



ai act czyli AI dziś i jutro

Jakub Cieśllicki

RADCA PRAWNY

Cieśllicki i wspólnicy spk

Narutowicza 14/2

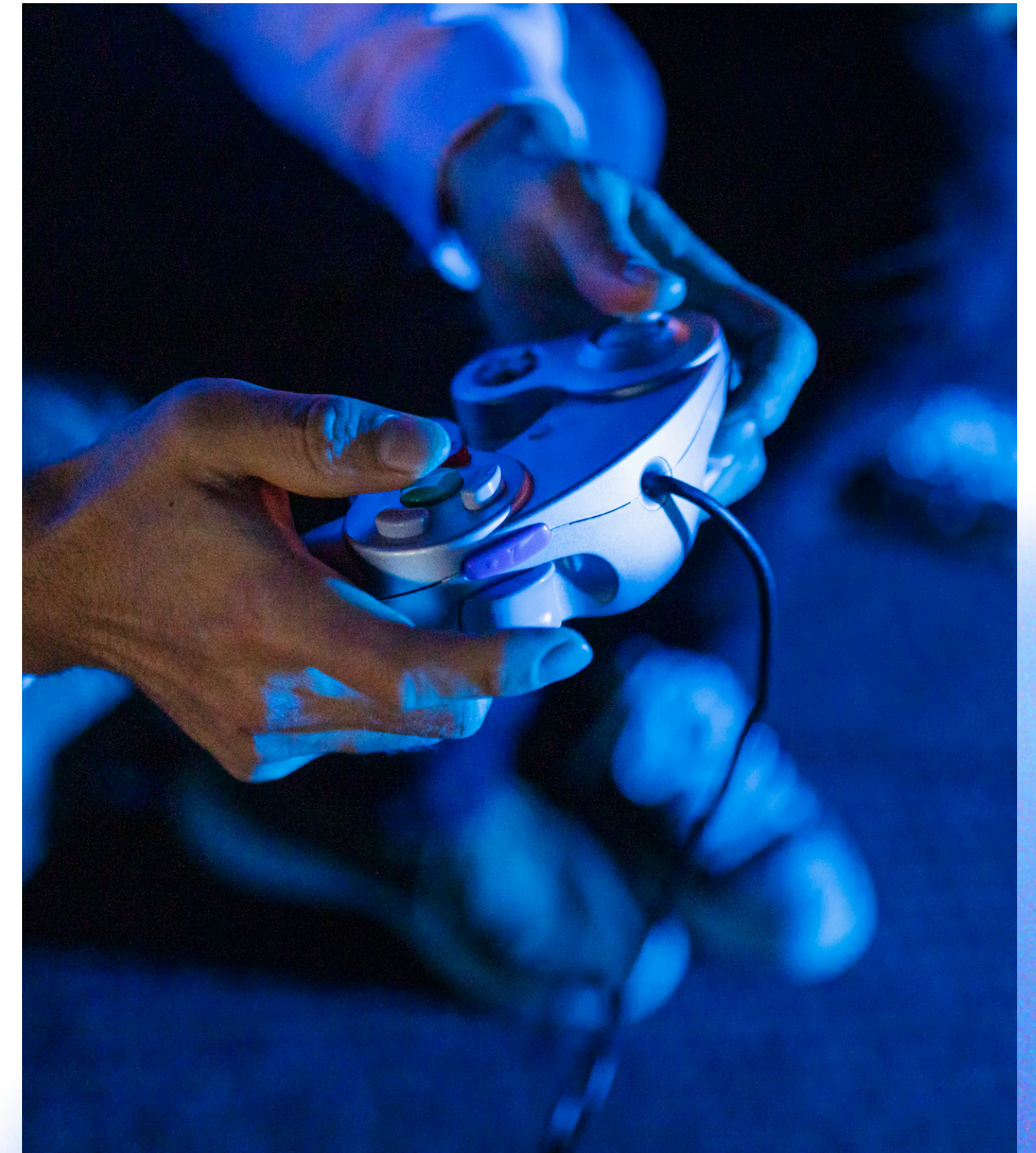
70-240 Szczecin

Problemy

1 normatywna definicja AI, która nie będzie poddawała się inflacji

2 zapewnienie bezpieczeństwa w niezwykle dynamicznym świecie IT

3 utrzymanie rozwoju branży



Propozycja wartości

- 1 AI może stwarzać zagrożenia i wyrządzać szkody dla interesu publicznego i praw podstawowych.
szkody te mogą być materialne lub niematerialne, w tym fizyczne, psychiczne, społeczne lub ekonomiczne.
- 2 AI ma być technologią zorientowaną na człowieka
- 3 AI powinna służyć jako narzędzie dla ludzi, którego ostatecznym celem jest zwiększenie dobrostanu człowieka



wymuszenie własnego zastosowania

Aby zapobiec obchodzeniu przepisów niniejszego rozporządzenia oraz zapewnić skuteczną ochronę osób fizycznych znajdujących się w Unii, niniejsze rozporządzenie powinno mieć również zastosowanie do dostawców i podmiotów stosujących systemy AI, którzy mają siedzibę lub miejsce zamieszkania w państwie trzecim, w zakresie, w jakim wyniki wytworzone przez te systemy są przeznaczone do wykorzystywania w Unii.



Dostawców
wprowadzających do
obrotu lub oddających
do użytku systemy AI
(niezależnie gdzie
siedziba)

Stosujących systemy AI
(w UE)

dostawców systemów
AI i podmiotów
stosujących systemy AI
(w UE lub poza) jeżeli
wyniki systemu AI są
stosowane w UE

importerów i
dystributorów
systemów AI

osób, na które AI ma
wpływ i które znajdują
się w UE



od 02.02.2025

stosuje się przepisy rozdziału I i II

ZAKAZANE PRAKTYKI

systemu AI, który stosuje techniki podprogowe będące poza świadomością danej osoby lub celowe techniki manipulacyjne lub wprowadzające w błąd, czego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub grupy osób poprzez znaczące ograniczenie ich zdolności do podejmowania świadomych decyzji, powodując tym samym podjęcie przez nie decyzji, której inaczej by nie podjęły, w sposób, który wyrządza lub może wyrządzić u niej, u innej osoby lub u grupy osób poważną szkodę;

systemu AI, który wykorzystuje słabości osoby fizycznej lub określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną, którego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub osoby należącej do tej grupy w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić u tej osoby lub u innej osoby poważną szkodę;

systemów AI na potrzeby oceny lub klasyfikacji osób fizycznych lub grup osób prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych, wywnioskowanych lub przewidywanych cech osobistych lub cech osobowości, kiedy to scoring społeczny prowadzi do jednego lub obu z następujących skutków:

- 1) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub grup osób w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zebrano dane;
- 2) krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub grup osób, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;

systemu AI do przeprowadzania ocen ryzyka w odniesieniu do osób fizycznych, by ocenić lub przewidzieć ryzyko popełnienia przestępstwa przez osobę fizyczną, wyłącznie na podstawie profilowania osoby fizycznej lub oceny jej cech osobowości i cech charakterystycznych; zakaz ten nie ma zastosowania do systemów AI wykorzystywanych do wspierania dokonywanej przez człowieka oceny udziału danej osoby w działalności przestępczej, która to ocena opiera się już na obiektywnych i weryfikowalnych faktach bezpośrednio związanych z działalnością przestępczą;

wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemów AI, które tworzą lub rozbudowują bazy danych służące rozpoznawaniu twarzy poprzez nieukierunkowane pozyskiwanie (ang. untargeted scraping) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej

wprowadzania do obrotu, oddawania do użytku w tym konkretnym celu lub wykorzystywania systemów AI do wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych, z wyjątkiem przypadków, w których system AI ma zostać wdrożony lub wprowadzony do obrotu ze względów medycznych lub bezpieczeństwa;

zakazuje się wprowadzania do obrotu, oddawania do użytku, lub wykorzystywania systemu AI, który:



stosuje techniki podprogowe będące poza świadomością danej osoby lub celowe techniki manipulacyjne lub wprowadzające w błąd



czego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub grupy osób poprzez znaczące ograniczenie ich zdolności do podejmowania świadomych decyzji,



powodując tym samym podjęcie przez nie decyzji, której inaczej by nie podjęły, w sposób, który wyrządza lub może wyrządzić u niej, u innej osoby lub u grupy osób poważną szkodę;

zakazuje się wprowadzania do obrotu, oddawania do użytku, lub wykorzystywania systemu AI, który:



wykorzystuje słabości osoby fizycznej lub określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną



którego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub osoby należącej do tej grupy w sposób,



który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić u tej osoby lub u innej osoby poważną szkodę;

zakazuje się wprowadzania do obrotu, oddawania do użytku, lub wykorzystywania systemu AI, który:



na potrzeby oceny lub klasyfikacji osób fizycznych lub grup osób



prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych, wywnioskowanych lub przewidywanych cech osobistych lub cech osobowości, kiedy to scoring społeczny prowadzi do jednego lub obu z następujących skutków



krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub grup osób w kontekstach społecznych, które nie są związane z kontekstami, w których pierwotnie wygenerowano lub zebrano dane;

krzywdzącego lub niekorzystnego traktowania niektórych osób fizycznych lub grup osób, które jest nieuzasadnione lub nieproporcjonalne do ich zachowania społecznego lub jego wagi;

zakazuje się wprowadzania do obrotu, oddawania do użytku, lub wykorzystywania systemu AI, do przeprowadzania ocen ryzyka w odniesieniu do osób fizycznych:



by ocenić lub przewidzieć ryzyko popełnienia przestępstwa przez osobę fizyczną, wyłącznie na podstawie profilowania osoby fizycznej lub oceny jej cech osobowości i cech charakterystycznych



zakaz ten nie ma zastosowania do systemów AI wykorzystywanych do wspierania dokonywanej przez człowieka oceny udziału danej osoby w działalności przestępczej, która to ocena opiera się już na obiektywnych i weryfikowalnych faktach bezpośrednio związanych z działalnością przestępczą;

zakazuje się wprowadzania do obrotu, oddawania do użytku, lub wykorzystywania systemu AI, które:



tworzą lub rozbudowują bazy danych służące rozpoznawaniu twarzy poprzez nieukierunkowane pozyskiwanie (ang. *untargeted scraping*) wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej

zakazuje się wprowadzania do obrotu, oddawania do użytku, lub wykorzystywania systemu AI



do wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy lub instytucjach edukacyjnych, z wyjątkiem przypadków, w których system AI ma zostać wdrożony lub wprowadzony do obrotu ze względów medycznych lub bezpieczeństwa



częściowo od 2.08.2025
całościowo od 2.08.2026

Dostawców
wprowadzających do
obrotu lub oddających
do użytku systemy AI
(niezależnie gdzie
siedziba)

Stosujących systemy AI
(w UE)

» wprowadzenie do obrotu:
udostępnienie po raz pierwszy systemu AI lub modelu ogólnego przeznaczenia na rynku Unii

udostępnienie na rynku:
dostarczenie systemu AI lub modelu AI ogólnego przeznaczenia w celu jego dystrybucji lub wykorzystania na rynku Unii w ramach działalności handlowej, odpłatnie lub nieodpłatnie

oddanie do użytku:
dostarczenie systemu AI do pierwszego użycia bezpośrednio podmiotowi stosującemu lub do użytku własnego w Unii, zgodnie z jego przeznaczeniem



dostawca:
podmiot, który rozwija system AI lub model AI
ogólnego przeznaczenia lub zleca ich rozwój

oraz

który odpłatnie lub nieodpłatnie, pod własną nazwą
lub własnym znakiem towarowym wprowadza je
do obrotu lub oddaje do użytku



podmiot stosujący:

podmiot, który wykorzystuje system AI, nad którym sprawuje kontrolę

(z wyłączeniem pozzawodowej działalności osobistej)



model AI ogólnego przeznaczenia

model, który wykazuje znaczną ogólność i jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań, niezależnie od sposobu, w jaki model ten jest wprowadzany do obrotu i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla - z wyłączeniem modeli AI, które są wykorzystywane na potrzeby działań w zakresie badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu



systemy ai wysokiego ryzyka



systemy ai wysokiego ryzyka

przeznaczony do wykorzystania jako
związany z bezpieczeństwem element
produktu objętego unijnym prawem
harmonizacyjnym, lub sam jest takim
produktem - załącznik nr 1



systemy ai wysokiego ryzyka

dyrektywa maszynowa 2006/42/WE

dyrektywa zabawkowa 2009/48/WE

dyrektywa dźwigowa 2014/33/WE

rozporządzenie wyroby medyczne 2017/745



systemy ai wysokiego ryzyka
produkt, w którym elementem
związanym z bezpieczeństwem jest
system AI lub samo AI jest tym
produktem, i jako produkt podlegają
ocenie zgodności przez podmiot trzeci
- załącznik nr 1



systemy ai wysokiego ryzyka

załącznik nr III

»» systemy ai wysokiego ryzyka

decydujące o przyjęciu do szkół

oceniania uczenia się i kierowania procesem uczenia się

ocena kandydatów do pracy

wspierające w decyzjach o awansie, rozwiązywania umowy

monitorujące wydajność pracownika

kwalifikowalność osób do korzystania z usług

publicznych

»» systemy ai wysokiego ryzyka wymagania

system zarządzania ryzykiem jako (1)
ciągły, (2) iteracyjny proces, (3)
planowany i realizowany przez (4)
cały cykl życia systemu AI
wysokiego ryzyka

» systemy ai wysokiego ryzyka

wymagania

zbiory danych treningowych

zbiory danych walidacyjnych

zbiory danych testowych

adekwatne, wystarczająco reprezentatywne, w jak największym stopniu wolne od błędów i kompletne oraz o odpowiednich właściwościach statystycznych ale jednocześnie specyficzne dla określonego otoczenia geograficznego, kontekstualnego, behawioralnego w którym AI ma być stosowane

»» systemy ai wysokiego ryzyka wymagania

Dokumentacja techniczna

ma wykazać, że system AI jest zgodny z
wymogami AI ACT

»» systemy ai wysokiego ryzyka wymagania

Techniczna możliwość
automatycznego rejestrowania
zdarzeń w całym cyklu życia danego
systemu.

»» systemy ai wysokiego ryzyka wymagania

skuteczny nadzór przez
osobę fizyczną

przez cały okres
wykorzystywania systemu AI

»» systemy ai wysokiego ryzyka wymagania

projektowanie i rozwijanie w
sposób zapewniający
odpowiedni poziom
dokładności solidności i
cyberbezpieczeństwa

»» systemy ai wysokiego ryzyka wymagania

odporność na próby osób
nieuprawnionych zmiany ich
wykorzystania, wyników lub
skuteczności działania

»» systemy ai wysokiego ryzyka wymagania

10 lat, od dnia wprowadzenia
systemu AI do obrotu lub oddania
go do użytku, DOSTAWCA
przechowuje szereg dokumentów
(m.in. dokumentację techniczną)



odpowiedzialność
obowiązki importerów
obowiązki dystrybutorów
obowiązki stosujących AI



chińczycy też mają AI ACT!





KONIEC :)