KONIECZNY WIERZBICKI
KANCELARIA RADCÓW PRAWNYCH

Artificial Intelligence Act- projekt unijnego rozporządzenia w sprawie sztucznej inteligencji

Konieczny Wierzbicki
Kancelaria Radców
Prawnych

2021

KONTEKST, ZAKRES I CEL

Artificial
Intelligence Act

Artificial Intelligence Act

KONTEKST

BUDOWA EUROPEJSKICH RAM PRAWNYCH AI

2018 Europejska strategia na rzecz sztucznej inteligencji

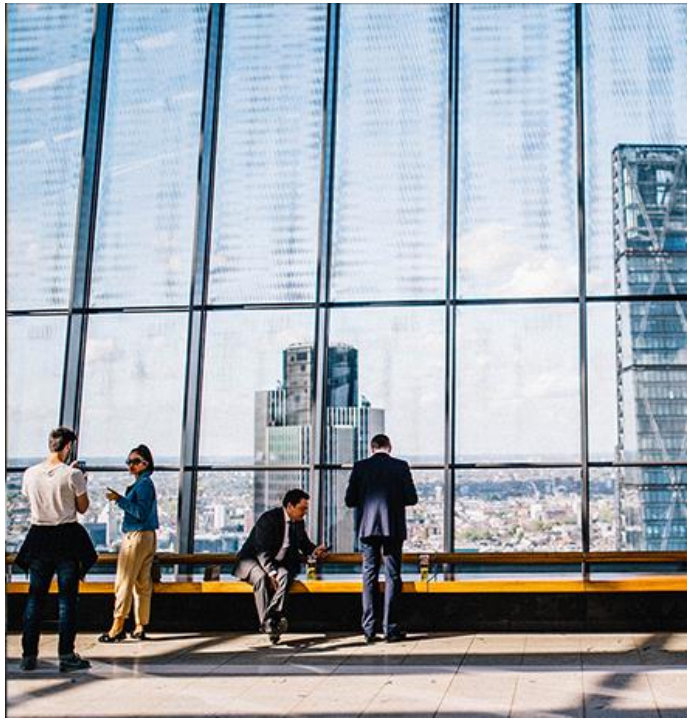
Skoordynowany plan wspierania rozwoju i stosowania sztucznej inteligencji w Europie

2019 Wytyczne dotyczące wiarygodności sztucznej inteligencji

2020 Lista kontrolna w zakresie wiarygodnej sztucznej inteligencji

Biała księga EU w sprawie AI

2021 Projekt unijnego rozporządzenia w sprawie sztucznej inteligencji (Artificial Intelligence Act)



Artificial Intelligence Act

CELE REGULACJI

BEZPIECZEŃSTWO

Zagwarantowanie bezpieczeństwa obywateli i przedsiębiorstw

POWSZECHNOŚĆ

Upowszechnienie rozwiązań opartych na sztucznej inteligencji

ROZWÓJ

Zwiększenie innowacyjności i inwestycji w dziedzinie sztucznej inteligencji w całej Unii Europejskiej

PRAWNE RAMY ROZPORZĄDZENIA

Artificial Intelligence Act

Artificial Intelligence Act

ZAKRES REGULACJI

- zharmonizowane przepisy dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w Unii;
- zakazy dotyczące określonych praktyk w zakresie sztucznej inteligencji;
- szczególne wymogi dotyczące systemów sztucznej inteligencji wysokiego ryzyka oraz obowiązki spoczywające na podmiotach będących operatorami takich systemów;
- zharmonizowane przepisy dotyczące przejrzystości w przypadku systemów sztucznej inteligencji przeznaczonych do wchodzenia w interakcję z osobami fizycznymi, systemów rozpoznawania emocji oraz systemów kategoryzacji biometrycznej, a także systemów sztucznej inteligencji wykorzystywanych do generowania obrazów, treści dźwiękowych lub treści wideo lub do manipulowania nimi;
- przepisy dotyczące monitorowania po wprowadzeniu do obrotu i nadzoru rynku.

Artificial Intelligence Act

DEFINICJA SZTUCZNEJ INTELIGENCJI

SYSTEM SZTUCZNEJ INTELIGANCJI

„System sztucznej inteligencji” oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.

TECHNIKI I PODEJŚCIA AI

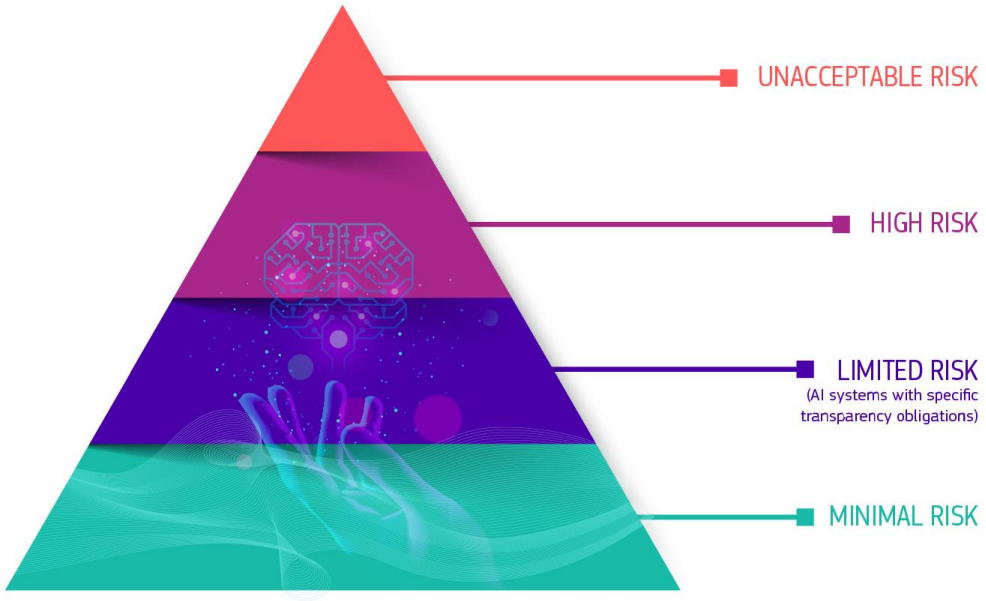
- mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego;
- metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki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

Artificial Intelligence Act

KLASYFIKACJA SYSTEMÓW AI

KLASYFIKACJA OPATA NA RYZYKU

- **Niedopuszczalne ryzyko** – systemy sztucznej inteligencji, które ze względu na ich sprzeczność z wartościami Unii, na przykład ze względu na fakt, że naruszają one prawa podstawowe, zostały zakazane.
- **Wysokie ryzyko** - systemy sztucznej inteligencji, które niosą za sobą znaczne ryzyko, dla bezpieczeństwa, a tym samym powinny podlegać ścisłym regulacjom i wymogom.
- **Ograniczone ryzyko** - systemy sztucznej inteligencji, które to nie wiążą się ze znaczącym ryzykiem takie jak np. chatboty. Systemy te powinny jednak podlegać pewnym, minimalnym obowiązkom w zakresie przejrzystości, tak by użytkownicy tych systemów mieli świadomość wchodzenia w interakcję ze sztuczną inteligencją.
- **Minimalne ryzyko** - pozostałe systemy sztucznej inteligencji takie jak np. gry komputerowe oparte na AI, których to wykorzystywanie wiąże się z minimalnym lub zerowym ryzykiem dla bezpieczeństwa. Systemy te nie podlegają przepisom i wymogom rozporządzenia.



Źródło: https://ec.europa.eu

Artificial Intelligence Act

NIEDOPUSZCZALNE RYZYKO

ZAKAZANE PRAKTYKI AI

- praktyki, które wykazują znaczny potencjał manipulowania ludźmi, oparte na technikach podprogowych działających na ich podświadomość lub wykorzystujące słabości określonych słabszych grup,
- praktyki pozwalające organom publicznym stosowanie systemów punktowej oceny społecznej,
- praktyki wykorzystujące zdalną identyfikację biometryczną w czasie rzeczywistym w przestrzeni publicznej do celów egzekwowania prawa (chyba że mają zastosowanie niektóre ograniczone wyjątki).

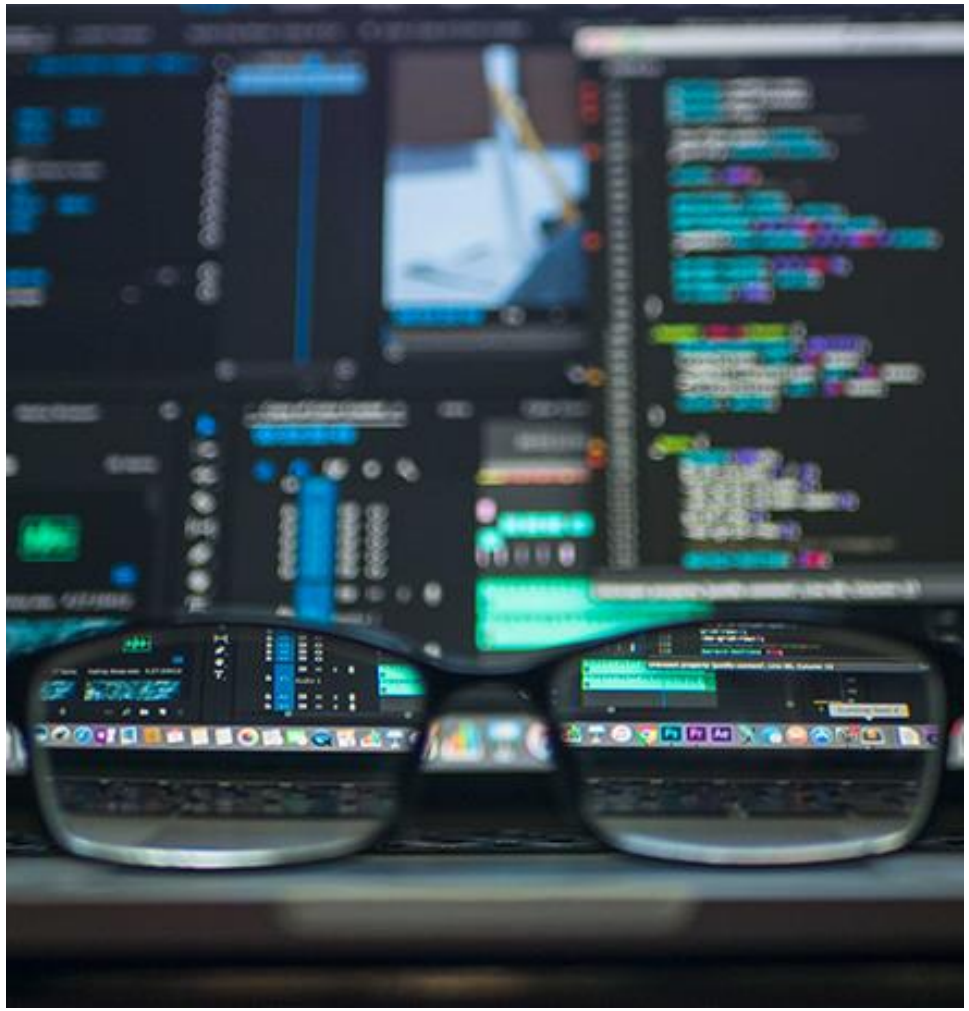
Artificial Intelligence Act

AI WYSOKIEGO RYZYKA

DEFINICJA AI WYSOKIEGO RYZYKA

Systemy AI wysokiego ryzyka obejmują swym zakresem technologię sztucznej inteligencji wykorzystywaną w:

- elementach bezpieczeństwa produktu,
- systemie kształcenia i szkolenia zawodowego (dostęp do szkolnictwa, ocena egzaminów)
- zarządzaniu infrastrukturą krytyczną i jej eksploatacją,
- identyfikacji i kategoryzacji biometrycznej osób fizycznych,
- zatrudnianiu, zarządzaniu pracownikami i dostępie do samozatrudnienia,
- zakresie dostępu do podstawowych usług prywatnych oraz usług i świadczeń publicznych, a także w zakresie korzystania z nich (np. w zakresie oceny zdolności kredytowej),
- celu ściganiu przestępstw i egzekwowania prawa,
- celu zarządzaniu migracją, azylem i kontrolą graniczną,
- sprawowaniu wymiaru sprawiedliwości i procesach demokratycznych.

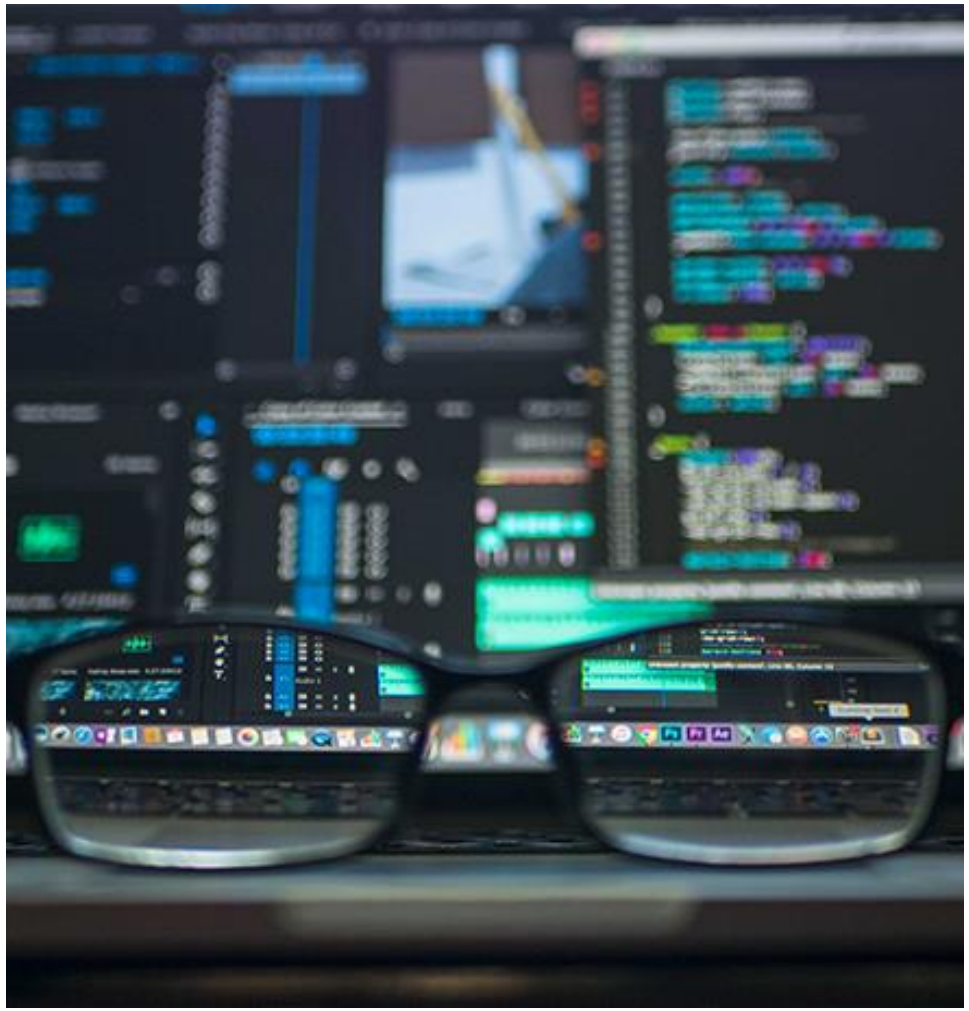


Artificial Intelligence Act

AI WYSOKIEGO RYZYKA

WYMOGI DLA AI WYSOKIEGO RYZYKA

- obowiązek posiadania odpowiedniego systemu oceny i ograniczania ryzyka;
- obowiązek wykorzystywania wysokiej jakości zbiorów danych do zasilania algorytmu sztucznej inteligencji, mający na celu zminimalizowanie ryzyka dyskryminującego działania algorytmu;
- ewidencjonowanie działania sztucznej inteligencji mające na celu umożliwienie oceny wyników pracy algorytmu i identyfikowalności wyników, w tym obowiązek sporządzania logów;
- obowiązek sporządzenia i aktualizowania dokumentacji zawierającej wszelkie informacji co do systemu sztucznej inteligencji i celu w jakim to system ten funkcjonuje, co ma pozwolić na ocenę zgodności systemu sztucznej inteligencji z wymogami przez odpowiednie organy;
- zapewnienie należytych środków nadzoru człowieka nad algorytmem sztucznej inteligencji;
- obowiązek przekazywania użytkownikom odpowiednio jasnych informacji o systemie sztucznej inteligencji;
- obowiązek zapewnienia wysokiego poziomu solidności, bezpieczeństwa i dokładności algorytmu sztucznej inteligencji.



Artificial Intelligence Act

SYSTEM KAR

KARY ZA NIEPRZESTRZEGANIE ROZPORZĄDZENIA

- Do **30 000 000 EUR** lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do **6 %** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa za:
  - nieprzestrzeganie zakazu praktyk w zakresie sztucznej inteligencji oraz za
  - niezgodność systemu sztucznej inteligencji z wymogami z zakresu jakości danych wykorzystywanych przez sztuczna inteligencję;
- do **20 000 000 EUR** lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do **4 %** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa w przypadku naruszenia pozostałych wymogów rozporządzenia;
- do **10 000 000 EUR** lub – jeżeli naruszenia dopuszcza się przedsiębiorstwo – w wysokości do **2 %** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa za przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji jednostkom notyfikowanym i właściwym organ krajowym w odpowiedzi na ich wezwanie.

PRZYSZŁOŚĆ REGULACJI AI

Artificial
Intelligence Act

Artificial Intelligence Act

NADCHODĄCE WYZWANIA I WĄTPLIWOŚCI

DEFINCIJE

- Czy definicja sztucznej inteligencji nie jest zbyt szeroka?
- Czy definicja sztucznej inteligencji nie obejmuje swym zakresem również i rozwiązań pseudo inteligentnych?
- Czy zastosowana definicja sztucznej inteligencji wysokiego ryzyka jest precyzyjna i czy faktycznie obejmuje swym zakresem wszelkie rozwiązania AI które to mogą nieść wysokie ryzyko dla bezpieczeństwa?
- Czy zastosowane definicje są neutralne technologicznie?

KONTROLA NAD AI

- Czy w praktyce wraz z rozwojem technologii AI, zapewnienie zrozumiałości algorytmu może stać się wyzwaniem?
- Czy wobec rosnącego stopnia skomplikowania algorytmów i zastosowania technologii uczenia maszynowego, kontrola i nadzór nad algorytmem ze strony człowieka może być w przyszłości utrudniony?

KONKURENCYJNOŚĆ

- Czy ustanowienie dodatkowych wymogów w zakresie AI nie wpłynie natywnie na konkurencyjność podmiotów działających na terenie Unii Europejskiej?

JAKOŚĆ DANYCH

- Jak duży jest wpływ jakości danych na efekty pracy algorytmu opartego na rozwiązaniach sztucznej inteligencji?
- Czy zapewnienie wysokiej jakości danych jakimi to zasilana jest sztuczna inteligencja stanowi wyzwanie?

KONIECZNY WIERZBICKI

KANCELARIA RADCÓW PRAWNYCH

NASZA STRONA