełnienie tych wymagań - i w tym zakresie postanowienia projektu rozporządzenia należy uznać za zasadne. Nie wydaje się jednak konieczne na tym etapie wprowadzanie dodatkowych wymagań *a priori* wskazanych w rozdziale 2 projektowanego rozporządzenia.

6. W powiązaniu z ww. uwagami należy wskazać, że dla systemów zakwalifikowanych w projekcie rozporządzenia jak systemy wysokiego ryzyka w sektorze publicznym, trudne do spełnienia są wymagania określone w art. 10 projektu rozporządzenia (odpowiednia jakość danych oraz zarządzanie danymi, treningowymi, walidacyjnymi i testowymi).

W przypadku systemów, których wdrożenie w sektorze publicznym mieści się w zakresie Załącznika nr 3 projektu rozporządzenia, gdy jednocześnie ich realny wpływ i udział w realizacji zadania publicznego jest niski, wymogi art. 10 mogą doprowadzić do całkowitego braku wdrożeń ww. zakresie. Koszty tego rodzaju systemu mogą okazać się zbyt duże w stosunku do korzyści. Nowe systemy sztucznej inteligencji nie są systemami opartymi o pojedyncze bazy danych oraz rejestry. W większości przypadków wykorzystywać będą one dane pochodzące z różnych źródeł. Należy zauważyć, że problemy z interoperacyjnością systemów teleinformatycznych, zapewnieniem wspólnych katalogów danych itp. dotyczą sfery wewnętrznej państw członkowskich, jak i wymiany transgranicznej. Doświadczenia pokazują, iż podejście „iteracyjne” prowadzi do najlepszych efektów, pozwala na trwałe doskonalenie systemów i rozwiązań teleinformatycznych oraz systematyczne poprawienie usług. Wymagania stawiane w AI act nie mogą abstrahować od poziomu cyfryzacji sektora administracji publicznej (w całej Europie jak i w Polsce).

Z punktu widzenia celów jakim jest poprawa efektywności i jakości usług publicznych, zasadne jest dopuszczenie do wdrożeń systemów sztucznej inteligencji w realnym działaniu jednocześnie wraz z dojrzałością (i w oparciu o uzyskane doświadczenia) stopniowego zwiększania jej udziału procesie realizacji usługi (realizacji zadania publicznego). Tego rodzaju podejście musi dotyczyć także oceny stopnia jakości danych, które mają stanowić podstawę dla trenowania (jak i działania) systemu sztucznej inteligencji.

Unia Metropolii Polskich uważa, że wymagania stawiane w art. 10 uniemożliwią wdrażanie sztucznej inteligencji w sektorze publicznym w podejściu iteracyjnym.

7. Zgodnie z art. 16 lit. d) projektu rozporządzenia *„dostawcy systemów sztucznej inteligencji przechowują rejestry zdarzeń generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka, jeżeli znajdują się one pod ich kontrolą.”*

Odpowiednio art. 29 ust. 5 rozporządzenia wskazuje, że *„Użytkownicy systemów sztucznej inteligencji wysokiego ryzyka przechowują rejestry zdarzeń generowane automatycznie przez dany system sztucznej inteligencji wysokiego ryzyka w zakresie, w jakim tego rodzaju rejestry zdarzeń znajdują się pod ich kontrolą. Rejestry zdarzeń przechowuje się przez okres odpowiedni w świetle przeznaczenia systemu sztucznej*

«środek zaskarżenia» użytego w art. 78 Konstytucji obejmuje nie tylko postępowanie o charakterze administracyjnym, w którym rozstrzygnięcie o prawach strony następuje w postępowaniu odzwierciedlającym relacje administracyjnoprawne między podmiotem wydającym decyzje («decydującym») a stroną (zob. wyrok z 13 czerwca 2006 r., sygn. SK 54/04, OTK ZU nr 6/A/2006, poz. 64), ale również inne postępowania prowadzone przez organy władzy publicznej w celu rozpatrzenia indywidualnych spraw jednostki i innych podmiotów prawa prywatnego (zob. wyrok TK z 14 marca 2006 r., sygn. SK 4/05, OTK ZU nr 3/A/2006, poz. 29). Może być to także ponowne rozpatrzenie sprawy przez ten sam organ, który wydał decyzję (zob. wyrok TK z 15 grudnia 2008 r., sygn. P 57/07, OTK ZU nr 10/A/2008, poz. 178). Zawsze są to jednak środki w ramach administracyjnego toku instancji. Wykładnia konstytucyjnego pojęcia «zaskarżenie» ma więc merytoryczne granice. Trybunał w swoim orzecznictwie wskazywał, że należy zdecydowanie odrzucić taką interpretację treści prawa, o którym mowa w art. 78 Konstytucji, która prowadziłaby do uznania, iż «materialnie równoważnym» korelatem środka odwoławczego od decyzji administracyjnej jest skarga do sądu administracyjnego. Chodzi o odmienną zakresu i kryteriów kontroli realizowanej w ramach postępowania odwoławczego sensu largo oraz przez sąd administracyjny, jak i o odmienną podejmowanych przez te organy rozstrzygnięć (por. wyrok TK z 11 maja 2004 r., sygn. K 4/03). Pogląd ten podtrzymał Trybunał Konstytucyjny także w wyroku z dnia 6 czerwca 2018 r. sygn. akt K 53/16.

⁹ Wprowadzanie rozwiązań od poziomu pilotażowego, przez wdrożenie w podstawowym zakresie i następnie jego rozwijanie w oparciu o uzyskane doświadczenia.

inteligencji wysokiego ryzyka i mających zastosowanie zobowiązań prawnych przewidzianych w prawie Unii lub prawie krajowym.”.

Projektowana regulacja nie odpowiada na pytanie, czy w przypadku zawarcia stosunku zobowiązanego (lub określenia ww. obowiązku prowadzenia rejestru zdarzeń na podstawie przepisu prawa krajowego) brak realizacji tego obowiązku przez podmiot, który „przejął” na siebie obowiązek prowadzenia takiego rejestru zwalnia użytkownika z odpowiedzialności za ten brak.

W przypadku samorządu terytorialnego jest to szczególnie istotne, z uwagi na fakt, że będą korzystały z systemów zakupionych od dostawców lub użytkować systemy centralne. W takim przypadku inne niż użytkownik podmioty będą przejmowały na siebie prowadzenie tych rejestrów (w trybie umowy lub np. przepisu prawa krajowego).

W ocenie Unii Metropolii Polskich wskazane jest uzupełnienie projektu rozporządzenia o rozstrzygnięcie ww. zagadnienia na poziomie prawa UE.

8. Zgodnie art. 17 ust. 1 *„Dostawcy systemów sztucznej inteligencji wysokiego ryzyka wprowadzają system zarządzania jakością, który zapewnia zgodność z niniejszym rozporządzeniem. System ten dokumentuje się w systematyczny i uporządkowany sposób w formie pisemnych polityk, procedur i instrukcji”.*

Należy potwierdzić na etapie prac nad rozporządzeniem, że we wskazanym przepisie został ustanowiony wymóg posiadania udokumentowania polityk i procedur i instrukcji za pomocą znaków pisarskich (w postaci papierowej lub elektronicznej) a nie jako wymóg ich posiadania formy pisemnej w postaci papierowej i opatrzenia własnoręcznym podpisem.

9. Art. 28 ust. 1 projektu rozporządzenia wskazuje, że *„dystrybutora, importera, **użytkownika** lub inną osobę trzecią uznaje się za dostawcę do celów niniejszego rozporządzenia i nakłada się na nich obowiązki równoważne obowiązkowi dostawcy określonym w art. 16 w dowolnym z poniższych przypadków:*

- a) jeżeli wprowadzają do obrotu lub oddają do użytku system sztucznej inteligencji wysokiego ryzyka opatrzony ich nazwą handlową lub znakiem towarowym;*
- b) jeżeli zmieniają przeznaczenie systemu sztucznej inteligencji wysokiego ryzyka, który został już wprowadzony do obrotu lub oddany do użytku;*
- c) jeżeli wprowadzają istotne zmiany w systemie sztucznej inteligencji wysokiego ryzyka.*

W przypadku zaistnienia okoliczności, o których mowa w ust. 1 lit. b) lub c), dostawcy, który pierwotnie wprowadził system sztucznej inteligencji wysokiego ryzyka do obrotu lub który oddał ten system do użytku, nie uznaje się już za dostawcę do celów niniejszego rozporządzenia.

W naszej ocenie powstaje wątpliwość, czy pod wskazanym w ust. 1 lit. b) zwrotem „przeznaczenie systemu sztucznej inteligencji” należy rozumieć np. rozszerzenie systemu sztucznej inteligencji o nowe funkcjonalności czy też o pozostawienie dotychczasowych funkcjonalności z jednoczesnym dokonaniem zmiany procedur/zakresu spraw, w których są one wykorzystywane.

Przepis wymaga doprecyzowania, iż chodzi wyłącznie o zmianę istotnie zmieniającą dotychczasowy sposób wykorzystania systemu.

W przypadku regulacji wskazanej w ust. 1 lit. c) powstaje wątpliwość czy użyty zwrot „istotne zmiany w systemie” dotyczą zmian o charakterze technologicznym lub metodologicznym, czy też zmian w zakresie danych wejściowych wprowadzanych do tego rodzaju systemu? Wprowadzona w treści rozporządzenia definicja „istotnej zmiany”, zgodnie z którą oznacza ona *„zmianę w systemie sztucznej inteligencji po jego wprowadzeniu do obrotu lub oddaniu do użytku, która wpływa na zgodność systemu sztucznej inteligencji z wymogami określonymi w tytule III rozdział 2 niniejszego rozporządzenia lub powoduje zmianę przeznaczenia, w odniesieniu do którego oceniono system sztucznej inteligencji;”* z jednej strony „nakłada się” na regulacje ust. 1 lit. b) poprzez odniesienie dotyczące dostępności, z drugiej strony nie odpowiada na pytanie zadane powyżej.

Naszym zdaniem przepis ten – z uwagi na specyfikę działania systemów sztucznej inteligencji – powinien ograniczać się wyłącznie do zmian technologicznych i metodologicznych, ponieważ

w pozostałym zakresie (np. zmiany wprowadzanych danych) tego rodzaju zmiana wchodzi w zakres ust. 1 lit. b) tj. zmiany przeznaczenia systemu.

10. Projekt rozporządzenia posługuje się podstawowymi pojęciami **Dostawca** lub **Użytkownik**. W każdej z tych ról może wystąpić podmiot publiczny. Projekt rozporządzenia nakłada na te podmioty określone obowiązki, które można podzielić na:

- obowiązek dostarczenia przez dostawcę systemu sztucznej inteligencji zapewniającego wymagania określone w rozporządzeniu oraz zakaz „wprowadzania do obrotu” zakazanych rozporządzeniem systemów,
- obowiązek zakazu wykorzystywania określonych w rozporządzeniu systemów sztucznej inteligencji przez użytkowników, obowiązek stosowania się do dokumentacji dostarczonej przez instrukcjach obsługi.

Uważamy, że projekt rozporządzenie pomija złożoność struktur organizacyjnych (biznesowych i administracyjnych), w których może dochodzić do wykorzystywania systemów sztucznej inteligencji. W państwach członkowskich funkcjonują różne modele ustrojowe administracji publicznej. Niniejszy projekt rozporządzenia określając rolę podmiotów, które obowiązane są do stosowania systemów sztucznej inteligencji powinien uwzględnić fakt, iż w przypadku administracji publicznej pomiędzy dostawcą a użytkownikiem mogą istnieć systemy zależności na szczeblu publicznoprawnym. W przypadku systemów sztucznej inteligencji częstym przykładem będzie wykorzystywanie systemów tworzonych na poziomie centralnym, przez podmioty publiczne niższego szczebla (samorządowe, jak i niesamorządowe). W takiej sytuacji określone w niniejszym rozporządzeniu obowiązki np. wskazany w art. 29 projektu rozporządzenia obowiązek wstrzymania wykorzystania systemu, obowiązek kontroli systemu sztucznej inteligencji (mimo, iż może wprowadzać dane wejściowe do systemu) stają się uprawnieniami nieegzekwowalnymi.

Zdaniem UMP zasadne jest uzupełnienie projektu o następującą regulację.

„Art. X.

Jeżeli użytkowanie systemów sztucznej inteligencji podwyższonego ryzyka przez użytkowników będących podmiotami sektora publicznego odbywa się na podstawie przepisów prawa krajowego lub na podstawie innych niż umowa instrumentów prawnych, postanowienia przepisów prawa krajowego lub innych niż umowa instrumentów prawnych mogą określać sposób realizacji obowiązków wynikających z rozporządzenia oraz odpowiedzialność dostawców i użytkowników wynikających z użytkowania systemów sztucznej inteligencji.”

11. Zgodnie z art. 29 ust. 4 projektu rozporządzenia *„Użytkownicy monitorują działanie systemu sztucznej inteligencji wysokiego ryzyka w oparciu o instrukcję obsługi. Jeżeli użytkownicy mają powody przypuszczać, że użytkowanie systemu sztucznej inteligencji zgodnie z instrukcją obsługi może doprowadzić do powstania ryzyka w rozumieniu art. 65 ust. 1 rozporządzenia, informują o tym fakcie dostawcę lub dystrybutora i wstrzymują użytkowanie systemu. Użytkownicy zgłaszają również dostawcy lub dystrybutorowi wszelkie stwierdzone przez siebie poważne incydenty lub wszelkie przypadki nieprawidłowego działania w rozumieniu art. 62 i zaprzestają użytkowania systemu sztucznej inteligencji. Jeżeli użytkownik nie jest w stanie skontaktować się z dostawcą, stosuje się odpowiednio przepisy art. 62.”*

W odniesieniu do użytkowników systemów sztucznej inteligencji będących podmiotami sektora publicznego powstaje pytanie, czy przepis ten ma charakter autonomiczny (i samo egzekwujący się) względem regulacji krajowych, czy też wymaga inkorporowania w przepisy prawa krajowego. W przypadku podmiotów sektora publicznego w większości przypadków wykorzystywanie tego rodzaju systemów będzie opierało się na podstawie prawnej na poziomie przepisów prawa krajowego. Mogą to być regulacje ustrojowe (np. regulujące działanie określonego systemu) w powiązaniu z przepisami proceduralnymi, przewidującymi sposób realizacji zadań przy jego udziale. Powstaje pytanie, czy w przypadku podejrzenia, że użytkowanie systemu „prowadzić do powstania ryzyka dla zdrowia i bezpieczeństwa lub praw podstawowych obywateli” można na podstawie art. 29 ust. 4 zaprzestać jego użytkowania (mimo, że przepis krajowy przewiduje taki obowiązek), czy też reguła z art. 29 ust. 4 powinna zostać przeniesiona do odpowiednich przepisów prawa krajowego.

Wskazana uwaga została zgłoszona na bazie doświadczeń z problemami interpretacyjnymi ogólnego rozporządzenia o ochronie danych osobowych, w szczególności w zakresie art. 18 i 19 i 21 tego aktu i wątpliwościami, czy przepisy te mają (a jeżeli tak, to jaki) wpływ na sposób funkcjonowania krajowych podmiotów publicznych realizujących ustawowe zadania.

12. W ocenie Unii Metropolii Polskich należy wprowadzić do rozporządzenia przepis o konieczności powołania przy organach nadzoru, niezależnego ciała opiniodawczego-doradczego. W skład ciała opiniodawczo-doradczego powinni wchodzić przedstawiciele organizacji pozarządowych, których celem statusowym (statutowym) jest podejmowanie działań na rzecz poprawności działania sztucznej inteligencji, przedstawiciele organizacji pracodawców i przedsiębiorców, przedstawiciele organizacji pracowników, administracji państwowej oraz samorządu terytorialnego, wskazywani przez organy nadzoru tych środowisk. Udział w tym gremium powinien mieć charakter kadencyjny a reprezentacja poszczególnych grup interesariuszy sprawiedliwa.

Działalność organu nadzoru będzie charakteryzowała się istotnym wpływem na obszary działania administracji państwowej (i samorządowej) oraz sektora przedsiębiorstw. Głosy wszystkich interesariuszy powinny być wysłuchane przez organ nadzoru, który - jak słusznie wskazuje projekt rozporządzenia - po ich wysłuchaniu powinien podjąć obiektywną i niezależną decyzję.

W przypadku powołania kilku organów (co przewiduje projekt rozporządzenia) ww. obowiązek powinien być stosowany odpowiednio. Jeżeli możliwe jest powołanie organów nadzoru ze względu na sektor, udział odpowiednich przedstawicieli powinien odzwierciedlać interesariuszy dla danego sektora.

13. W art. 57 projektu rozporządzenia należy wprowadzić obowiązek zasięgnięcia opinii odpowiednich Komitetów UE (Europejskiego Komitetu Ekonomiczno-Społecznego, Europejskiego Komitetu Regionów) oraz Komisji Europejskiej¹⁰ lub Rady w przypadku spraw wchodzących w zakres merytoryczny ww. ciał. Wydaje się, iż zapewnienie odpowiedniego głosu podmiotom reprezentującym istotny segmenty sfery publicznej jest zasadne z uwagi na skutki potencjalnych decyzji.

Szanowny Panie Ministrze,

Unia Metropolii Polskich w swoim stanowisku do projektu rozporządzenia (jak we wstępie) zwraca uwagę na nieściśności i braki w przygotowywanej regulacji w aspekcie administracji samorządowej. Z praktyki wiemy, jak trudna jest realizacja zadań i obowiązków, w szczególności przy wdrażaniu nowych technologii. Dlatego prosimy o uwzględnienie naszych uwag w dalszych pracach legislacyjnych.

Z wyrazami szacunku

DYREKTOR BIURA
UNII METROPOLII POLSKICH



Tomasz Fijołek

Do wiadomości:

Pan Poseł Grzegorz Napieralski - Przewodniczący Podkomisji Stałej do spraw regulacji prawnych algorytmów cyfrowych (CBN01S) Sejmowej Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

¹⁰ W art. 57 przewidziano organizacyjną rolę Komisji względem Rady, jednakże w ocenie Unii Metropolii Polskich rola ta w zakresie stosowania systemów sztucznej inteligencji w zakresie w jakim dotyczy agencji i instytucji nadzorowanych przez KE powinna mieć charakter podmiotowy - i obejmować prawo do wyrażenia oficjalnej opinii w trakcie podejmowania decyzji przez przyszły organ.