LAW MORE

ebook o prawnych aspektach Gen AI

Spis treści

Słowem wstępu - krótko o AI

Istnieje wiele definicji sztucznej inteligencji (Artificial Intelligence, AI). Tradycyjnie definiowano sztuczną inteligencję jako algorytm, który posiada cechy ludzkiej (naturalnej) inteligencji. Dzisiaj wskazuje się najczęściej, że AI to algorytm, który posiada zdolność uczenia się.

Kluczową dziedziną sztucznej inteligencji jest właśnie uczenie maszynowe. W dużym uproszczeniu uczenie maszynowe to technologia, która pozwala na uczenie systemów wykonywania zadań na podstawie dostarczonych danych i otrzymanych wyników, zamiast klasycznego precyzyjnego programowania.

Proces uczenia maszynowego opiera się na następujących etapach:

1. **wprowadzenie źródła danych**
2. **użycie tych danych do uzyskania rezultatu**
3. **porównanie rezultatu z danymi kontrolnymi**
4. **zapamiętanie rezultatów i użycie ich do kolejnej iteracji związanej z przetwarzaniem wprowadzonego zbioru danych.**

Słowem wstępu - krótko o AI

W powyższy sposób, w kolejnych iteracjach, algorytm zostaje ukierunkowany na osiągnięcie wskazanego celu (czyli znalezienia prawidłowego lub najbardziej prawdopodobnego wyniku) związanego z analizą wprowadzonych danych.

Z kolei uczenie głębokie jest formą uczenia maszynowego, w której trenowana jest sztuczna sieć neuronowa składająca się z kilku lub więcej warstw pomiędzy wejściem a wyjściem danych. W większości pod pojęciem uczenia głębokiego rozumie się wykorzystanie do uczenia maszynowego szeregu warstw sieci neuronowych ułożonych „jedna na drugiej".

Wyróżnia się dwie, najbardziej popularne, metody uczenia sieci:

- uczenie nadzorowane, zwane również „uczeniem z nauczycielem", które polega na porównaniu sygnału wyjściowego sieci ze znanymi prawidłowymi odpowiedziami,
- uczenie bez nadzoru, zwane również „uczeniem bez nauczyciela", które polega na tym, że sieć, na podstawie zależności w podawanych danych wejściowych, musi tworzyć własne kategorie w celu właściwego rozpoznawania sygnałów wejściowych.

Na potrzeby niniejszego opracowania, sztuczną inteligencją (AI), nazywamy narzędzia oparte na technologii uczenia maszynowego, w tym głębokiego.

LAW MORE

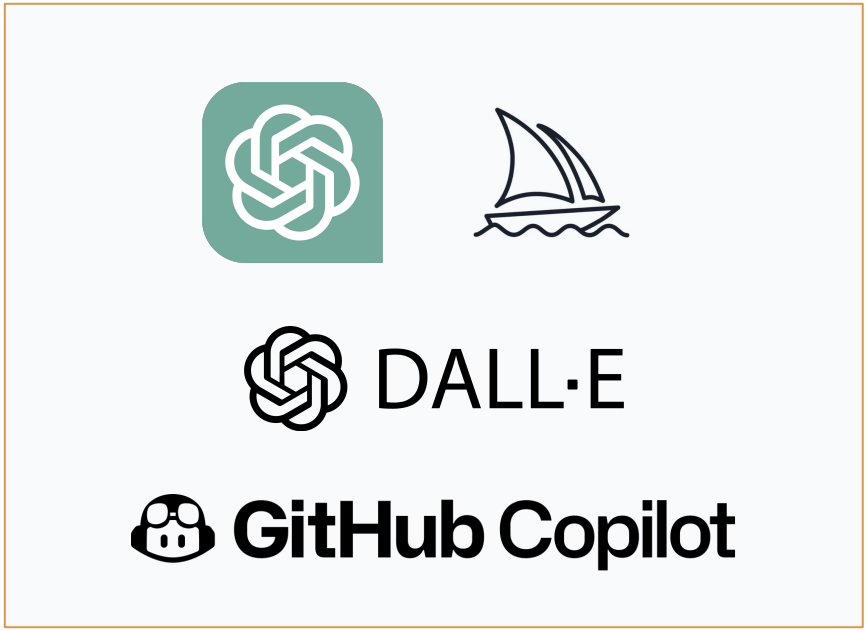
prawa autorskie a obiekty tworzone przy użyciu AI

Prawa autorskie a obiekty tworzone przy użyciu AI

Szybki rozwój narzędzi takich jak ChatGPT, Midjourney, CoPilot czy Dall-e, pozwalających na łatwe generowanie treści tekstowych, programistycznych, wizualnych, muzycznych etc. (dalej jako "output") prowadzi do zasadniczego pytania o to, czy to, co zostanie stworzone przy użyciu narzędzi AI może stanowić utwór chroniony przez prawa autorskie - a jeżeli tak, to komu te prawa przysługują?

Dla uporządkowania powyższej kwestii wskażmy, że w prawie polskim pojęcie „prawa autorskie" obejmuje prawa osobiste i majątkowe (chociaż podział ten jest podobny do systemów z innych krajów). Prawa **osobiste** obejmują prawo autora utworu do m.in. oznaczenia utworu swoim nazwiskiem lub pseudonimem czy nienaruszalności treści i formy utworu oraz jego rzetelnego wykorzystania.

Z kolei prawa **majątkowe**, obejmują prawo autora do wyłącznego korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu. Innymi słowy, autor ma prawo do decydowania o tym: kto, kiedy, na jakich warunkach – również finansowych - i w jaki sposób będzie korzystał z jego utworu lub ten utwór rozpowszechniał.



Prawa autorskie a obiekty tworzone przy użyciu AI

Prawa maszyny? Prawa twórcy algorytmu?

W toczącej się obecnie dyskusji co do możliwości przyznania praw autorskich do wygenerowanych przy użyciu AI prac (tekstów, kodów źródłowych etc.), najczęściej podkreślany jest fakt, że zgodnie z prawem polskim (ale nie tylko, dotyczy to również prawa europejskiego i prawa amerykańskiego) utworem podlegającym ochronie prawnej może być jedynie przejaw działalności twórczej **człowieka.**

Zatem efekty działania sił natury, zwierząt lub **właśnie maszyn, nie stanowią utworu** w rozumieniu ustawy o prawie autorskim. Wobec tego output wygenerowany przy użyciu AI - co do zasady - nie powinien być chroniony prawami autorskimi.

Z kolei twórca algorytmu/programista może mieć prawa autorskie do kodu źródłowego, nie zaś do samych wytworów sztucznej inteligencji (chociaż - przy bardzo określonych i wyjątkowych okolicznościach - może tak się zdarzyć). Przy czym, będzie też tak, że prawa autorskie do algorytmu jako metody czy koncepcji matematycznej, w ogóle nie powstaną, ponieważ jak mówi prawo: ochroną objęty może być wyłącznie sposób wyrażenia; nie są objęte ochroną odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne.

Prawa osoby promptującej?

Czy tak samo jest z prawami użytkowników, tj. osób dostarczających dane wejściowe do narzędzia AI? Tutaj kwestia jest bardziej złożona.

Podmiotem praw autorskich może być tylko człowiek.

Praw autorskich do wygenerowanego “dzieła” na pewno nie będzie więc posiadać sztuczna inteligencja. Co do zasady, nie będzie go również posiadał twórca algorytmu, ponieważ nie decyduje on, w jakim kształcie powstanie ostatecznie output.

Jeżeli zaś nie powstają prawa autorskie do “dzieła” sztucznej inteligencji, to nie ma też utworu chronionego prawami autorskimi. Czyli w ogóle nie możemy mówić o jakichkolwiek prawa autorskich w takim przypadku*.

*Zwróć proszę jednak uwagę, że nie mówimy tutaj o prawie autorskim do algorytmu - to zupełnie inny obszar rozważań.

Prawa autorskie a obiekty tworzone przy użyciu AI

Aby ustalić, czy wygenerowany output może stanowić utwór w rozumieniu polskiej ustawy o prawie autorskim i tym samym podlegać prawom autorskim, należy odpowiedzieć na następujące pytania:

1. **Czy jest on wynikiem twórczej działalności?**

   Przesłanka twórczości – jak wskazuje Sąd Najwyższy – „opiera się na badaniu procesu twórczego w tym sensie, że weryfikuje, czy w jego trakcie twórca zakładał stworzenie nowego obiektu (subiektywizm) oraz czy założenie to spełnił, tworząc w pełni samodzielny, nierutynowy i niespotykany dotąd element rzeczywistości." (wyrok SN z 6.03.2014 r., V CSK 202/13)

2. **Czy ma indywidualny charakter?**

   Chodzi tutaj o zbadanie, czy osiągnięty rezultat jest możliwy do osiągnięcia w takiej samej postaci przez inne osoby, które podejmą się podobnego zadania. Jeżeli tak, to należy dalej zbadać, czy mimo możliwości osiągnięcia podobnego rezultatu przez inną osobę, poszczególne elementy dzieła, ich dobór, prezentacja itp. w dwóch różnych odsłonach będą tożsame, czy jednak przy kształtowaniu treści i formy dzieła twórca korzystał z obszaru swobody, a w dziele występują elementy, których kształt zależał od ich osobistego ujęcia. W tej drugiej sytuacji przesłanka indywidualnego charakteru zostaje spełniona.

3. **Czy został ustalony w jakiejkolwiek postaci, pozwalającej na jego percepcję?**

   To najprostsza do ustalenia przesłanka, sprowadzająca się do wskazania, że utwór istnieje i może być postrzegany. Utwór powinien być ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia. Chwila ustalenia utworu jest istotna, ponieważ to od tego momentu utwór jest chroniony prawami autorskimi - nawet jeżeli w zamiarze twórcy utwór nie został jeszcze ukończony.

Prawa autorskie a obiekty tworzone przy użyciu AI

Powyższe przesłanki prowadzące do ustalenia, czy dany output może stanowić utwór, a tym samym podlegać ochronie na gruncie prawa autorskiego, są trudne do prostego, nie-opisowego zdefiniowania i zamknięcia w sztywne ramy.

Problem pojawia się w odniesieniu do podstawowej przesłanki - dzieło musi być rezultatem **pracy człowieka**, nie zaś maszyny.

W przypadku narzędzi AI można jednak rozważać kwestię, gdy wygenerowany output był tworzony lub współtworzony przez człowieka poprzez bardzo precyzyjne prompty twórcy.

AI jako pomocnik twórcy?

W momencie pisania tego ebooka nie mamy wyroków, które potwierdzałyby powyższą teorią. Mamy jednak mnóstwo spraw sądowych, w których autor nie był technicznym wykonawcą dzieła, a jedynie przekazywał wskazówki osobom trzecim, które wykonując je, tworzyły bezpośrednio dane dzieło.

Weźmy chociażby sprawę, w której asystentka fotografa rościła sobie prawa autorskie (uważała że jest współtwórczynią) do utworów fotograficznych, które zostały co prawda technicznie wykonane przez nią, ale to fotograf decydował o całej wizji artystycznej i sposobie wykonania zdjęć (sygn. akt II CR 575/71). Po długim procesie, w końcu Sąd Najwyższy rozstrzygnął, że asystentka fotografa nie była współautorką fotografii, ponieważ jej udział w wykonywaniu zdjęć polegał na wykonywaniu czynności pomocniczych, jakkolwiek na bardzo wysokim poziomie. Skoro jednak decydujący głos miał fotograf i on decydował o ostatecznym kształcie twórczym wykonywanych fotografii, to nie można uważać asystentki za współtwórczynię.

Sąd Najwyższy argumentował w powyższej sprawie, że współtwórczość w rozumieniu prawa autorskiego nie zachodzi, gdy współpraca określonej osoby nie ma charakteru twórczego, lecz pomocniczy, chociażby umiejętność wykonywania czynności pomocniczych wymagała wysokiego stopnia wiedzy fachowej, zręczności i inicjatywy osobistej.

Swego czasu sąd w sprawie o autorstwo uznał, że nie można uznać za autora dzieła podmiotu, którego udział w jego stworzeniu polegał na wykonywaniu czynności pomocniczych, jakkolwiek na bardzo wysokim poziomie. Dla uznania autorstwa było, kto miał decydujący głos w ostatecznym kształcie twórczym wykonywanych dzieła.

Wiemy zaś, że często AI pełni właśnie takie czynności pomocnicze, ale to człowiek decyduje o efekcie.

Prawa autorskie a obiekty tworzone przy użyciu AI

Inne rozstrzygnięcie miało miejsce w sprawie, w której artysta - plastyk zorganizował sesję zdjęciową swoich prac (sygn. akt III CKN 1096/00). W czasie wykonywania zdjęć artysta wykonywał kadrowanie, decydował o oświetleniu oraz o wszystkich parametrach zdjęć, w tym ich wielkości, rodzaju nasycenia i rodzaju papieru, decydował też o momencie wykonania zdjęcia, dając znak do naciśnięcia migawki. Fotografowie natomiast dostarczali sprzęt fotograficzny, tło, w czasie sesji obsługiwali sprzęt i aparat fotograficzny, zmieniali filmy i na znak artysty wykonywali zdjęcia.

Artysta uczestniczył także w wywoływaniu zdjęć i wykonywaniu odbitek, decydując o ich kadrowaniu, kształcie i wielkości. Sam decydował o wyborze zdjęć do publikacji.

W opisie zdjęć, artysta wskazał fotografów jako jedynie obsługę techniczną, a nie – jak chcieli fotografowie – jako współtwórców. Wobec tego złożyli przeciwko artyście pozew o zaniechanie naruszania ich praw autorskich do zdjęć.

Ostatecznie Sądu Najwyższego orzekł, że osoba, która przy tworzeniu obiektu fotograficznego wykonuje tylko czynności techniczne obsługi sprzętu fotograficznego ściśle według wskazówek twórcy, nie jest współtwórcą w rozumieniu ustawy o prawie autorskim, a więc nie przysługują jej prawa autorskie do zdjęć.

W drodze analogii do dotychczasowego orzecznictwa, jeżeli dostarczane AI prompty są szczegółowe w stopniu decydującym o ostatecznym kształcie dzieła, **a sztuczna inteligencja wykonuje tylko i wyłącznie czynności techniczne**, to można tu uznać twórczość człowieka.

Taka twórczość zaś będzie utworem, o ile dzieło spełni trzy przesłanki z prawa autorskiego: jest przejawem działalności twórczej o indywidualnym charakterze i zostało ustalone w jakiejkolwiek postaci.

⇒Jeżeli zaś możemy mówić o utworze, to możemy też mówić o tym, że dzieło wygenerowane za pomocą AI objęte jest prawami autorskimi.

Nie mamy jeszcze w polskim orzecznictwie przykładów spraw o zaniechanie naruszeń praw autorskich do dzieł wygenerowanych przy użyciu AI. Jednakże, skoro w opisanych wyżej sprawach za jedynych autorów fotografii SN uznał osoby, które nie wykonywały bezpośrednio zdjęć, ale dostarczały szczegółowych poleceń innym osobom, które jedynie technicznie wykonywały fotografie, to - na zasadzie analogii - osoby dostarczające sztucznej inteligencji szczegółowych promptów, mogą zostać uznane za autorów tak wygenerowanego dzieła (jeżeli spełnia ono przesłanki twórczości i indywidualności, o których była mowa powyżej).

Prawa autorskie a obiekty tworzone przy użyciu AI

AI jako pomocnik twórcy - jak to wygląda w USA

Aktualnie wydaje się, że do kwestii tej jednak zupełnie inaczej podchodzi się w USA. Mianowicie, niedawno amerykański Urząd Praw Autorskich (USCO) wydał wytyczne dotyczące rejestracji utworów/praw autorskich w kontekście prac wygenerowanych przez sztuczną inteligencję. Poniżej pozwalamy sobie na kilka cytatów:

- Badanie wniosku o rejestrację takiej pracy, zaczyna się pytaniem, „czy dzieło jest zasadniczo autorstwa człowieka, a komputer (lub inne urządzenie) jest jedynie narzędziem **pomocniczym**, czy też tradycyjne elementy autorstwa dzieła zostały faktycznie wymyślone i wykonane nie przez człowieka, ale przez maszynę".
- Jeżeli tradycyjne elementy autorstwa dzieła zostały stworzone przez maszynę, dzieło nie jest autorstwa człowieka i Urząd go nie zarejestruje.
- Według Urzędu, gdy technologia sztucznej inteligencji otrzymuje **wyłącznie prompt od człowieka** i w odpowiedzi tworzy złożone utwory literackie, wizualne lub muzyczne, wówczas uznaje się, że dzieło określane jest i wykonywane przez technologię, a nie przez użytkownika. Dla Urzędu kluczowe jest, że użytkownicy nie sprawują ostatecznej twórczej kontroli nad tym, jak takie systemy interpretują prompty i generują materiały. Zamiast tego, te podpowiedzi działają **bardziej jak instrukcje dla artysty na zlecenie** - identyfikują, co prompter chciałby przedstawić, ale maszyna określa, w jaki sposób te instrukcje są implementowane w jej wynikach.
- Jednak, w niektórych przypadkach, praca zawierająca materiał wygenerowany przez AI będzie również zawierała taki wkład ludzki, który uzasadnia roszczenie dotyczące praw autorskich. Na przykład człowiek może **wybrać lub zaaranżować materiał** wygenerowany przez sztuczną inteligencję w wystarczająco kreatywny sposób, aby „uzyskane w ten sposób dzieło - jako całość - stanowiło autorskie dzieło". Albo artysta może **zmodyfikować materiał** pierwotnie wygenerowany przez technologię AI w takim stopniu, że modyfikacje spełnią standardy ochrony praw autorskich.

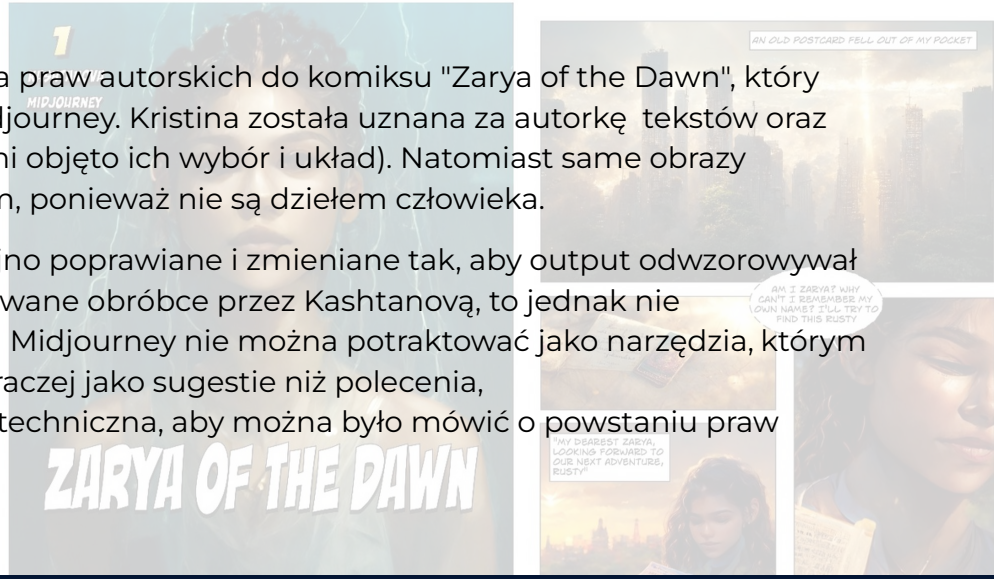
Prawa autorskie a obiekty tworzone przy użyciu AI

- W takich przypadkach prawo autorskie chroni jedynie te aspekty pracy, które są autorstwa człowieka, które są „niezależne” i „nie wpływają” na status praw autorskich samego materiału wygenerowanego przez sztuczną inteligencję.
- Autorzy od dawna używają różnych narzędzi do tworzenia swoich dzieł. Na przykład artysta wizualny, który używa programu Adobe Photoshop do edycji obrazu, pozostaje autorem zmodyfikowanego obrazu, a artysta muzyczny może podczas tworzenia nagrania dźwiękowego używać specjalnych efektów. W każdym przypadku liczy się zakres, w jakim człowiek miał twórczą kontrolę nad ekspresją dzieła i „faktycznie ukształtował” tradycyjne elementy autorstwa.

Z pełną treścią wytycznych Urzędu można zapoznać się tutaj.

W tę narrację wpisuje się też głośna decyzja USCO, dotycząca praw autorskich do komiksu "Zarya of the Dawn", który został stworzony przez Kristinę Kashtanovą przy pomocy Midjourney. Kristina została uznana za autorkę tekstów oraz kompilacji złożonej z obrazków i tekstów (prawami autorskimi objęto ich wybór i układ). Natomiast same obrazy wygenerowane przez AI nie zostały objęte prawem autorskim, ponieważ nie są dziełem człowieka.

Urząd stwierdził, że mimo iż prompty były szczegółowe, kolejno poprawiane i zmieniane tak, aby output odwzorowywał wizję artystki, a wygenerowane obrazy były następnie poddawane obróbce przez Kashtanovą, to jednak nie kontrolowała ona algorytmu, output był nieprzewidywalny, a Midjourney nie można potraktować jako narzędzia, którym Kashtanova kierowała. Według USCO, prompty funkcjonują raczej jako sugestie niż polecenia, a dalsza obróbka obrazów powinna być bardziej twórcza niż techniczna, aby można było mówić o powstaniu praw autorskich.



Prawa autorskie a obiekty tworzone przy użyciu AI

Wspomniana decyzja została poddana krytyce ze strony zarówno specjalistów AI jak i środowiska prawnego. M.in. profesor Edward Lee z Chicago Kent College of Law podnosił na łamach The Washington Post, że decyzja ta opiera się na niezrozumiałym wymaganiu szczegółowego przewidzenia przez twórcę jaki będzie efekt pracy z AI, podczas gdy w innych dziedzinach działalności twórczej nikt nie wymaga od twórców, aby **z wyprzedzeniem** potrafili określić, jaki będzie efekt ich działań. Takie oczekiwania uniemożliwiłyby uznanie za chronione prawami autorskimi dzieła oparte na **improwizacji**, takie jak jazz czy niektóre rodzaje malarstwa.

Aktualnie sytuacja osób promptujących i to, czy posiadają one prawa autorskiego do wygenerowanego przez AI dzieła, jest niejasna.

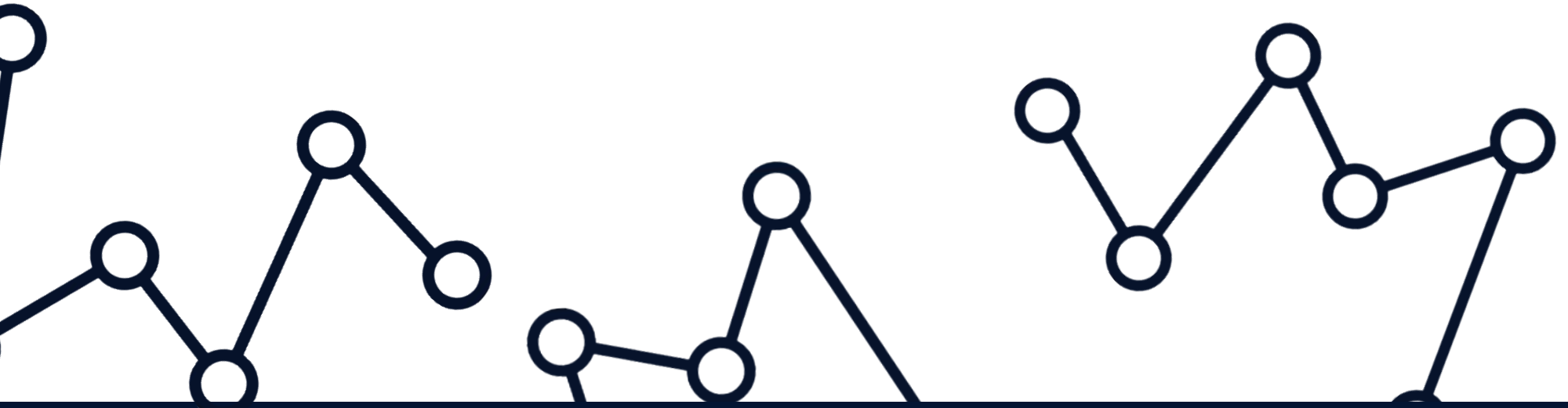
W USA raczej mówi się o braku takich praw autorskich w całości lub w części. Z kolei, patrząc na polskie orzecznictwo - wprawdzie dotyczące innych obszarów niż AI, ale o podobnej tematyce - można uznać, że przy spełnieniu odpowiednich przesłanek, osoba promptująca mogłaby zostać uznana za posiadającą prawa autorskie do danego dzieła.

Prawa autorskie a obiekty tworzone przy użyciu AI

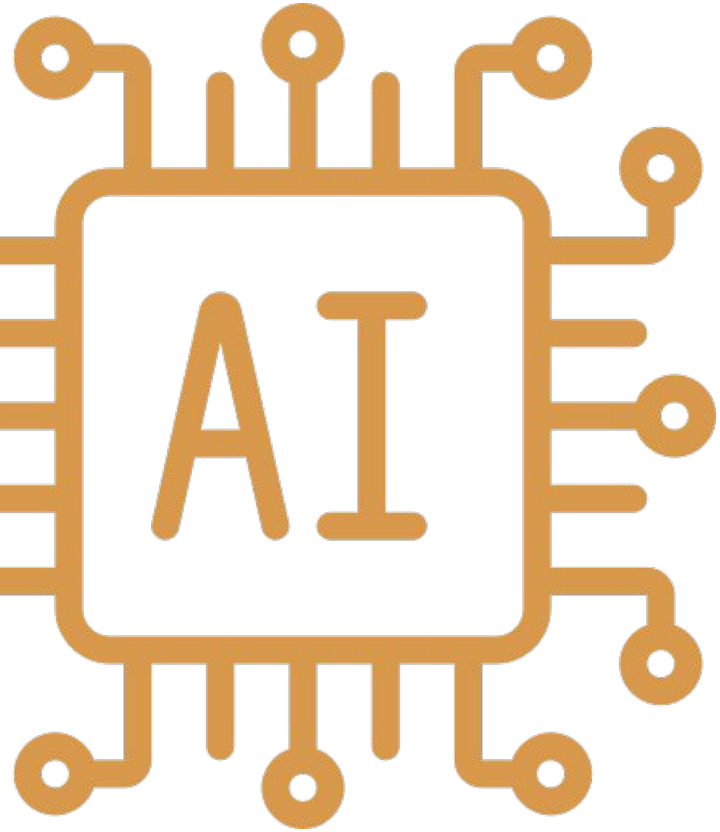
W prawie brytyjskim już od lat funkcjonuje pojęcie tzw. utworów generowanych maszynowo („computer generated works"). Zgodnie z brytyjską ustawą z 1988 r. Copyright, Designs and Patents Act tego typu utwory definiowane są jako utwory wygenerowane komputerowo w okolicznościach, gdzie brak jest człowieka będącego autorem (twórcą) danego utworu („the work is generated by computer in circumstances such that there is no human author of the work").

Utwory te, objęte są ochroną prawną, a prawa autorskie do takiego utworu przysługują osobie, która podjęła działania niezbędne do jego wytworzenia. Wprowadzenie analogicznego rozwiązania do polskiego – czy szerzej – europejskiego porządku prawnego, z pewnością ułatwiłoby ocenę jakie prawa i komu przysługują do prac wygenerowanych przy pomocy narzędzi AI.

Obecnie brak jest jednak planów wprowadzenia do obowiązujących praw na poziomie unijnym lub naszym, krajowym, przepisów dotyczących utworów generowanych maszynowo.



Prawa autorskie a obiekty tworzone przy użyciu AI



Jakie praktyczne znaczenie ma powyższa dyskusja?

Otóż w przypadku uznania, że output uzyskany przy użyciu AI jest utworem w rozumieniu ustawy o prawie autorskim, a użytkownik narzędzia AI (wprowadzający input do takiego narzędzia) jest twórcą w rozumieniu tej ustawy, to będą mu przysługiwały wyłączne prawa autorskie. Oznacza to, że użytkownik będzie mógł decydować o tym czy, kiedy i w jaki sposób udostępni output wygenerowany przez AI, czy i w jaki sposób inne osoby będą mogły korzystać z niego. W tym, będzie mógł zawierać odpłatne licencje na korzystanie z niego, żądać zaniechania naruszeń w przypadku, gdy ktoś wykorzysta utwór bez jego zgody lub niezgodnie z udzieloną licencją.

W przypadku, gdy stwierdzimy, że wytwór wygenerowany przy użyciu AI nie jest utworem w rozumieniu prawa autorskiego, użytkownik co prawda będzie mógł z niego korzystać, jednakże w przypadku jego dalszego udostępnienia inne osoby również będą mogły dowolnie z niego korzystać, a użytkownikowi nie będą przysługiwały w związku z tym roszczenia autorskie.

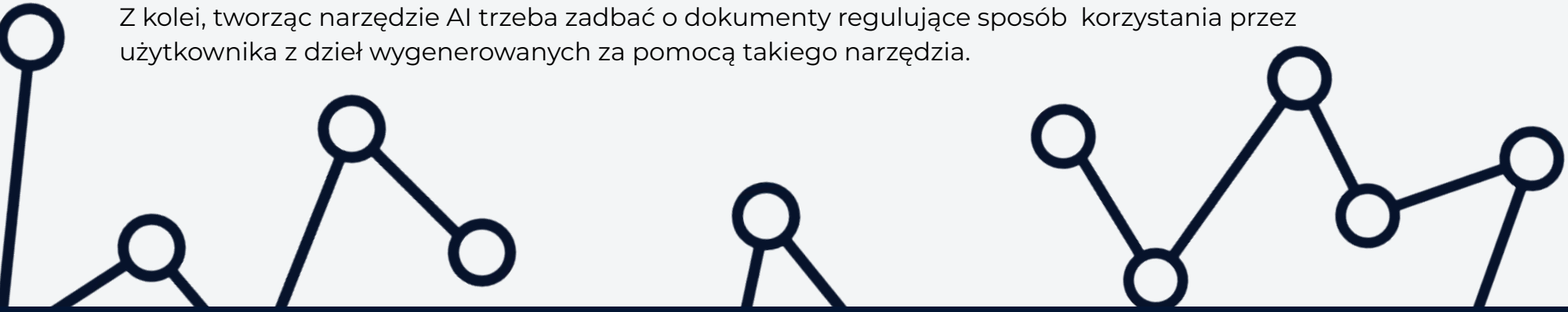
Prawa autorskie a obiekty tworzone przy użyciu AI

Większość firm dostarczających narzędzia AI zabezpieczyło się na okoliczność niejasności co do statusu prawnego wytworów uzyskiwanych przy pomocy tych narzędzi. Przykładowo regulamin Midjourney stanowi, że użytkownik udziela Midjourney bezpłatnej licencji do korzystania zarówno z promptów i danych przesłanych Midjourney do nauki jak i efektów pracy AI. Zatem wydaje się, że Midjourney zakłada istnienie po stronie użytkownika praw autorskich do wytworów AI.

Tymczasem regulamin OpenAI wskazuje, że użytkownikowi przysługuje prawo własności danych treningowych oraz promptów, z kolei prawo własności (ale nie prawo autorskie) do efektów działania AI przysługuje OpenAI. Przy tym firma jednocześnie udziela użytkownikowi praw do reprodukcji i wyświetlania wygenerowanego dzieła, połączone z zapewnieniem, że OpenAI nie będzie wysuwać żadnych roszczeń wobec użytkownika (w tym roszczeń związanych z prawami autorskimi).

Zatem korzystając z narzędzi AI warto zapoznać się z polityką/treścią licencji /regulaminem korzystania z danego narzędzia, aby upewnić się, czy dozwolony sposób korzystania z outputu odpowiada naszym celom.

Z kolei, tworząc narzędzie AI trzeba zadbać o dokumenty regulujące sposób korzystania przez użytkownika z dzieł wygenerowanych za pomocą takiego narzędzia.



Jeżeli uznać, że dzieło wytworzone z pomocą AI podlega pod prawo autorskie, konieczne będzie zaadresowanie wszystkich kwestii związanych z przeniesieniem praw, wynagrodzeniem za przeniesienie lub licencję, oznaczeniem autorstwa etc.

Jeżeli jednak, uznane zostanie, że dzieło wytworzone z pomocą AI nie podlega pod prawo autorskie, nie można mówić o udzieleniu takich praw przez człowieka, stojącego za promptami. Wówczas też, wykonawca nie może w umowie z zamawiającym np. oświadczać, że posiada wszystkie prawa autorskie do dzieła albo, że pobiera wynagrodzenie za przeniesienie praw autorskich do dzieła (tak jak to zazwyczaj pisze się np. w umowach o dzieło).

Prawa autorskie a obiekty tworzone przy użyciu AI

AI a prawa autorskie osób trzecich - inspiracja czy opracowanie?

Skoro przyjmujemy, że niektóre efekty korzystania z narzędzi AI mogą stanowić utwory w rozumieniu prawa autorskiego, to pojawia się też pytanie czy istnieje tutaj ryzyko określonego naruszenia praw autorskich osób trzecich (chociaż na skutek złego treningu, to naruszenie może również nastąpić w każdej okoliczności).

Mianowicie, biorąc pod uwagę, że narzędzia AI są trenowane na właściwie nieograniczonej liczbie danych zasysanych z sieci, a jednocześnie firmy dostarczające tych narzędzi nie zawsze transparentnie komunikują jakich zbiorów danych używano do trenowania danego narzędzia AI, istnieje duże prawdopodobieństwo, że wygenerowana przez nas praca będzie oparta na dziełach chronionych prawem autorskim.

Pytanie - gdzie w takiej sytuacji leży granica między inspiracją (dozwoloną z punktu widzenia praw autorskich niezależnie od zgody autora utworu pierwotnego) a przeróbką lub opracowaniem.

Z kolei rozporządzanie i korzystanie z opracowania zależy od zezwolenia twórcy utworu pierwotnego (chyba że autorskie prawa majątkowe do utworu pierwotnego wygasły).

W przypadku baz danych spełniających cechy utworu, zezwolenie twórcy jest konieczne także na sporządzenie opracowania.

Ponadto, jeżeli dana praca stworzona przy użyciu narzędzi AI będzie imitować styl danego artysty, wychodząc poza ramy inspiracji, a jednocześnie nie stanowiąc opracowania konkretnego utworu tego artysty, to rozpowszechnianie tak stworzonych dzieł może zostać zakwalifikowane jako naruszenie dóbr osobistych autora utworu pierwotnego, mimo że sam styl nie podlega ochronie prawa autorskiego.

Krótko mówiąc, w określonych okolicznościach
może się okazać, że to co wytworzymy
za pomocą AI, jest plagiatem.

Prawa autorskie a obiekty tworzone przy użyciu AI

Wykorzystanie licencji a trenowanie AI

Kolejną kwestią jest możliwość trenowania narzędzi AI na danych udostępnionych w sieci na licencjach otwartych (np. licencjach Creative Commons, Apache, MIT czy GNU), które wskazują w jaki sposób użytkownik może bezpłatnie korzystać z utworu. Niektóre licencje pozwalają na dowolne kopiowanie i modyfikowanie treści, inne zezwalają jedynie na kopiowanie, ale bez modyfikacji, jeszcze inne ograniczają prawo używania treści jedynie do celów niekomercyjnych itd. Łączy je konieczność wskazania autora licencjonowanego utworu.

Do tej pory Creative Commons wypowiedziało się pozytywnie o możliwości używania treści publikowanych na licencjach CC do trenowania narzędzi AI. Nie wskazano jednak jak korzystanie z utworów licencjonowanych wpłynie na wygenerowane w ten sposób efekty AI.

Tymczasem efekty pracy AI na treściach licencjonowanych mogą naruszać wspomniane licencje.

Przykładowo, rozwiązania, które są używane do generowania kodu i wspomagane są przez sztuczną inteligencję (jak np. GitHub Copilot), zwykle szkolone są m.in w ten sposób, że analizują miliardy linijek otwartych kodów źródłowych. Następnie dane te, używane są do generowania kodów w ramach oferowanych rozwiązań (dostarczają sugestie etc.). Nie tak dawno pojawiała się jednak informacja, że GitHub Copilot jest trenowany także na publicznych repozytoriach GitHub, co spowodowało zarzuty w przedmiocie naruszeń praw twórców, którzy opublikowali swoje kody na licencjach open source na GitHub (np. licencje MIT, GPL etc.).

Prawa autorskie a obiekty tworzone przy użyciu AI

Zasadnicze pozostaje więc pytanie - czy deweloper korzystający z takiego narzędzia i kodu, stworzonego w oparciu o wygenerowane np. określone podpowiedzi, może naruszyć licencje, na których udostępniane są kody źródłowe służące do trenowania modelu takiego narzędzia AI?

Zważywszy na fakt, że w tym kontekście pojawił się już chociażby pozew zbiorowy przeciwko GitHub, Microsoft i Open AI, w którym użytkownicy GitHub kwestionują legalność GitHub Copilot i OpenAi Codex, zarzucając właśnie naruszanie takich licencji open source, ciężko jest na ten moment jednoznacznie stwierdzić czy programistę korzystającego z takiego narzędzia obowiązuje również licencja open source kodu, na którym takie narzędzie trenowało. Sprawa jest obecnie w toku, warto jednak odnotować, że sąd wskazał za istotne, czy będzie możliwe udowodnienie, że GitHub Copilot lub Codex można nakłonić do wygenerowania kodu, którego autorstwo można jednoznacznie przypisać danej osobie (w tym wypadku jednemu z powodów w tej sprawie) i taką reprodukcję uwzględnić w pozwie.

Korzystanie z niektórych kodów źródłowych na wolnych licencjach w celu trenowania modeli AI może naruszać warunki licencji tego kodu.

Prawa autorskie a obiekty tworzone przy użyciu AI

AI a prace programistyczne

Jest jeszcze wiele wątków powiązanych z powyższymi kwestiami, ale za kluczowe uznajmy następujące:

- **Miejsce, w którym wykorzystywany kod jest hostowany**

  Jedna z teorii sprowadza się do tego, że stwierdzenie naruszenia może zależeć od tego, gdzie kod wykorzystywany do trenowania modelu jest hostowany. Jeżeli jest on na GitHubie to może nie dochodzić do naruszenia praw autorskich, bo w ich warunkach użytkowania jest mowa o tym, że kod może być używany do ulepszania ich produktów i funkcji, ale w przypadku szkolenia modelu na kodach hostowanych poza GitHubem, należałoby rozważyć kwestię fair use (o czym dalej).

- **Fair use**

  Pojawiają się również poglądy, które usprawiedliwiają trenowanie modeli AI w ramach tzw. fair use. Przy czym, należy też pamiętać, że jest to instytucja i stanowisko, które funkcjonuje w USA. Fair use to instytucja zbliżona do naszego “dozwolonego użytku” (ale nie tożsama). W kontekście fair use mówi się tutaj o kryteriach takich jak: cel i charakter użytku, z uwzględnieniem okoliczności, czy ma ono charakter komercyjny czy też jest wykorzystywane do celów edukacyjnych nie przynoszących dochodów; charakter utworu; ilość i rozmiar użytego fragmentu w odniesieniu do utworu jako całości; wpływ użytku na potencjalny rynek lub wartość utworu. Chociaż zakres wymienionych kryteriów jest nieostry, mogą one na pewno okazać się praktycznymi wskazówkami podczas korzystania z narzędzi AI.

Prawa autorskie a obiekty tworzone przy użyciu AI

- **Informacje o licencji open source wskazywane przez narzędzia AI**

  W licencjach open source istotne jest zwykle, żeby uznawać autorstwo oprogramowania. Przykładowo, właśnie w GitHub Copilot nie pojawia się uznanie autorstwa (informacje o pochodzeniu kodu, autorze czy licencji). Dlatego nie jest nawet technicznie możliwe przestrzeganie tej licencji przez użytkownika takiego narzędzia, skoro nie zna on warunków licencji utworu pierwotnego.

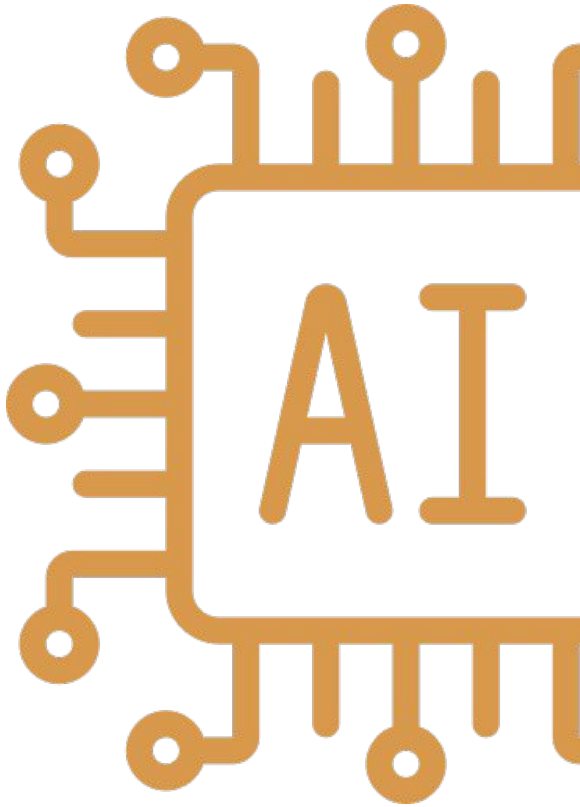
- **Kopiowanie kodu czy tworzenie nowego**

  Ponadto, wskazuje się także, że tego rodzaju narzędzia zwykle działają w ten sposób, że nie kopiują takiego kodu open source dosłownie, a jedynie uczą się na nim, wykorzystując ten kod do stworzenia nowego "autorskiego" kodu, tak przynajmniej wskazuje GitHub Copilot (abstrahując od samej kwestii autorstwa do kodu stworzonego przez AI). Należy przy tym zwrócić uwagę, że takie zjawisko nie jest nowe. Dotychczas programiści też tworzyli własne kody, ucząc się i czerpiąc z innych kodów open source (bez ich kopiowania, ale w celu stworzenia swojego, autorskiego kodu). Natomiast nie sposób pominąć też informacji wskazujących na to, że niektóre sugestie zawierają nawet spore fragmenty skopiowanych kodów, zaś niektóre z licencji open source wprost wskazują chociażby np. na wymóg oznaczania, że są dokonywane modyfikacje w oprogramowaniu open source.

Prawa autorskie a obiekty tworzone przy użyciu AI

- Nowe pole eksploatacji

W Unii Europejskiej funkcjonują także poglądy, zgodnie z którymi maszynową analizę tekstów i danych należałoby zakwalifikować jako nowe, nienazwane pole eksploatacji wytwarzania kopii cyfrowych utworu. Przyjęcie takiego stanowiska powodowałoby konieczność uzyskania zgody autora utworu pierwotnego na korzystanie z jego dzieła na takim polu eksploatacji. Jednak obecnie są to wyłącznie formy postulatów i nie sposób tutaj odnosić się do takiego stanowiska jako argumentu mającego poparcie w naszych przepisach prawa.



- Utwór zależny

To, co tworzymy za pośrednictwem narzędzia AI może zostać też uznane za tzw. utwór zależny. Zwłaszcza możemy mówić o utworze zależnym w przypadku stworzenia kodu w oparciu o sugestie bardziej złożone, dłuższe (większe prawdopodobieństwo, że będzie to chronione prawem autorskim). Nasze (polskie) przepisy odnoszące się do prawa autorskiego pozwalają twórcy utworu pierwotnego na pewną kontrolę nad utworami zależnymi. To znaczy, w przypadku, gdy twórca utworu zależnego chciałby swój utwór zależny dalej rozpowszechniać, np. tworzyć w oparciu o tak powstały kod źródłowy rozwiązanie komercyjne, powinien uzyskać zgodę twórcy utworu pierwotnego.

Prawa autorskie a obiekty tworzone przy użyciu AI

W przypadku tworzenia w oparciu o kody na licencjach open source najbardziej problematyczne byłoby to w odniesieniu do kodów - nazwijmy ich pierwotnymi - udostępnionymi na tzw. wirusowych licencjach, które wymagają w takim przypadku udostępniania na takich samych zasadach co taka licencja. Zgodnie z takimi licencjami wirusowymi to, co tworzymy w oparciu o utwory pierwotne, czyli dzieła pochodne "zarażają się" taką licencją, a więc należy je publikować na takich samych warunkach.

Każdorazowo istotna pozostaje więc sama sugestia. Jeżeli jest ona na tyle niewielka (nieznacząca), że nie sposób jej traktować jako czegoś twórczego, co może być przedmiotem ochrony praw autorskich, to też większe prawdopodobieństwo, że nie dojdzie do naruszenia praw. Powinniśmy już to wszyscy wiedzieć, ale nie należy korzystać z sugestii, które zawierają rozbudowane fragmenty kodu, a już w szczególności, które są wyraźnie wyekstrahowane z innego źródła, zwłaszcza jeżeli nadal mają dołączone do niego komentarze.

Powyższe przykłady pokazują, że należy zachować ostrożność przy korzystaniu z outputu wygenerowanego przy pomocy narzędzi takich jak chociażby GitHub Copilot. Jeżeli praca stworzona w ten sposób naruszy zasady licencji lub prawa autorskie osób trzecich – korzystanie z niej również będzie stanowiło naruszenie.

Prawa autorskie a obiekty tworzone przy użyciu AI

Rekomendacje:

- Korzystając z narzędzi AI należy zapoznać się z polityką/licencją/regulaminem korzystania z danego narzędzia, aby upewnić się czy dozwolony sposób korzystania z outputu odpowiada naszym celom;

- Trzeba pamiętać, że obecnie nie ma żadnych regulacji co do ewentualnych praw autorskich do wytworów sztucznej inteligencji. Dyskusyjne jest czy utwór wygenerowany przy pomocy AI w ogóle może stanowić przedmiot prawa autorskiego oraz czy można kwalifikować go jako opracowanie lub przeróbkę cudzego utworu. Z tego względu należy za każdym razem ostrożnie podchodzić do utworów wygenerowanych przy pomocy narzędzi AI i w miarę możliwości upewnić się, czy output nie przypomina zbytnio dzieł konkretnych autorów;

- Z powyższych względów w praktyce trudne może okazać się egzekwowanie praw do utworów wygenerowanych przy pomocy AI (nawet jeżeli w naszej ocenie output spełnia wszystkie warunki uznania go za dzieło w rozumieniu ustawy o prawach autorskich);

- Dopóki brak jest konkretnych regulacji dotyczących praw autorskich w odniesieniu do sztucznej inteligencji, to budując narzędzie AI należy zadbać również o odpowiednie opracowanie warunków korzystania z takiego narzędzia;

- Należy zweryfikować zatem biznesowo, czy mamy przemyślaną strategię sprzedaży outputów z narzędzia AI (skoro nie sprzedajemy praw autorskich do dzieła) oraz w jaki sposób będziemy bronić takie outputy przed kopiowaniem (skoro nie podlegają prawom autorskim).

LAW MORE

AI a prawa własności przemysłowej

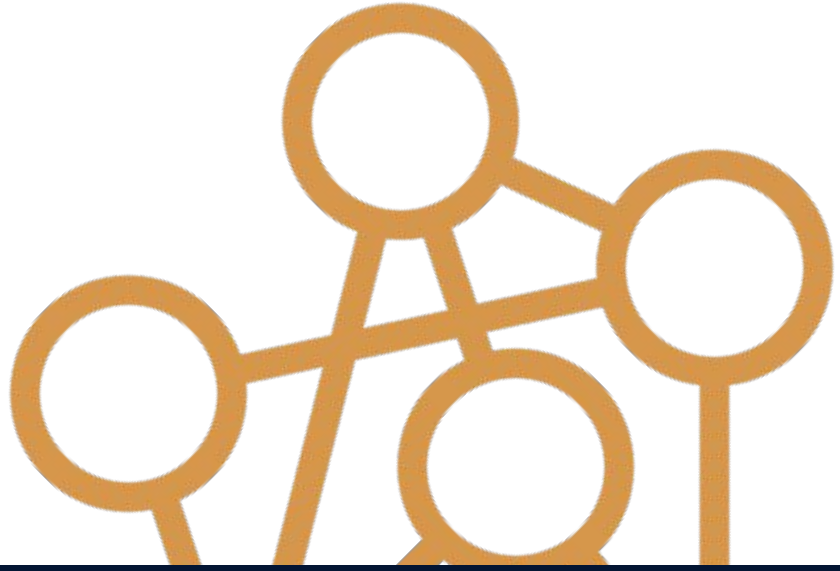
AI a prawa własności przemysłowej

Od jakiegoś już czasu trwa również debata, czy możliwe jest opatentowanie tego, co wytworzy sztuczna inteligencja. Tutaj sytuacja będzie dość podobna do kwestii objęcia wytworu stworzonego z pomocą AI prawami autorskimi, gdyż za wynalazcę uważa się tylko człowieka.

Sprawa ta była przedmiotem analizy chociażby Europejskiego Urzędu Patentowego (EPO), który stwierdził, że podmiotem patentu nie może być urządzenie lub narzędzie. Przy czym Urząd też sam wskazał, że przepisy dotyczące patentowania nie wskazują wprost, że dotyczą tylko wynalazków wytworzonych przez człowieka (tak w: J 0008/20 Designation of inventor / DABUS).

Parafrazując niektóre myśli zawarte w decyzji EPO, to pokusić się można o stwierdzenie - oprócz oczywistości takiej, że opatentowaniu podlegają wynalazki stworzone z pomocą AI - że wynalazki generowane przez sztuczną inteligencję są patentowalne, o ile jako wynalazcę wskaże się człowieka (cytując skład wydający ww. decyzję: “The Board is not aware of any case law which would prevent the user or the owner of a device involved in an inventive activity to designate himself as inventor under European patent law.”)

Na marginesie wspomnijmy, że nie tak dawno amerykański urząd patentowy (USPTO) rozpoczął konsultacje publiczne, w których zapytuje między innymi, czy sztuczna inteligencja powinna być uznawana za współwynalazcę.



Sztuczna inteligencja nie może być wynalazcą i nie może być podmiotem patentu (nie mylić z przedmiotem patentu - bo takim jak najbardziej może być i o tym dalej). Stąd wpisywanie jej do zgłoszenia patentowego to pisanie się o problemy.

Być może warto wskazać siebie jako wynalazcę, a to, czy rozwiązanie zostało stworzone za pomocą sztucznej inteligencji, potraktować jako sprawę drugorzędną.

AI a prawa własności przemysłowej

Patentowanie sztucznej inteligencji

Prawo własności przemysłowej mówi wprost, że za wynalazki nie uważa się w szczególności programów komputerowych i metod matematycznych (jak również m.in. teorii naukowych). Niestety, przepis ten przedostał się do świadomości powszechnej jako całkowity zakaz patentowania tego typu rozwiązań. Podczas gdy - pod pewnymi warunkami - rozwiązania wykorzystujące czy to programy komputerowe, czy to algorytmy, mogą być patentowalne.

Mianowicie w takich przypadkach, jeżeli w ramach zgłaszanego rozwiązania wykażemy jego techniczny charakter lub tzw. dalszy efekt techniczny, będziemy mogli opatentować taki wynalazek. O co jednak chodzi z tymi "technikaliami"?

Jak podaje Urząd Patentowy, „dalszy efekt techniczny" to efekt techniczny wykraczający poza „normalne" oddziaływania fizyczne między programem (software) i komputerem (hardware), na którym jest on uruchamiany.

W orzecznictwie, taki efekt bywa też określany jako „efekt techniczny na fizyczną jednostkę w realnym świecie" lub efektem technicznym wymagającym „bezpośredniego związku z rzeczywistością fizyczną", ale mogą to być również inne efekty, takie jak efekty techniczne w ramach systemu komputerowego lub sieci (osiągnięte np. poprzez konkretne dostosowania systemu komputerowego lub transferu danych).

Z kolei w przypadku programów symulacji komputerowej, można mówić o „efekcie technicznym wykraczającym poza implementację symulacji" lub „efekcie technicznym wykraczającym poza prostą lub nieokreśloną implementację symulacji na standardowym systemie komputerowym" (cytaty pochodzą z decyzji EPO w sprawie G1/19, która dotyczyła wynalazku pt. „Symulacja ruchu autonomicznej jednostki w środowisku", dot. symulacji ruchu pieszych w określonym budynku w celu umożliwienia zaprojektowania lub zweryfikowania bezpiecznej i funkcjonalnej struktury budynku).

AI a prawa własności przemysłowej

Dodatkowo, sztuczna inteligencja i uczenie maszynowe opierają się na modelach obliczeniowych oraz algorytmach do klasyfikacji, grupowania, regresji i redukcji wymiarowości itd. Takie modele obliczeniowe i algorytmy są z natury abstrakcyjnymi modelami matematycznymi i jako takie podlegają wyłączeniu z patentowania. Jednak tak jak wyżej zostało wspomniane, nie jest to ostateczność i aby dać tutaj kilka praktycznych wskazówek, posłużymy się Wytycznymi dotyczącymi postępowania przed Europejskim Urzędem Patentowym (wydanymi oczywiście przez sam Urząd; z całą treścią można zapoznać się tutaj).

Mianowicie jeżeli owe modele będą implikować samodzielne użycie środków technicznych, a tym samym będą miały charakter techniczny, wówczas można się pokusić o patent. Tego przykładem będzie chociażby zastosowanie sieci neuronowej w urządzeniu do monitorowania serca w celu identyfikacji nieregularnych rytmów serca albo klasyfikacja obrazów cyfrowych, wideo, sygnałów audio lub mowy na podstawie cech niskopoziomowych (np. krawędzi lub atrybutów pikseli dla obrazów).

Ale - już przykładowo - klasyfikacja dokumentów tekstowych wyłącznie ze względu na ich treść tekstową nie jest jednak uznawana za samą w sobie cel techniczny, lecz lingwistyczny (tak w: decyzja T 1358/09). Klasyfikacja abstrakcyjnych rekordów danych lub nawet "rekordów danych sieci telekomunikacyjnej" bez żadnego wskazania na techniczne zastosowanie wynikającej klasyfikacji nie jest również samą w sobie celem technicznym, nawet jeśli algorytm klasyfikacji może być uważany za posiadający wartościowe właściwości matematyczne, takie jak odporność (tak w: decyzja T 1784/06).

AI a prawa własności przemysłowej

I uwaga, w przypadku, gdy metoda klasyfikacji służy celom technicznym, kroki generowania zestawu treningowego i trenowania klasyfikatora mogą również przyczyniać się do charakteru technicznego wynalazku, jeśli wspierają osiągnięcie tego celu technicznego (a więc nadają się do patentowania).

Musimy jednak pamiętać, że sam fakt, że metoda matematyczna może służyć celowi technicznemu, nie jest wystarczający. Wymóg funkcjonalnego ograniczenia dotyczy celu technicznego, zarówno w sposób jawny, jak i domyślny. Można to osiągnąć, tworząc wystarczającą relację między celem technicznym a krokami metody matematycznej, np. poprzez określenie, jak dane wejściowe i wyjściowe sekwencji kroków matematycznych odnoszą się do celu technicznego, aby metoda matematyczna miała związany przyczynowo efekt techniczny.

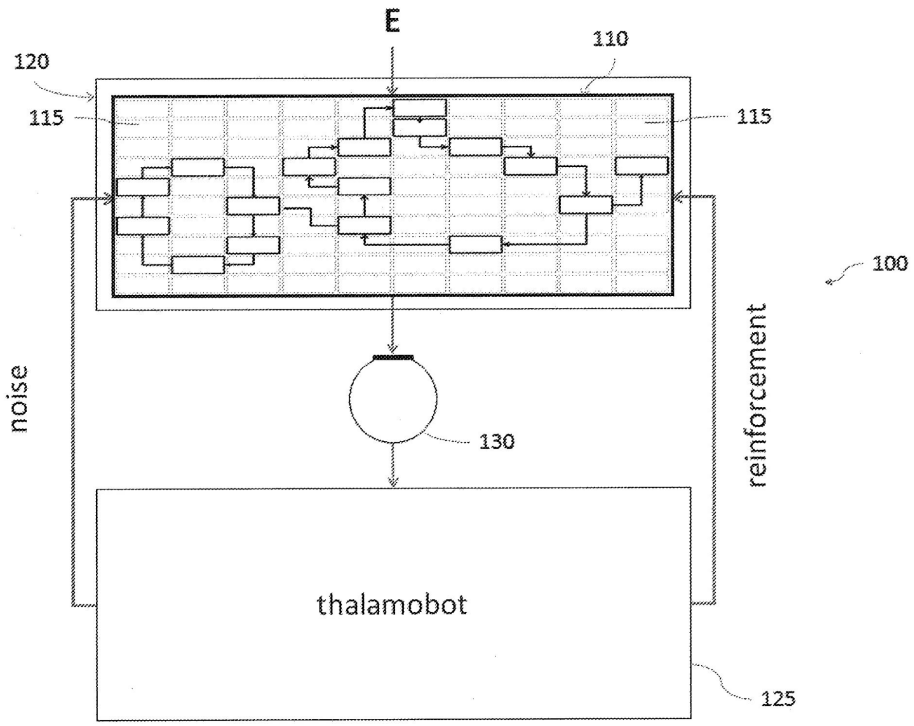
Określanie charakteru danych wejściowych dla metody matematycznej nie implikuje koniecznie, że metoda matematyczna wnosi wkład w charakter techniczny wynalazku, a więc - w zależności o innych przesłanek - prawdopodobnie będziemy podlegać pod wyłączenie możliwości patentowania.

Jeśli kroki metody matematycznej są wykorzystywane do wyznaczania lub przewidywania stanu fizycznego istniejącego rzeczywistego obiektu na podstawie pomiarów właściwości fizycznych, jak w przypadku pomiarów pośrednich, te kroki wniosą wkład techniczny, niezależnie od tego, jakie zastosowanie jest wykorzystane w wynikach - możemy więc w takim przypadku spróbować patentowania.

AI a prawa własności przemysłowej

Może też mieć miejsce przypadek, że metoda matematyczna jest zaprojektowana w celu wykorzystania szczególnych właściwości technicznych systemu, na którym jest wdrażana, w celu uzyskania efektu technicznego, takiego jak efektywne wykorzystanie mocy obliczeniowej lub przepustowości sieciowej komputera - taka sytuacja jest patentowalna.

Na przykład, dostosowanie algorytmu redukcji wielomianowej do wykorzystania przesunięć rozmiaru słowa dopasowanych do rozmiaru słowa sprzętu komputerowego opiera się na takich technicznych względach i może przyczynić się do uzyskania efektu technicznego, jak efektywne sprzętowe wdrożenie tego algorytmu. Innym przykładem jest przypisanie wykonania etapów treningowych algorytmu uczenia maszynowego do jednostki przetwarzania grafiki (GPU), a etapów przygotowawczych do standardowej jednostki centralnej (CPU), aby wykorzystać architekturę równoległą platformy obliczeniowej. Zastrzeżenie wówczas powinno dotyczyć wdrożenia kroków na GPU i CPU, aby metoda matematyczna miała charakter techniczny.



US Patent 10423875B2, Stephen L. Thaler

Nie tylko w Stanach Zjednoczonych można patentować algorytmy i programy komputerowe. W Unii Europejskiej również jest to możliwe. Mianowicie w takich przypadkach, jeżeli w ramach zgłaszanego rozwiązania wykażemy jego techniczny charakter lub tzw. dalszy efekt techniczny, będziemy mogli opatentować taki wynalazek.

Upraszając, chodzi o to, aby w przypadku oprogramowania wykazać „dalszy efekt techniczny", czyli efekt techniczny wykraczający poza „normalne" oddziaływania fizyczne między programem komputerowym (software) i komputerem (hardware), na którym jest on uruchamiany. Z kolei, w przypadku metody matematycznej (jaką może być algorytm), trzeba wykazać, że zastrzeżenie dotyczy nie tylko czysto abstrakcyjnej metody matematycznej, ale wymaga też wykorzystania środków technicznych. Przy czym, podczas oceniania wkładu metody matematycznej w techniczny charakter wynalazku, należy wziąć pod uwagę, czy metoda ta, w kontekście wynalazku, wywołuje efekt techniczny służący celowi technicznemu.

LAW MORE

AI a informacje chronione

AI a informacje chronione

Narzędzia AI bazują na ogromnych ilościach danych, niemożliwych do analizy przez człowieka w tak krótkim czasie, w jakim robi to sztuczna inteligencja. Jednocześnie, oprócz danych ogólnodostępnych, narzędzia AI uczą się również na podstawie inputu – promptów dostarczanych im przez użytkowników danego narzędzia. Aby bezpiecznie korzystać z tych narzędzi, trzeba zastanowić się jakie zagrożenia wiążą się z używaniem danych chronionych prawem, np. stanowiących dane osobowe lub tajemnicę przedsiębiorstwa.

Tajemnica przedsiębiorstwa

Zgodnie z ustawą o zwalczaniu nieuczciwej konkurencji, tajemnicą przedsiębiorstwa są informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji, które są poufne oraz zostały podjęte kroki w celu zachowania ich w poufności.

Ochrona informacji stanowiących tajemnicę przedsiębiorstwa jest obowiązkiem pracowników oraz innych osób mających do nich dostęp.

Dlatego używając narzędzia opartego na AI należy zachować szczególną ostrożność przy dostarczaniu danych wejściowych.

Należy rozważyć czy użycie nawet tylko fragmentu informacji stanowiącej tajemnicę przedsiębiorstwa nie spowoduje ujawnienia tej informacji, a nawet więcej – czy udostępniany AI fragment informacji nie umożliwi algorytmowi odtworzenia części nieujawnionej.

AI a informacje chronione

Oceniając zagrożenia związane z wykorzystaniem ogólnodostępnych narzędzi AI, należy wziąć pod uwagę również regulaminy, licencje i zasady użytkowania wskazane przez samego dostawcę – np. w przypadku ChatGPT jest to firma OpenAI L.L.C.

Regulaminy korzystania z ChatGPT - Service Terms i Terms of Use – stanowią, że OpenAI L.L.C. ma prawo do wykorzystywania treści dostarczanych przez użytkownika w ramach korzystania z ChatGPT na potrzeby wsparcia i ulepszania tworzonych przez OpenAI technologii. Mowa tu nie tylko o promptach, ale również o danych wyjściowych, wygenerowanych przez AI na bazie poleceń użytkownika.

Te informacje są przekazywane do przetwarzania i wykorzystania przez dostawcę, a zakres tego przetwarzania nie jest wprost wskazany. Ponadto z ww. regulaminów wynika, że OpenAI nie zobowiązuje się wobec użytkowników do zachowania poufności wprowadzanych informacji.

Oznacza to, że użytkownik wprowadzając do ChatGPT dane stanowiące tajemnicę przedsiębiorstwa (a także każdą inną informację prawnie chronioną – czy to na podstawie umowy o zachowaniu poufności czy też na podstawie przepisów szczególnych, np. tajemnicę lekarską, adwokacką czy bankową) przekazuje te informacje podmiotowi trzeciemu. Co więcej – akceptując regulaminy użytkowania ChatGPT – wprost wyraża zgodę na bliżej nieokreślone przetwarzanie dostarczonych informacji.

AI a informacje chronione

Nieco inaczej wygląda sytuacja w przypadku, gdy użytkownik przesyła dane za pośrednictwem API. OpenAI wskazuje wówczas, że takie dane nie są wykorzystywane do trenowania modeli OpenAI czy ulepszania ich usług (chyba, że zostanie wyrażona na to zgoda). Nie zmienia to jednak tego, że dane takie będą udostępniane personelowi OpenAI (skoro dostawca je przetwarza). W ChatGPT istnieje także możliwość skorzystania z funkcjonalności pozwalającej na wyłączenie historii konwersacji, co pozwala na wykluczenie jej z trenowania i ulepszania ich modeli (dane te jednak nadal będą przechowywane przez 30 dni).

Skorzystaj z dodatkowej funkcjonalności w ChatGPT, pozwalającej na wyłączenie historii konwersacji. OpenAI wskazuje, że w takim przypadku wybrane rozmowy (w stosunku, do których taka funkcjonalność została uruchomiona) nie będą służyły do trenowania i ulepszania ich modeli.

Należy także mieć na względzie, że wszelkie ograniczenia w powyższym zakresie, tj. nie pozwalające na wykorzystywanie danych do trenowania modeli jednocześnie mogą wpłynąć na rozwiązywanie konkretnych przypadków użycia.

AI a informacje chronione

Teoretycznie, w Regulaminach OpenAI jest wskazane, że dokładają wszelkich starań celem zapewnienia odpowiedniego bezpieczeństwa, usuwają wszelkie informacje umożliwiające identyfikację osób z danych, które zamierzają wykorzystać do ulepszania modelu i że ta próbka tych danych (na każdego klienta) jest niewielka. Trzeba jednak podchodzić do takich zapewnień z dużą dozą ostrożności, ponieważ nadal nie są to gwarancje takich działań, a jedynie informacje wskazujące na podejmowane starania w tym zakresie. W związku z tym, w razie ewentualnych naruszeń tego rodzaju oświadczenia nie stanowią dla nas większego wsparcia.

Dodatkowo, istnieje ryzyko, że dane wprowadzane do niektórych z narzędzi AI są przesyłane i przechowywane na zewnętrznych serwerach, a więc ujawniane i udostępniane są dalej, co również powoduje naruszenie tajemnicy przedsiębiorstwa.

Zatem korzystając z narzędzi AI, zwłaszcza w celach biznesowych np. do analizy danych, trzeba mieć na względzie, że może to doprowadzić do ujawnienia informacji prawnie chronionych, a co za tym idzie - do naruszenia zobowiązań umownych lub przepisów prawa zobowiązujących do zachowania w poufności tajemnicy przedsiębiorstwa. Wobec tego, zwłaszcza w sytuacji upowszechnienia narzędzi opartych na otwartych licencjach, a korzystających z AI, konieczne jest co najmniej odpowiednie przeszkolenie kadry pracowniczej, a optymalnie - wprowadzenie odpowiednich postanowień do umów z pracownikami, współpracownikami (zwłaszcza w kontraktach B2B) oraz podwykonawcami. Postanowienia te z jednej strony powinny regulować dopuszczalność korzystania z narzędzi AI, a z drugiej strony konsekwencje ich użycia przy realizacji umowy.

Również w umowach z klientami warto wpisać odpowiednie zastrzeżenia, jeżeli planujemy korzystać z zewnętrznych dostawców AI.

AI a informacje chronione

Rekomendacje:

- Korzystając z ogólnodostępnych narzędzi AI takich jak ChatGPT czy Midjourney konieczne jest zapoznanie się z regulaminami tych serwisów pod kątem podziału praw co do danych wejściowych i wyjściowych oraz sposobów przechowywania tych danych. To z kolei powinno posłużyć za punkt wyjścia do oceny czy i ewentualnie jakie dane możemy wykorzystywać jako input;

- Dopuszczalność korzystania z ogólnodostępnych narzędzi AI oraz konsekwencje użycia generowanych przez nie wyników w toku realizacji umowy powinny zostać uregulowane w ramach postanowień w umowach z pracownikami, współpracownikami (zwłaszcza w modelu B2B) oraz podwykonawcami. Zalecane jest również wprowadzenie w umowach obowiązku informacyjnego o wykorzystywaniu takich narzędzi w ramach realizacji umowy;

- W organizacjach, w których praca kreatywna stanowi istotny element działalności można również rozważyć wprowadzenie generalnych polityk stosowania narzędzi opartych na AI. W ramach tych polityk możliwe jest kompleksowe uregulowanie kwestii związanych z korzystaniem przez personel czy współpracowników z narzędzi AI. Przyczyni się to do zagwarantowania bezpieczeństwa i poufności danych przetwarzanych w organizacji;

- W przypadku, gdy nie chcemy, żeby nasze dane były wykorzystywane do poprawy wydajności modelu OpenAI można wypełnić formularz udostępniony na stronie OpenAI;

- Warto dodatkowo rozważyć uruchomienie nowej funkcjonalności pozwalającej na wyłączenie historii konwersacji w Chat GPT. Open AI wskazuje, że w takim wypadku wybrane rozmowy, w przypadku, których taka funkcjonalność została uruchomiona nie będą służyły do trenowania i ulepszania ich modeli;

AI a informacje chronione

Rekomendacje:

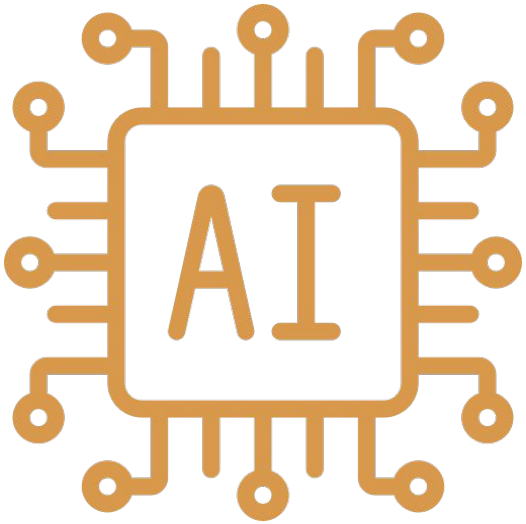
- Korzystanie z usług przez API, jeżeli korzystamy przez API OpenAI wskazuje, że wprowadzany przez nas Input nie jest wykorzystywany do trenowania modelu czy ulepszania usług - w przeciwieństwie do korzystania z ChatGPT lub DALL-E;
- Korzystanie z AI lokalnie, tj. warto wybierać modele, które funkcjonują lokalnie na Twoich serwerach;
- Do rozważanie korzystanie z ChatGPT-4 za pośrednictwem platformy Azure OpenAI, która podobno oferuje odpowiednie środki bezpieczeństwa danych, wskazując, że wszystkie dane pozostają w ramach usługi Azure OpenAI i nie są wysyłane do OpenAI;
- W miarę możliwości używaj platform AI bardziej wyspecyfikowanych tj. przeznaczonych do określonego użytku (np. marketing, sprzedaż etc.), często takie platformy oferują bardziej szczegółowe zasady dotyczącego bezpieczeństwa danych;
- Ostrożnie korzystać z narzędzi AI wprowadzając dane, w szczególności, czy nie zostanie wprowadzona informacja stanowiąca tajemnicę przedsiębiorstwa, czy wprowadzane w ten sposób dane np. o potencjalnym wynalazku nie pozbawią mojego wynalazku przesłanki nowości etc.

LAW MORE

AI a dane osobowe

AI a dane osobowe

W dobie szerokiej ochrony danych osobowych jakiej wymaga Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO), szczególnie uważnie należy podchodzić do przetwarzania danych osobowych w narzędziach AI. Dane osobowe to - zgodnie z rozporządzeniem - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W definicji tej mieszczą się identyfikatory umożliwiające identyfikację osoby fizycznej takie jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.



Pamiętać jednak należy, że jest to katalog otwarty – jeśli zebrane informacje (również w powiązaniu z innymi, którymi dysponujemy) umożliwiają nam dokonanie identyfikacji, **wówczas będą one traktowane jako dane osobowe.**

Z kolei „przetwarzanie" danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie danych osobowych. Zatem definicja przetwarzania danych jest szeroka i należy pamiętać, że obejmuje nie tylko aktywne działania na danych ale również np. przechowywanie czy przeglądanie danych zgromadzonych przez inny podmiot.

Dane osobowe to wszystkie informacje, które mogą prowadzić do identyfikacji osoby fizycznej. Identyfikacja często jest możliwa, gdy pozyskane informacje są ze sobą łączone.

AI a dane osobowe

Podmiot który decyduje o celu i sposobach przetwarzania danych to zgodnie z przepisami RODO – administrator danych osobowych. Natomiast podmiot, który przetwarza dane w imieniu administratora zwany jest „podmiotem przetwarzającym" lub „procesorem". Procesor wykonuje operacje przetwarzania danych na rzecz administratora (na jego zlecenie), czyli sam nie decyduje o celu i sposobach przetwarzania. Kluczowe do rozróżnienia powyższych jest stwierdzenie czy dany podmiot decyduje o samym fakcie przetwarzania danych – jeżeli tak, to mamy do czynienia z administratorem danych. W praktyce podmioty przetwarzające realizują w imieniu administratora pewne operacje – przykładowo przechowują dane osobowe (np. dostawcy rozwiązań chmurowych).

Pamiętaj, że pojęcie przetwarzania dotyczy tak naprawdę każdej czynności dokonywanej na danych osobowych, od momentu ich pozyskania aż do momentu ich usunięcia, zniszczenia lub ostatecznej anonimizacji.

Administrator odpowiada za zgodne z prawem przetwarzanie danych osobowych. Ogólne zasady przetwarzania danych zostały wskazane w art. 5 RODO i są to m.in. zasada rzetelności i przejrzystości, minimalizacji danych, ograniczonego przechowywania, ograniczonego celu, a także rozliczalności. Ponadto administrator **odpowiada za wybór podmiotu przetwarzającego** – przed powierzeniem mu przetwarzania danych osobowych powinien zweryfikować czy dostawca danych usług działa zgodnie z RODO oraz czy stosuje odpowiednie zabezpieczenia w ramach realizowanych procesów przetwarzania.

AI a dane osobowe

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z warunków wskazanych w art. 6 RODO, tj.:

A. osoba, której dane dotyczą wyraziła **zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

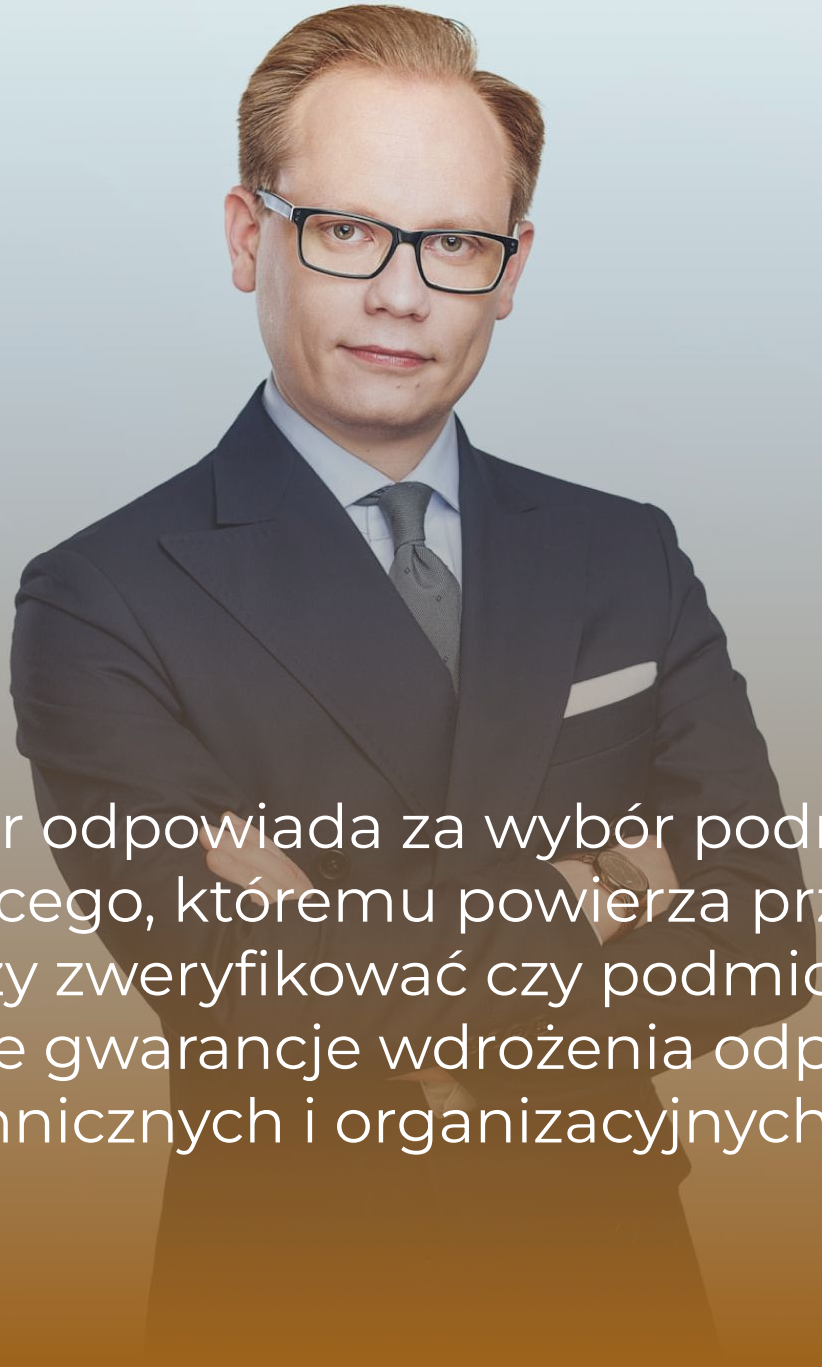
B. przetwarzanie jest niezbędne do **wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

C. przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego** ciążącego na administratorze;

D. przetwarzanie jest niezbędne do ochrony **żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej;

E. przetwarzanie jest niezbędne do wykonania zadania realizowanego **w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

F. przetwarzanie jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów realizowanych przez administratora** lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.



Administrator odpowiada za wybór podmiotu przetwarzającego, któremu powierza przetwarzanie. Zawsze należy zweryfikować czy podmiot taki zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.

AI a dane osobowe

Zgodnie z RODO niektóre dane osobowe podlegają szczególnej ochronie. Są to szczególne kategorie danych (zwane też czasem danymi wrażliwymi), tj. informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Dane osobowe mogą być przetwarzane tylko w przypadku posiadania odpowiedniej przesłanki. Osoba, której dane dotyczą zawsze powinna być poinformowana o tym w jakich celach przetwarzane będą jej dane osobowe.

Zasadą jest, że przetwarzanie szczególnych kategorii danych osobowych jest zabronione, chyba że wystąpią szczególne warunki wskazane w art. 9 RODO (przetwarzanie danych wrażliwych jest możliwe m.in. gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, konieczne jest to do diagnozy medycznej etc.).

AI a dane osobowe

Przepisy RODO nakładają na administratora danych osobowych szereg obowiązków, związanych ze szczególnymi sposobami przetwarzaniem danych. W kontekście narzędzi AI trzeba tu przede wszystkim zwrócić uwagę na następujące kwestie:

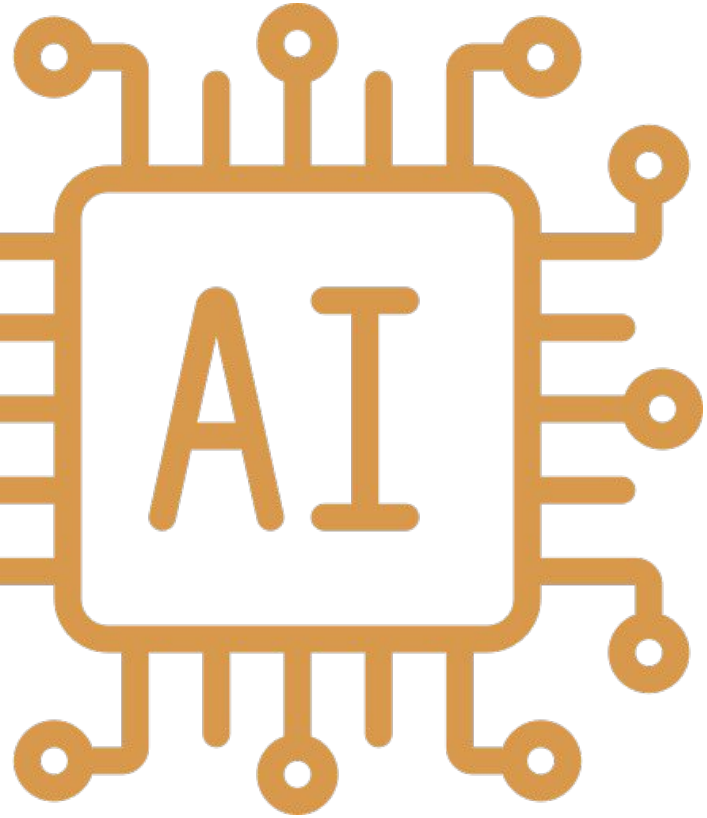
1. Obowiązek przeprowadzenia przez administratora oceny skutków dla ochrony danych (z ang. Data Protection Impact Assessment – DPIA). Chodzi tu o ewaluację ryzyka na etapie planowania, a jeszcze przed rozpoczęciem przetwarzania danych osobowych. Obowiązek przeprowadzenia DPIA będzie występował w szczególności w następujących przypadkach:

- przetwarzanie przy pomocy sztucznej inteligencji danych na dużą skalę, przy czym pojęcie dużej skali dotyczy: liczby osób, których dane są przetwarzane, zakresu przetwarzania, okresu przechowywania danych oraz geograficznego zakresu przetwarzania;
- systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni
- przetwarzanie informacji pozyskiwanych przez Internet rzeczy (opaski medyczne, smartwatche itp.) oraz ich przesyłanie w sieci przy użyciu urządzeń mobilnych typu smartfon czy tablet;
- przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu;
- przetwarzanie danych genetycznych – w każdym przypadku;

AI a dane osobowe

- przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł;
- ocena oraz scoring – profilowanie oraz przewidywanie, w szczególności dotyczące takich danych, jak: zdrowie, zainteresowania, lokalizacja;
- ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych (np. ocena zdolności kredytowej, przy użyciu algorytmów sztucznej inteligencji, objęta obowiązkiem zachowania tajemnicy i żądanie ujawnienia danych niemających bezpośredniego związku z oceną zdolności kredytowej).

W przypadku planowania niektórych procesów przetwarzania danych osobowych wymagane będzie przeprowadzenie DPIA (z ang. Data Protection Impact Assessment, tj. ocena skutków dla ochrony danych). Przy korzystaniu z AI warto zawsze zweryfikować, czy taka ocena nie jest konieczna.



2. Obowiązek powołania inspektora danych osobowych – dotyczy podmiotów, których główna działalność obejmuje przetwarzanie danych wrażliwych na dużą skalę lub regularne i systematyczne monitorowanie osób na dużą skalę. W takim przypadku monitorowanie zachowań osób oznacza między innymi wszelkie formy obserwowania i profilowania w internecie, także dla celów reklamy behawioralnej.

3. Obowiązki związane z przekazywaniem danych poza Europejski Obszar Gospodarczy (EOG). Zgodnie z art. 44 – 47 RODO, przekazywanie danych osobowych europejczyków poza teren EOG jest możliwe w przypadku gdy:

I. Komisja wyda decyzję że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia,

II. W razie braku ww. decyzji, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej gdy zapewnią odpowiednie zabezpieczenia i **pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej**, tj.:

- prawnie wiążące i egzekwowalne instrumenty między organami lub podmiotami publicznymi;
- wiążące reguły korporacyjne;
- standardowe klauzule umowne ochrony danych przyjęte przez Komisję Europejską;
- zatwierdzony kodeks postępowania zgodnie z art. 40 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą;
- zatwierdzony mechanizm certyfikacji zgodnie z art. 42 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą;
- standardowe klauzule umowne ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję Europejską.

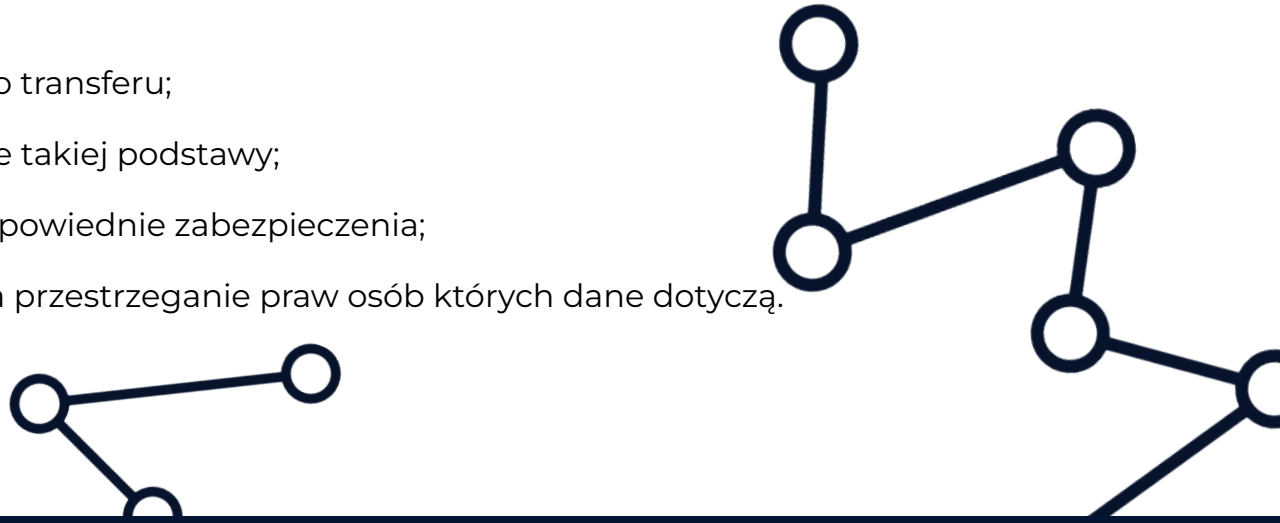
W przypadku braku decyzji Komisji oraz braku odpowiednich zabezpieczeń i środków ochrony prawnej, dane osobowe mogą być przekazywane poza obszar EOG w sytuacjach wyjątkowych, wskazanych w art. 49 RODO.

AI a dane osobowe

W każdym przypadku przekazując dane poza obszar EOG, administrator lub podmiot przetwarzający odpowiadają za przetwarzanie danych osobowych zgodnie z zasadami RODO. Jeżeli używając narzędzia opartego na sztucznej inteligencji wykorzystujemy w trenowaniu lub jako input dane osobowe osób przebywających w Europejskim Obszarze Gospodarczym (a nawet osób spoza tego obszaru, jeśli czynności przetwarzania są realizowane na obszarze EOG), które poprzez narzędzie AI trafią poza obszar EOG (tak jak np. w przypadku Chatu GPT, który gromadzi dane na serwerach znajdujących się w USA) trzeba stwierdzić czy istnieje któraś z powyższych przesłanek pozwalających na transgraniczne przetwarzanie danych. Jeżeli żadna z przesłanek nie zachodzi, to używając takiego narzędzia AI nie można przetwarzać danych osobowych.

Jeśli ma dojść do przekazywania danych osobowych do państwa trzeciego zawsze należy zweryfikować:

- na jakiej podstawie dochodzi do transferu;
- czy możliwym jest zastosowanie takiej podstawy;
- czy odbiorca danych stosuje odpowiednie zabezpieczenia;
- czy państwo odbiorcy zapewnia przestrzeganie praw osób których dane dotyczą.



AI a dane osobowe

Powyższe zasady przekazywania danych osobowych poza obszar EOG są dla organów regulacyjnych i nadzorczych bardzo istotne, co pokazuje chociażby głośna ostatnio sprawa kary grzywny wymierzonej przez Europejską Radę Ochrony Danych firmie Meta posiadającej m.in Facebook i Instagram za przesyłanie danych europejskich użytkowników Facebooka do USA. Kara grzywny została wymierzona w wyniku dochodzenia wszczętego przez irlandzką Komisję Ochrony Danych i wyniosła 1,2 mld euro. Jest tym samym najwyższą karą wymierzoną dotychczas na podstawie RODO.

Przetwarzanie danych osobowych przy użyciu AI.

Przetwarzając dane osobowe z użyciem narzędzi AI należy pamiętać, że przetwarzanie danych wymaga m.in.:

- poinformowania osoby, której dane dotyczą o konkretnych sposobach i celach przetwarzania jej danych osobowych,
- wskazania podstawy prawnej przetwarzania danych (może to być m.in. umowa łącząca osobę której dane są przetwarzane z administratorem lub zgoda tej osoby),
- uzyskania zgody osoby, której dane są przetwarzane – w braku innej podstawy prawnej przetwarzania, przy czym zgoda ta nie może być dorozumiana,
- umożliwienia osobie zainteresowanej wykonywania praw przysługujących jej na mocy RODO, w tym przede wszystkim prawa do żądania dostępu do danych, sprzeciwu co do ich przetwarzania oraz sprostowania danych lub ich usunięcia.

AI a dane osobowe

Wobec powyższego, zapewne większość dotychczas używanych w obrocie polityk prywatności, klauzul informacyjnych czy postanowień umownych dotyczących przetwarzania danych nie obejmuje treści wymaganych w związku z używaniem w tym celu narzędzi AI, tj. **przykładowo zgoda wyrażona przez użytkownika na założenie konta w danym serwisie nie pozwala na używanie danych tej osoby do trenowania narzędzia AI.**

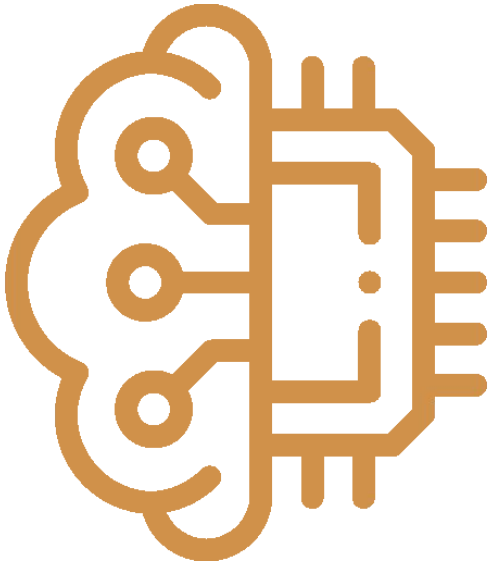
Szczególnie problematyczne w kontekście obecnie dostępnych narzędzi AI jest umożliwienie osobie zainteresowanej wykonywania praw przysługujących jej na mocy RODO – nie ma obecnie mechanizmu umożliwiającego usunięcie danych już przekazanych w ramach inputu do narzędzia AI ani też wglądu w sposób przetwarzania danych i ich sprostowania.

Pamiętać również należy, że dane osobowe nie mogą być przetwarzane „w nieskończoność” – należy je usunąć gdy podstawa prawna do ich przetwarzania przestanie obowiązywać, jak również, gdy utracą one swoją przydatność.

Narzędzia AI - aby być zgodnymi z RODO - powinny zapewniać egzekwowalną możliwość realizacji praw osób, których dane dotyczą.

AI a dane osobowe

Z kolei w odniesieniu do nowopowstających narzędzi AI - zakładając, że powyższe obowiązki administratora zostaną spełnione - należy dodatkowo pamiętać o zasadach ogólnych przetwarzania danych osobowych. Chodzi tu w szczególności o zasady uczciwości i rzetelności przetwarzania danych. Zasady te wymagają, aby dane osobowe nie były przetwarzane w sposób niesprawiedliwy, nieoczekiwany lub w złych intencjach, a także w sposób mogący negatywnie wpłynąć na osoby, których dane były przetwarzane. Należy tu przede wszystkim pamiętać, że dostarczając dane tendencyjne do nauki sztucznej inteligencji algorytm będzie **powielał te tendencje w swoich wynikach**, co może spowodować w konsekwencji, że dane osobowe będą przetwarzane w sposób nieuczciwy.



Dobrym przykładem ilustrującym powyższą zależność jest próba stworzenia algorytmu zatrudniania przez firmę Amazon. Algorytm w założeniu miał – na bazie danych osób już zatrudnionych - tworzyć krótką listę kandydatów na dane stanowisko, tj. miał wybierać spośród przesłanych CV osoby, które zostaną zaproszone na rozmowy kwalifikacyjne. Okazało się, że algorytm „faworyzował" mężczyzn w wynikach, czyli wskazywał wyższą pozycję kandydatów płci męskiej.

Wynikało to z faktu, że algorytm został przetrenowany na danych dotychczasowych pracowników, którymi najczęściej byli mężczyźni. W ten sposób narzędzie, które w założeniu nie miało wykorzystywać danych w sposób nieuczciwy, de facto – w sposób niezamierzony - stało się środkiem dyskryminującym, powielając nierówności z danych szkoleniowych w swoich wynikach. W tym kontekście pamiętać należy, że efektem błędnego działania algorytmu może być naruszenie nie tylko przepisów RODO, lecz również innych aktów prawnych.

AI a dane osobowe

Rekomendacje:

Konieczne jest upewnienie się, w jaki sposób przechowywane są dane treningowe zgodnie z regulaminami użytkowania danego narzędzia AI – jeżeli poza terenem EOG (tak większość ogólnodostępnych narzędzi AI) to do przetwarzania danych za pomocą takiego narzędzia konieczne jest spełnienie którejś z przesłanek wcześniej wymienionych. W razie niespełnienia wskazanych tam warunków nie jest możliwe przetwarzanie danych osobowych z użyciem takiego narzędzia.

Obecnie dostępne narzędzia AI nie zawierają mechanizmu umożliwiającego usunięcie lub zmodyfikowanie danych przetworzonych przez system, zatem właściwie wykluczone jest przetwarzanie danych osobowych za pomocą tych narzędzi w zgodzie z przepisami RODO.

Zakładając że używane narzędzie AI umożliwi usunięcie lub zmodyfikowanie danych przetwarzanych przez algorytm, zbierając dane osobowe do treningu AI należy zadbać o pełne i rzetelne poinformowanie osób będących podmiotami danych o celu i sposobie przetwarzania danych, jak również o podstawie prawnej przetwarzania, a w przypadku takiej konieczności, uzyskać jednoznaczną zgodę na przetwarzanie danych osobowych w danym celu.

Wykorzystując sztuczną inteligencję do analizowania danych osobowych, należy przeprowadzić DPIA i ocenić jej prawdopodobny wpływ na poszczególne osoby, w szczególności - ocenić czy efekty działania AI nie wpłyną negatywnie na osoby, których dane dotyczą i czy nie powodują nieuczciwego lub dyskryminującego przetwarzania danych.

Budując narzędzie oparte na sztucznej inteligencji, należy zwrócić szczególną uwagę na zbiory danych używanych do trenowania sztucznej inteligencji, tak aby ich wykorzystanie nie stanowiło o nieuczciwym przetwarzaniu danych osobowych, prowadząc np. do dyskryminujących wyników (jak miało to miejsce w przykładzie Amazona).

LAW MORE

sztuczna inteligencja a ryzyka po stronie konsumentów

Sztuczna Inteligencja a ryzyka po stronie konsumentów

Dynamiczny rozwój sztucznej inteligencji powoduje, że coraz częściej korzystające z niej systemy są używane w ramach oprogramowania, z którego korzystają konsumenci. Ma to niebagatelne znaczenie w kontekście szerokiej ochrony praw konsumentów zapewnianą przez przepisy obowiązujące na obszarze Unii Europejskiej, w tym również Polski, jak również postulatów dot. rozszerzania tej ochrony ze względu na wciąż powstające, nowe zagrożenia.

Obecnie konsumenci na szeroką skalę korzystają z systemów wykorzystujących AI do generowania tekstów pisanych oraz obrazów. Założyć jednak należy, że w niedalekiej przyszłości AI będzie wykorzystywane przez konsumentów w wielu innych celach. Jednak już obecnie można zidentyfikować szereg ryzyk dla konsumentów związanych z wykorzystywaniem sztucznej inteligencji. Za najważniejsze z nich należy uznać:

- **ryzyko manipulacji** – może ono wystąpić w dwóch alternatywnych przypadkach, tj.: i) AI, której zapewniono niskiej jakości dane wejściowe może wygenerować błędne lub wprowadzające w błąd przekazy kierowane do użytkowników; ii) AI zaprojektowane jest tak, aby wywoływać konkretny efekt u odbiorcy za pomocą generowanych treści;
- **wprowadzanie w błąd** – niezależnie od przyczyn (źle opracowany model, treść danych wejściowych, świadome działanie twórców), AI może generować treści wprowadzające w błąd konsumentów. Jest to szczególnie groźne w przypadku próby pozyskania specjalistycznej wiedzy, np. z zakresu medycyny lub prawa;
- **dezinformacja** – od dłuższego czasu sztuczna inteligencja jest wykorzystywana do tworzenia fałszywych przekazów (głosowych, tekstowych, obrazów), w szczególności do generowania tzw. deepfake'ów. Generowanie, a następnie rozpowszechnianie tego typu materiałów, może służyć do rozpowszechniania nieprawdziwych informacji, a co za tym idzie wpływać na zachowania konsumentów – odbiorców treści, również w bardzo istotnych aspektach, jak np. udział w wyborach lub oddanie głosu na konkretnego kandydata;

Sztuczna Inteligencja a ryzyka po stronie konsumentów

- **naruszenie prywatności** – modele AI wykorzystują dla swojego rozwoju szereg informacji, które mogą obejmować również dane osobowe. Pamiętać należy, że przedmiotowe dane mogą być dowolnie przetwarzane przez dane rozwiązanie, zaś usunięcie z nich danych osobowych na ten moment wydaje się być niemożliwe. Ponadto, hipotetycznie sztuczna inteligencja na podstawie już zebranych danych może generować dodatkowe, nieprawdziwe dane dotyczące danej osoby.

W przypadku wykorzystywania systemów AI pamiętać należy o konieczności stosowania przepisów krajowych implementujących tzw. dyrektywę Omnibus (dyrektywa 2019/2161). W tym przypadku sprowadzać się to będzie przede wszystkim do wprowadzenia szeregu bezpieczników gwarantujących prawidłowe wyświetlanie informacji generowanych lub zarządzanych przez sztuczną inteligencję. Przykładowo, należy pamiętać o tym, że jeśli system AI samodzielnie podejmuje decyzje o zmianie (obniżce) ceny danego produktu lub usługi (np. ze względu na zwiększony popyt lub akcję promocyjną) koniecznym będzie wyświetlanie wszystkich informacji wymaganych prawem, a więc - co do zasady - o cenie promocyjnej, najniższej cenie w ciągu ostatnich 30 dni oraz cenie stosowanej przed zastosowaniem obniżki.

Możliwym jest również, że dany system będzie dokonywać samodzielnego plasowania produktów oferowanych w ramach internetowej platformy handlowej (upraszając – marketplace'u). W takim przypadku należy udostępnić na platformie informację dotyczącą głównych parametrów decydujących o plasowania produktów w ramach wyszukiwarki udostępnianej konsumentowi oraz względnego znaczenia tych parametrów w porównaniu z innymi. Wydaje się, że w części przypadków realizacja tego obowiązku będzie szczególnie utrudniona, w szczególności gdy dany system będzie posiadać dużą autonomię decyzyjną.

Obecnie trwają prace nad takimi przepisami jak AI Act (Articifial Intelligence Act), czy ALID (AI Liability Directive), które mogą znacząco wpłynąć na możliwość, zakres oraz sposób oddziaływania AI na konsumentów.

Sztuczna Inteligencja a ryzyka po stronie konsumentów

Sztuczna Inteligencja a zasady ponoszenia odpowiedzialności za jej działania.

Przedmiotowe zagadnienie tak naprawdę można podzielić na dwa, tj. jak jest obecnie oraz jak będzie, w bliższej lub dalszej przyszłości. Obecnie bowiem należy dokonywać oceny AI zgodnie z obowiązującymi przepisami, które nie są adekwatne i po prostu nie obejmują skomplikowanych zagadnień związanych ze sztuczną inteligencją oraz potencjalnymi szkodami, które mogą powstać wskutek jej błędów.

Przede wszystkim nie sposób uznać AI za produkt niebezpieczny. Na gruncie polskich przepisów (art. 449(1) Kodeksu cywilnego) za produkt taki uznaje się bowiem rzecz ruchomą, choćby została połączona z inną rzeczą, jak również zwierzęta i energię elektryczną. Co za tym idzie, nie jest możliwe zastosowanie względem twórców AI reżimu odpowiedzialności za produkt niebezpieczny, zgodnie z którym, kto wytwarza w zakresie swojej działalności gospodarczej taki produkt, odpowiada za szkodę wyrządzoną komukolwiek przez ten produkt.

Oznacza to, że odpowiedzialność za szkody powstałe w związku z wykorzystaniem sztucznej inteligencji powinna być oceniana na zasadach ogólnych.

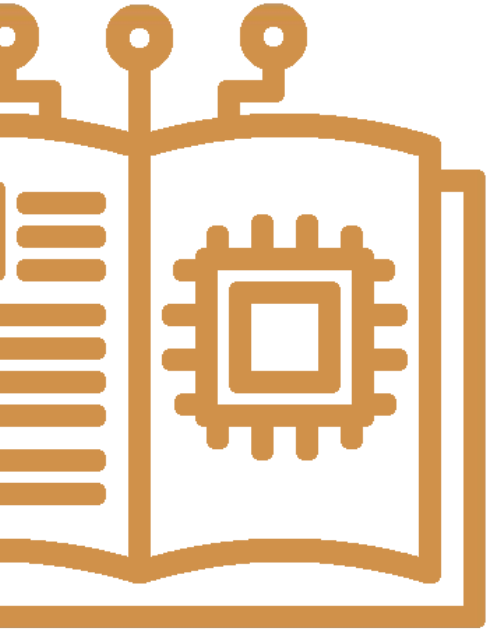
Co za tym idzie, w celu skutecznego dochodzenia roszczeń dany podmiot musi udowodnić:

I. wysokość poniesionej szkody;
II. **winę** osoby trzeciej;
III. związek przyczynowy pomiędzy działaniem lub zaniechaniem danej osoby a powstałą szkodą.

Takie uregulowanie zasad odpowiedzialności w kontekście AI powoduje, że obecnie dochodzenie ewentualnych roszczeń może być ekstremalnie trudne. Dlaczego?

Jest to specyfika prawa cywilnego. Gwoli zajawki, wina sprawcy może być umyślna albo nieumyślna. Nawet na poziomie winy nieumyślnej trzeba wykazać niezachowanie wymaganej staranności, a sam miernik należytej staranności nie może być z góry określony na poziomie ogólnym i powinien być każdorazowo określany indywidualnie na gruncie okoliczności faktycznych danej sprawy.

Sztuczna Inteligencja a ryzyka po stronie konsumentów



Organy Unii Europejskiej zdają sobie sprawę, że obecnie istniejące normy prawne nie uwzględniają kwestii AI. W związku z tym, w zeszłym roku Komisja Europejska opublikowała projekt dyrektywy w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję).

W ślad za AI Act (o którym piszemy dalej), dyrektywa ta wyróżnia zarówno systemy sztucznej inteligencji, jak i systemy sztucznej inteligencji wysokiego ryzyka, jednocześnie nakazując państwom członkowskim wprowadzenie przepisów umożliwiających zabezpieczenie oraz ujawnienie dowodów dotyczących sposobów działania systemu sztucznej inteligencji wysokiego ryzyka.

Ponadto projekt dyrektywy zakłada wprowadzenie wzruszalnego domniemania istnienia związku przyczynowego w przypadku winy (oznacza to, że przy spełnieniu pewnych przesłanek powstawać będzie możliwe do zakwestionowania domniemanie, że istnieje związek przyczynowy pomiędzy winą pozwanego podmiotu, a wynikiem uzyskanym przez system sztucznej inteligencji lub faktem nieuzyskania przez taki system wyniku).

Proponowane przez Komisję przepisy mają na celu ułatwienie dochodzenia roszczeń odszkodowawczych związanych z działaniem sztucznej inteligencji. Mając na uwadze te propozycje z pewnością w przyszłości obrona swoich interesów naruszonych przez działanie sztucznej inteligencji będzie łatwiejsze i skuteczniejsze.

Sztuczna Inteligencja a ryzyka po stronie konsumentów

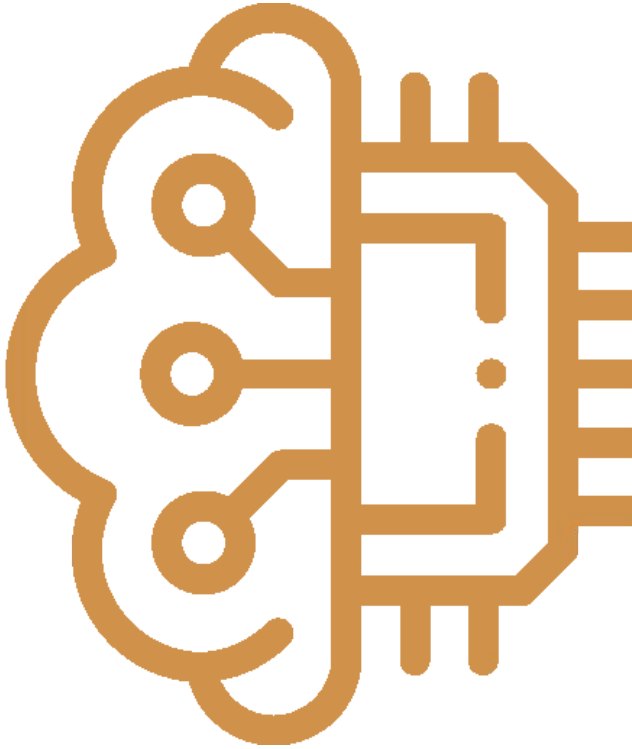
Kto ponosi odpowiedzialność: producent, programista czy użytkownik?

Ponadto na gruncie obecnie obowiązujących przepisów wątpliwości może budzić to kto ponosi odpowiedzialność za dane zdarzenie. Czy będzie podmiot, który wprowadził AI na rynek, dany programista czy może użytkownik, który w taki a nie inny sposób wykorzystał możliwości, które daje dany system sztucznej inteligencji.

W większości przypadków sam **programista** będzie ponosić ewentualną odpowiedzialność wyłącznie względem podmiotu, który zlecił mu prace nad AI (chyba, że samodzielnie działa jako producent lub dystrybutor danego systemu sztucznej inteligencji).

Wynika to bowiem z istoty odpowiedzialności kontraktowej – twórca działa na podstawie umowy, w ramach której ustalone zostały zasady jego odpowiedzialności (mogą one również wynikać z przepisów ogólnych, jeśli odpowiednie postanowienia nie znalazły się w umowie).

Pamiętać przy tym należy, że jeśli AI będzie posiadać ukryte błędy, które spowodują szkody wśród użytkowników, w niektórych przypadkach możliwe jest dochodzenie od programisty roszczeń przez producenta/dystrybutora w ramach tzw. **odpowiedzialności regresowej**.



Sztuczna Inteligencja a ryzyka po stronie konsumentów

Z kolei podmiot, który **wprowadził dany system na rynek** może ponosić zarówno odpowiedzialność kontraktową, jak i deliktową. Odpowiedzialność kontraktowa powstanie np. wtedy gdy AI nie będzie mogła być wykorzystywana do założonych celów, a podmiot trzeci dokonał zapłaty za dostęp do danego systemu. W przypadku odpowiedzialności deliktowej aktualne pozostają problemy dowodowe, o których mowa wcześniej, jednak teoretycznie możliwe jest pociągnięcie do odpowiedzialności podmiotu, który oferuje dane rozwiązanie.

Sam **użytkownik** (osoba, która w jakimś celu będzie korzystać z AI) również może ponieść przede wszystkim odpowiedzialność deliktową (za czyn niedozwolony) – przykładowo można wyobrazić sobie sytuację, w której system posłuży do wygenerowania nieprawdziwych treści dotyczących danej osoby, które to treści następnie zostaną opublikowane przez użytkownika jako prawdziwe. Takie działanie stanowić będzie naruszenie dóbr osobistych osoby trzeciej, która w związku z tym będzie mogła dochodzić roszczeń przeciwko osobie na polecenie której doszło do wygenerowania poszczególnych treści. W tym kontekście pamiętać należy, że przy ocenie działania użytkownika należy brać pod uwagę czy działał świadomie, czy też to system AI wprowadził go w błąd.

W przypadku AI zakres oraz podstawa odpowiedzialności mogą bardzo się różnić - wszystko zależy od relacji danej osoby z danym systemem. Odpowiedzialność programisty zwykle będzie ograniczona do odpowiedzialności kontraktowej (umownej) z jego zleceniodawcą. Z kolei podmiot, który wprowadził dany system na rynek, odpowiadać będzie zarówno za niezgodność działania systemu z umową zawartą z użytkownikiem końcowym, jak również za szkody wywołane po stronie osób trzecich.

LAW MORE

planowane regulacje dotyczące AI

Planowane regulacje dotyczące AI

Unia Europejska i AI Act

Dnia 21 kwietnia 2021 r. Komisja Europejska przedstawiła projekt unijnego Rozporządzenia w sprawie sztucznej inteligencji (Artificial Intelligence Act). Jest to wynik kilkuletniego planu, tzw. europejskiej strategii na rzecz sztucznej inteligencji, która została przyjęta w kwietniu 2018 r.

W założeniu, AI Act ma zapewniać działanie systemów sztucznej inteligencji w UE w sposób bezpieczny, przejrzysty, etyczny, bezstronny i kontrolowany przez człowieka, a sama Unia Europejska ma w założeniu stać się **globalnym centrum wiarygodnej sztucznej inteligencji**.

AI Act ma za zadanie wprowadzić przepisy m.in. dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w całej Unii Europejskiej. Jednocześnie na jego mocy ustanowione mają zostać zakazy dotyczące określonych praktyk związanych z wykorzystaniem sztucznej inteligencji, szczególne wymogi dotyczące systemów AI wysokiego ryzyka, jak również wymogi w zakresie przejrzystości - w szczególności co do narzędzi AI mających wchodzić w interakcje z osobami fizycznymi.

Rozporządzenie obejmuje również wymogi jakości zbiorów danych treningowych, walidacyjnych i testowych używanych do trenowania systemów AI, a także kwestie monitorowania narzędzi AI po ich wprowadzeniu do obrotu i nadzoru nad rynkiem.

Komisja przyjęła w AI Act założenie, że narzędzia sztucznej inteligencji powinny zostać **skategoryzowane pod względem ryzyka dla praw i wolności człowieka** jakie wiąże się z ich używaniem, a im wyższe ryzyko, tym więcej obowiązków i obostrzeń.

Planowane regulacje dotyczące AI

Wskazano następujące kategorie ryzyka:

1. Niedopuszczalne ryzyko (i tzw. zakazane systemy AI)

   Jako obarczone niedopuszczalnym ryzykiem wskazuje się szczególne zastosowania AI. W tej kategorii wymienia się m.in. prowadzona przez rządy punktowa ocena obywateli – tzw. social scoring (system używany w Chińskiej Republice Ludowej) służący do monitorowania zachowania obywateli pod kątem zgodności z normami prawnymi i społecznymi. W tej kategorii wymieniane jest także stosowanie podprogowych technik lub techniki celowej manipulacji, jak również systemów zdalnej identyfikacji biometrycznej ‘w czasie rzeczywistym’ w miejscach publicznie dostępnych. Powyższe sposoby używania AI jako sprzeczne z prawami podstawowymi, zostaną zakazane.

2. Wysokie ryzyko

   Systemy AI wysokiego ryzyka klasyfikowane jako takie na podstawie dwóch przesłanek. Po pierwsze, musi to być rozwiązanie wskazane w załączniku nr 3 do Rozporządzenia, tj. w wykazie systemów AI wysokiego ryzyka. Po drugie, taki system będzie jeszcze musiał stwarzać znaczące ryzyko powstania szkody dla zdrowia, bezpieczeństwa, praw obywatelskich lub środowiska. Z kolei w załączniku zostały wskazane systemy AI wykorzystywane w - przykładowo - następujących obszarach:

   - zarządzanie infrastrukturą krytyczną i jej eksploatacja - systemy AI wykorzystywane w procesach zarządzania i obsługi ruchu drogowego oraz zaopatrzenia w wodę, gaz, ciepło i energię elektryczną;
   - kształcenie i szkolenie zawodowe - systemy AI przeznaczone do stosowania w celu podejmowania decyzji o dostępie do instytucji edukacyjnych i instytucji szkolenia zawodowego lub nadawania osobom przydziału do tych instytucji;

Planowane regulacje dotyczące AI

- zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia - systemy sztucznej inteligencji przeznaczone do rekrutacji lub wyboru osób fizycznych, w szczególności w przypadku informowania o wakatach, selekcji lub filtrowania podań o pracę, oceny kandydatów w trakcie rozmów kwalifikacyjnych, podejmowania decyzji o awansie i rozwiązaniu stosunku pracy, przydzielania zadań oraz monitorowania i oceny wydajności i zachowania osób pozostających w takich stosunkach.

Tworząc i wdrażając systemy AI wysokiego ryzyka konieczne będzie zachowanie wymagań wskazanych w AI Act. Wymagania te to m.in. obowiązek wdrożenia systemu zarządzania ryzykiem, spełnianie kryteriów jakości dla zbiorów danych wykorzystywanych do szkolenia i testowania AI oraz wymóg sporządzania i aktualizowania dokumentacji technicznej systemu.

Dodatkowo, systemy AI wysokiego ryzyka muszą być zaprojektowane w taki sposób, aby automatycznie rejestrowały zdarzenia podczas działania systemu (tzw. logi) oraz aby umożliwić ludziom skuteczne ich nadzorowanie, w tym zrozumienie możliwości i ograniczeń danego systemu sztucznej inteligencji. Nadzór człowieka nad systemem AI ma obejmować m.in. podjęcie decyzji o nieużywaniu systemu AI w danej sytuacji, zignorowanie decyzji podjętej przez system AI lub natychmiastowe przerwanie działania systemu.

W celu skutecznego zapewnienia ochrony podstawowych praw, osoba wdrażająca systemy AI wysokiego ryzyka powinna również przeprowadzić ***fundamental rights impact assessment*** przed uruchomieniem systemu. Ocena taka powinna być poprzedzona szczegółowym planem opisującym środki lub narzędzia, które pomogą zminimalizować ryzyka dla podstawowych praw, zidentyfikowane najpóźniej od momentu uruchomienia systemu. Przy przeprowadzaniu ww. oceny, osoba wdrażająca powinna powiadomić m.in. krajowy organ nadzorczy. Zachęca się również do udostępnienia publicznie, podsumowania przeprowadzonej *fundamental rights impact assessment* na stronie internetowej danego systemu.

Planowane regulacje dotyczące AI

3. Ograniczone ryzyko

Ograniczone ryzyko przypisano systemom AI, których wykorzystanie może wiązać się z wyraźnym ryzykiem manipulacji (np. w przypadku chatbotów). AI Act zakłada minimalne obowiązki w zakresie przejrzystości co do tych systemów, tak aby użytkownik mógł podejmować świadome decyzje wchodząc w interakcję z takim narzędziem. Użytkownicy powinni być świadomi, że wchodzą w interakcję z maszyną, tak aby mogli podjąć decyzję o kontynuowaniu korzystania z danej aplikacji (narzędzia) lub o rezygnacji z jej używania.

Modele fundamentalne

AI Act uwzględnia również modele fundamentalne i AI ogólnego przeznaczenia. W ramach modeli fundamentalnych powinno zostać m.in. ocenione i ograniczone możliwe ryzyka i szkody poprzez odpowiednie projektowanie, testowanie i analizę, powinny zostać wprowadzone środki zarządzania danymi (w tym przeciwdziałanie dyskryminacji) oraz powinny zostać spełnione wymagania techniczne i projektowe dla zapewnienia odpowiedniego poziomu wydajności, przewidywalności, interpretowalności, poprawności, bezpieczeństwa i cyberbezpieczeństwa oraz dla zaadresowania odpowiednich norm środowiskowych. Nie oznacza to jednak, że modele fundamentalne będą traktowane jako systemy AI wysokiego ryzyka.

Planowane regulacje dotyczące AI

- **Piaskownice regulacyjne**

Poza powyższą kategoryzacją systemów AI i związanymi z tym obowiązkami, Rozporządzenie przewiduje również wprowadzenie piaskownic regulacyjnych (tzw. regulatory sandbox). Piaskownice regulacyjne mają zapewniać kontrolowane środowisko ułatwiające opracowywanie, testowanie i walidację systemów AI przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem ich do użytku zgodnie z określonym planem.

- **AI Office**

Ponadto, AI Act przewiduje wprowadzenie nowego organu tj. AI Office. Do zadań Biura będzie należało m.in.: gromadzenie i rozpowszechnianie wiedzy specjalistycznej i dobrych praktyk wśród państw członkowskich, wydawanie opinii i rekomendacji w sprawach związanych z implementacją oraz przyczynianie się do jednolitego stosowania rozporządzenia, szczególnie w odniesieniu do tzw. piaskownic regulacyjnych.

- **Standaryzacje**

Branża AI nie zostanie jednak pozostawiona sama sobie w stosowaniu AI Act. Rozporządzenie przewiduje szereg instytucji, które mają wyklaryfikować aspekty praktyczne i doprecyzować wymogi prawa, między innymi będą to unijne standaryzacje i specyfikacje. Komisja określi również między innymi kryteria umożliwiające przedsiębiorstwom ocenę, czy ich system AI może być systemem wysokiego ryzyka.

- **Open source**

Autorzy darmowych i open source'owych komponentów AI pod pewnymi warunkami nie będą podlegać pod wymogi AI Act, a w szczególności nie wobec dostawcy, który wykorzystał taki komponent sztucznej inteligencji.

Planowane regulacje dotyczące AI

Wielka Brytania i podejście „pro-innowacyjne” do regulacji AI

W opublikowanym w marcu 2023 r. policy paper (dokumencie niezawierającym konkretnych przepisów a jedynie dyrektywy działania) opisano plan Wielkiej Brytanii w odniesieniu do regulowania sztucznej inteligencji. W dokumencie tym, wprost wskazano, że celem prawodawstwa UK powinno być takie podejście, które umożliwi szybki rozwój i wdrożenie narzędzi AI w Wielkiej Brytanii i tym samym pozwoli zająć Wielkiej Brytanii pozycję lidera we wprowadzaniu tej technologii.

Podobnie jak Komisja Europejska, regulator brytyjski promuje podejście oparte na ewaluacji ryzyka związanego z systemami AI. W odróżnieniu jednak od unijnego AI Act, ustawodawca brytyjski zakłada wprowadzenie regulacji, które „zapewnią jasne wytyczne, które jednak niekoniecznie przełożą się na szczególne obostrzenia”.

Brytyjczycy wskazali również odmienny od unijnego sposób nadzorowania podmiotów stosujących rozwiązania oparte o sztuczną inteligencję. W Wielkiej Brytanii nadzór nad rozwojem i wdrażaniem sztucznej inteligencji i związanych z tym regulacji, zostanie powierzony istniejącym już organom kontrolnym, m.in.:Financial Conduct Authority (odpowiednik Komisji Nadzoru Finansowego), Competition and Markets Authority (Urząd ds. Konkurencji i Rynku), Information Commissioner's Office (Komisarz ds. informacji) oraz Medicine and Healthcare products Regulatory Agency (Agencja Regulacyjna ds. Leków i Produktów Ochrony Zdrowia). Instytucje te zyskają nowe obowiązki i kompetencje związane m.in. z identyfikacją i oceną występujących ryzyk.

Które podejście jest lepsze? Czas pokaże.

podsumowanie

Podsumowanie

Mając do czynienia z szybkim rozwojem algorytmów sztucznej inteligencji, a jednocześnie z brakiem aktualnych i wdrożonych rozwiązań prawnych dotyczących stricte AI trzeba szczególnie dokładnie oceniać ryzyko związane z używaniem, tworzeniem i wdrażaniem narzędzi AI. Poniżej znajduje się zbiór rekomendacji dotyczących prawnych aspektów związanych z prowadzeniem projektów opartych na sztucznej inteligencji.

- Rozpoczynając prace nad wdrożeniem systemu AI warto zastanowić się co chcemy monetyzować: sam algorytm, dane treningowe, dane wyjściowe, czy jeszcze jakiś inny aspekt wykorzystania AI. Będzie to wpływało na strategię ochrony tych komponentów, sposób realizacji obowiązków prawnych oraz pośrednio na zakres naszej odpowiedzialności.

- Należy ocenić jakie dokładnie prawa możemy mieć albo chcemy mieć do tego najbardziej interesującego dla klienta elementu projektu, np. czy możemy mieć wyłączność na korzystanie z tego elementu, czy też musimy udostępnić go na pewnych zasadach; czy w danym przypadku powstaną prawa wyłączne tj. autorskie albo do wynalazku; czy zawsze prawa autorskie muszą być tutaj przekazywane w całości, czy jednak zależy nam np. na licencji wyłącznej etc.

- W każdym przypadku należy zadbać o zbiory danych używanych do trenowania algorytmu. Należy pamiętać, że jeżeli dane treningowe będą tendencyjne, obarczone błędami lub błędnie zebrane, możemy ponosić za to odpowiedzialność. Dodatkowo trzeba ocenić, czy używanie konkretnych danych treningowych nie naruszy tajemnicy przedsiębiorstwa (lub innej tajemnicy prawnie chronionej) lub praw autorskich osoby trzeciej.

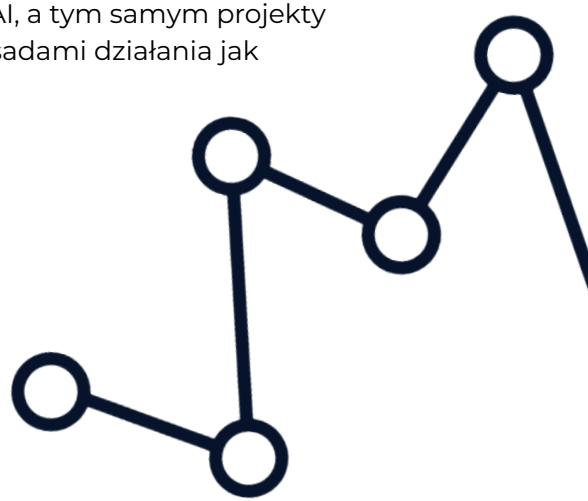
- Jeżeli algorytm AI w projekcie jest tworzony w ramach umowy – należy w niej dokładnie określić rolę każdej ze stron, w tym przede wszystkim w zakresie odpowiedzialności co do spełniania przez system AI wymogów przewidzianych przez prawo (np. przez AI Act który wkrótce wejdzie w życie).

Podsumowanie

Używając do trenowania danych osobowych należy szczególnie uważnie ocenić ryzyko z tym związane, w szczególności w zakresie możliwości zapewnienia prawa do zaprzestania przetwarzania danych osobowych. Należy ocenić czy konieczne jest przeprowadzenie DPIA oraz ustalić czy dane będą przekazywane poza obszar EOG – a jeżeli tak, to konieczne będzie spełnienie warunków takiego przekazywania. Trzeba również zastanowić się czy osoby trzecie będą w ramach projektu przetwarzać dane osobowe – jeżeli tak to należy zawrzeć z tymi osobami odpowiednie umowy o powierzeniu przetwarzania danych. Aby uniknąć powyższych obowiązków rekomendowane jest używanie danych zanonimizowanych.

Jeżeli w ramach projektu korzystamy z algorytmu AI od zewnętrznego dostawcy lub dostępnego na podstawie licencji etc. istotne jest, aby ocenić ryzyko wystąpienia po naszej stronie odpowiedzialności za działanie algorytmu niezgodnie z obowiązującymi wytycznymi. Ma to znaczenie zwłaszcza przy systemach wysokiego ryzyka opisanych w załączniku nr III do unijnego Rozporządzenia AI.

Pamiętaj, że w świetle wdrażanych obecnie przepisów – zwłaszcza unijnych – narzędzia AI, a tym samym projekty wdrażające rozwiązania oparte na sztucznej inteligencji, powinny kierować się takimi zasadami działania jak transparentność, rozliczalność i bezpieczeństwo.



LAWMORE

ebook o prawnych aspektach Gen AI

Autorki i autor:

r.pr. Dominika Wcisło
rz.pat. Aleksandra Maciejewicz
r.pr. Milena Balcerzak
adw. Bartłomiej Serafinowicz

Kontakt:

biuro@lawmore.pl