

ZAJĘCIA 4

Sztuczna inteligencja a prawo

Ramy prawne, prawa autorskie
i odpowiedzialność w kontekście bibliotek

⌚ 90 min | Wszystkie osoby pracujące w bibliotekach

Krajobraz prawny

Wdrażanie AI w bibliotekach rodzi pilne pytania prawne w czterech powiązanych ze sobą obszarach:

© Prawa autorskie

Kto posiada prawa do treści wygenerowanych przez AI? Jakie ryzyka wiążą się z danymi treningowymi i tworzeniem treści wspieranym przez AI?

🛡️ Ochrona danych

W jaki sposób RODO ma zastosowanie, gdy AI przetwarza dane użytkowników bibliotek, zapytania lub profile użytkowników?

⚖️ Europejski AI Act

Pierwsze na świecie kompleksowe prawo regulujące sztuczną inteligencję, określające poziomy ryzyka, obowiązki podmiotów wdrażających AI oraz zasady egzekwowania przepisów.

📋 Odpowiedzialność

Co dzieje się, gdy AI popełnia błędy?
Kto ponosi odpowiedzialność?
Biblioteka czy dostawca systemu?

Prawa autorskie a sztuczna inteligencja

DANE TRENINGOWE

Modele AI są trenowane na ogromnych zbiorach danych, które często zawierają materiały objęte prawem autorskim. Trzy kluczowe pytania dla bibliotek:

1

Czy twórcy systemów AI potrzebują zgody na wykorzystywanie treści objętych prawem autorskim do trenowania modeli?

2

Czy trenowanie AI na materiałach chronionych prawem autorskim może być uznane za naruszenie prawa autorskiego?

3

Czym różnią się przepisy UE, USA i Wielkiej Brytanii dotyczące wyjątków dla eksploracji tekstu i danych (TDM)?

Dyrektywa UE o prawie autorskim (2019/790)

Wprowadziła wyjątek dotyczący eksploracji tekstu i danych (TDM) dla organizacji badawczych oraz instytucji dziedzictwa kulturowego. Biblioteki mogą kwalifikować się do tego wyjątku, jednak nadal trwa dyskusja, czy obejmuje on również komercyjne trenowanie modeli AI.

Prawa autorskie a sztuczna inteligencja

KTO POSIADA PRAWA DO TREŚCI GENEROWANYCH PRZEZ AI?

W większości systemów prawnych

W większości systemów prawnych ochrona prawnoautorska opiera się na ludzkiej twórczości.

Treści wygenerowane przez AI bez istotnego wkładu twórczego człowieka mogą nie podlegać ochronie.

Warunki dostawców różnią się

Regulaminy usług AI znacząco się różnią.

W zależności od dostawcy prawa do wygenerowanych treści mogą należeć do użytkownika, dostawcy lub pozostawać poza ochroną prawa autorskiego.

Znaczenie praktyczne dla bibliotek

Biblioteki powinny dokładnie analizować umowy i regulaminy dostawców AI, szczególnie wtedy, gdy wygenerowane treści mają być publikowane lub udostępniane użytkownikom (np. rekordy katalogowe, opisy zbiorów i materiały dla użytkowników).

RODO i ochrony danych osobowych

Jeżeli system AI przetwarza dane osobowe (np. zapytania użytkowników, historię wypożyczeń lub profile badawcze) zastosowanie mają przepisy RODO.

Podstawa prawna

Biblioteki muszą wskazać legalną podstawę przetwarzania danych osobowych z użyciem AI (np. uzasadniony interes, zgodę użytkownika lub realizację zadania publicznego).

Minimalizacja danych

Narzędzia AI nie powinny zbierać ani przetwarzać większej ilości danych niż jest to konieczne do określonego celu.

Zautomatyzowane decyzje

Artykuł 22 RODO ogranicza podejmowanie decyzji opartych wyłącznie na automatycznym przetwarzaniu danych, w tym profilowaniu użytkowników i systemach dostępu opartych na AI.

Obowiązek przeprowadzania DPIA

Ocena skutków dla ochrony danych (DPIA) jest wymagana w sytuacjach wysokiego ryzyka. Takim przykładem są systemy AI profilujące użytkowników.



DLACZEGO POWSTAŁ
EUROPEJSKI AI ACT?



Europejski AI Act



**Holenderski rząd Rutte podaje się do dymisji
z powodu skandalu związanego z oszustwami
przy zasiłkach na dzieci**



„Jesteś samotną matką trójki dzieci w wieku od ośmiu do jedenastu lat. Ledwo wiążesz koniec z końcem i zastanawiasz się, co dalej. Zdarzało się, że moje dzieci i ja kładliśmy się spać głodni.”

Dulce Gonçalves Tavares
usłyszała w 2013 roku, że musi zwrócić
125 tysięcy euro



W ubiegłym miesiącu premier Holandii Mark Rutte wraz z całym swoim rządem podał się do dymisji po tym, jak trwające półtora roku śledztwo wykazało, że od 2013 roku około 26 tysięcy niewinnych rodzin zostało niesłusznie oskarżonych o wyłudzenie świadczeń socjalnych, częściowo z powodu działania dyskryminującego algorytmu.

Europejski AI Act



Audyt algorytmów wykorzystywanych przez administrację publiczną wykazał, że 6 z nich nie spełniało podstawowych wymagań.

News item | 18052022 | 10:45

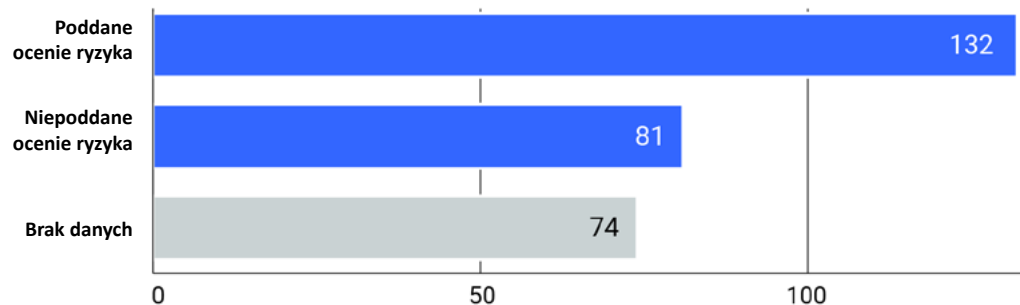
Odpowiedzialne wykorzystywanie algorytmów przez instytucje publiczne jest możliwe, ale w praktyce nie zawsze ma miejsce. Holenderski Trybunał Obrachunkowy ustalił, że tylko część analizowanych algorytmów spełniała wszystkie podstawowe wymagania. Pozostałe systemy narażały administrację publiczną na różne ryzyka, od niewystarczającej kontroli nad działaniem i wpływem algorytmów po uprzedzenia, wycieki danych i nieautoryzowany dostęp.

Europejski AI Act

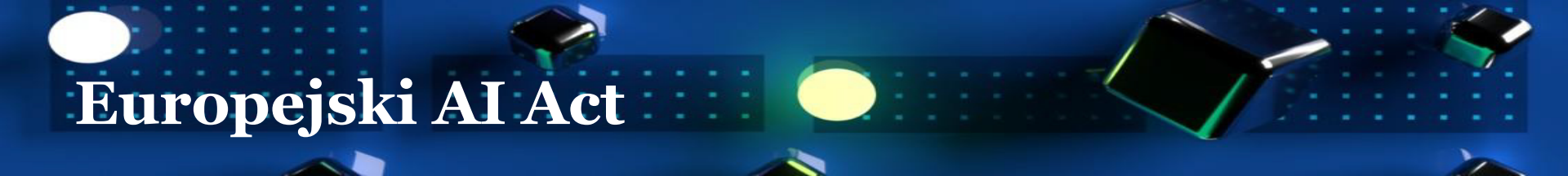


Rys. 14. Ocena ryzyka systemów AI

Nie wszystkie systemy AI przeszły ocenę ryzyka



Wykres przedstawia dane wyłącznie dotyczące 287 systemów AI, które są obecnie opracowywane lub wykorzystywane.



Europejski AI Act

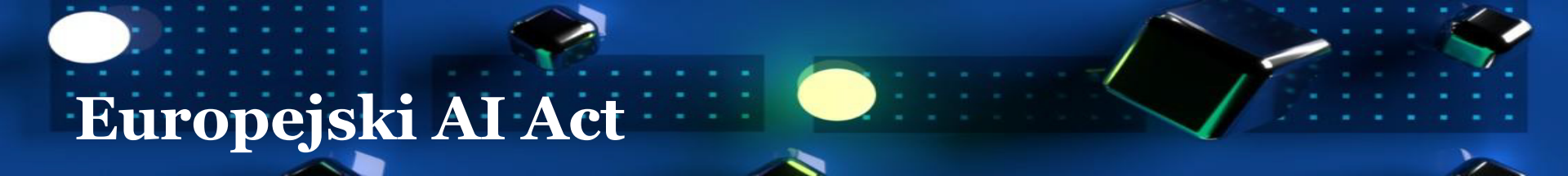
Pierwsze na świecie kompleksowe prawo regulujące sztuczną inteligencję, oparte na klasyfikacji ryzyka, obowiązujące i prawnie wiążące.

NIEDOPUSZCZALNE RYZYKO – Praktyki zakazane. Całkowicie zabronione zastosowania AI.

WYSOKIE RYZYKO – Ścisłe wymagania, obowiązkowy nadzór człowieka oraz oceny wpływu systemu.

OGRANICZONE RYZYKO – Obowiązek przejrzystości (użytkownicy muszą wiedzieć, że korzystają z AI).

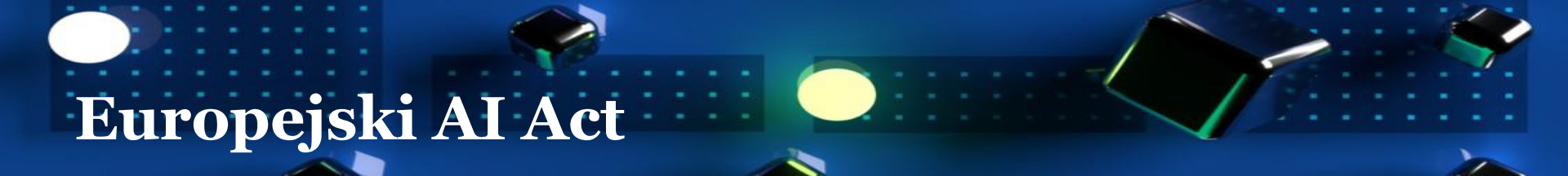
MINIMALNE RYZYKO – Brak szczególnych obowiązków prawnych, zalecane dobre praktyki.



Europejski AI Act

Niedopuszczalne ryzyko

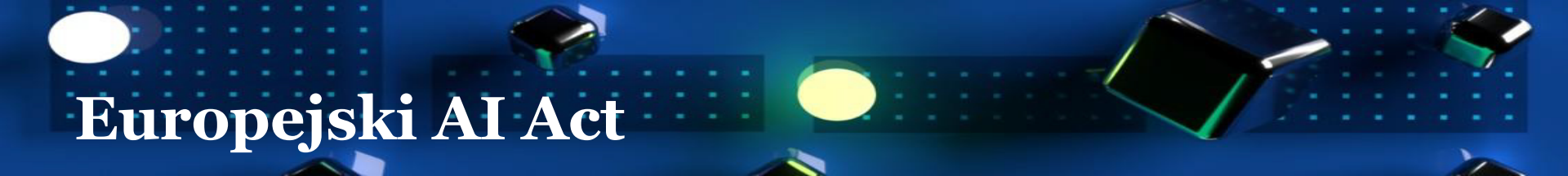
- Techniki podprogowe, manipulacyjne lub wprowadzające w błąd
- Wykorzystywanie szczególnej podatności lub słabości osób
- Systemy biometryczne analizujące wrażliwe informacje o osobach
- Systemy punktowej oceny obywateli na podstawie ich danych i zachowań
- Ocenianie ryzyka popełnienia przestępstwa przez konkretną osobę
- Tworzenie baz danych do rozpoznawania twarzy
- Rozpoznawanie emocji w miejscach pracy i instytucjach edukacyjnych
- Zdalna identyfikacja biometryczna „w czasie rzeczywistym” w przestrzeni publicznej na potrzeby organów ścigania



Europejski AI Act

Wysokie ryzyko

- Systemy biometryczne, które nie są całkowicie zakazane
- Infrastruktura krytyczna
- Edukacja i szkolenia zawodowe
- Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia
- Dostęp do podstawowych usług publicznych i prywatnych
- Organy ścigania
- Migracja, azyl i kontrola granic
- Wymiar sprawiedliwości i procesy demokratyczne

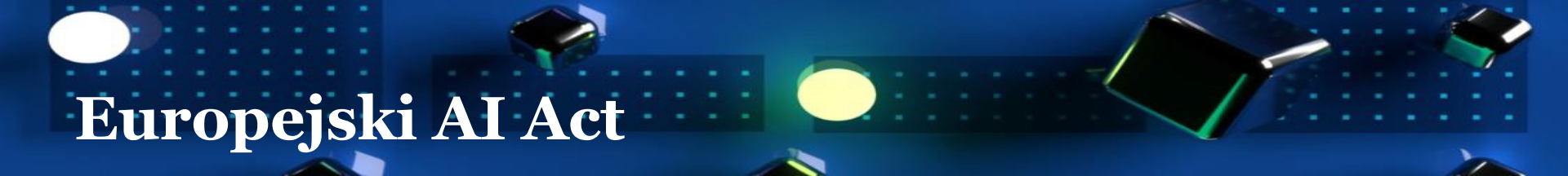


Europejski AI Act

Wysokie ryzyko

Dostawcy systemów wysokiego ryzyka muszą zapewnić m.in.:

- System zarządzania ryzykiem
- Zarządzanie danymi
- Dokumentację techniczną
- Prowadzenie rejestrów
- Instrukcję użytkowania
- Możliwość nadzoru człowieka nad systemem



Europejski AI Act

Ograniczone ryzyko

- Obowiązkowa przejrzystość działania systemu
- Przykłady: deepfake'i

Minimalne ryzyko

- Brak regulacji
- Przykłady: filtry spamu, gry komputerowe wykorzystujące AI

Europejski AI Act – przypadki użycia w bibliotekach

Do której kategorii ryzyka należą narzędzia AI wykorzystywane w bibliotekach?

Narzędzie / zastosowanie	Poziom ryzyka	Główny obowiązek
Systemy oceniające użytkowników lub monitorujące ich zachowania	 Niedopuszczalne	Zakazane – nie wdrażać
Profilowanie użytkowników i przewidywanie zachowań	 Wysokie ryzyko	Obowiązkowy nadzór człowieka i rejestrowanie incydentów
Chatbot AI odpowiadający na pytania użytkowników	 Ograniczone ryzyko	Obowiązek informowania użytkowników o wykorzystaniu AI
Narzędzia generujące treści	 Ograniczone ryzyko	Jasne oznaczanie treści wygenerowanych przez AI
AI wspierająca katalogowanie (narzędzie dla pracowników)	 Minimalne ryzyko	Brak szczególnych obowiązków, stosowanie dobrych praktyk

Europejski AI Act – obowiązki bibliotek jako podmiotów wdrażających AI

Biblioteki korzystające z narzędzi AI (nawet wyłącznie jako użytkownicy końcowi) są uznawane przez EU AI Act za „podmioty wdrażające” i mają w związku z tym określone obowiązki prawne.

SYSTEMY WYSOKIEGO RYZYKA

- Przed wdrożeniem należy przeprowadzić ocenę wpływu systemu na prawa podstawowe
- Należy prowadzić rejestry działania systemu i zapewnić stały nadzór człowieka
- Osoby objęte decyzjami wspieranymi przez AI powinny być o tym informowane

NARZĘDZIA AI OGÓLNEGO ZASTOSOWANIA (np. modele językowe takie jak ChatGPT, Claude, Gemini)

- Należy korzystać z systemu wyłącznie zgodnie z przeznaczeniem określonym przez dostawcę
- Nie należy wdrażać AI w sposób generujący ryzyka nieuwzględnione w dokumentacji
- Przed podpisaniem umowy należy poprosić dostawcę o dokumentację zgodności dla modeli GPAI

TREŚCI GENEROWANE PRZEZ AI I CHATBOTY

- Użytkownicy powinni wiedzieć, że komunikują się z systemem AI
- Treści wygenerowane przez AI powinny być jasno i konsekwentnie oznaczane
- Nie należy wykorzystywać deepfake'ów ani syntetycznych materiałów bez wyraźnego oznaczenia

Odpowiedzialność za błędy AI

Systemy AI mogą generować błędne, stronnicze lub szkodliwe treści. W kontekście bibliotek może to oznaczać m.in.:

Błędne rekordy

Niepoprawne rekordy bibliograficzne lub cytowania wygenerowane przez narzędzia AI wspierające katalogowanie.

Stronnicze wyniki

Dyskryminujące lub niesprawiedliwe rekomendacje oraz systemy dostępu oparte na AI.

Naruszenia prywatności

Treści wygenerowane przez AI mogą ujawniać informacje o rzeczywistych osobach.

Dezinformacja

Fałszywe informacje prezentowane przez chatboty i systemy odpowiadające na pytania użytkowników.

Umowy z dostawcami są pierwszą linią obrony dla bibliotek. Powinny obejmować odpowiedzialność prawną, limity odpowiedzialności, gwarancje jakości, obowiązek zgłaszania incydentów, a także możliwość odzyskania danych po zakończeniu współpracy.

Analiza prawna z perspektywy bibliotekarza

Umiejętności wykorzystywane przy ocenie źródeł informacji można bezpośrednio stosować również do oceny systemów AI.

Obszar prawny	Kluczowe pytanie
Prawa autorskie	Kto posiada prawa do wygenerowanych treści i czy model był trenowany na materiałach chronionych prawem autorskim?
Ochrona danych	Czy narzędzie przetwarza dane osobowe? Czy potrzebna jest DPIA i umowa DPA?
EU AI Act	Do jakiej kategorii ryzyka należy system? Jakie obowiązki ma biblioteka jako podmiot wdrażający?
Odpowiedzialność	Kto odpowiada za szkody lub błędy wygenerowane przez AI?
Umowa z dostawcą	Czy umowa obejmuje odpowiedzialność, zgłaszanie incydentów i możliwość odzyskania danych?

Kluczowe pojęcia związane ze sztuczną inteligencją

EU AI Act

Rozporządzenie UE 2024/1689 – pierwsze na świecie kompleksowe prawo dotyczące sztucznej inteligencji, oparte na podejściu uwzględniającym poziom ryzyka systemów AI oraz obowiązki podmiotów je wdrażających.

GPAI Model

Model AI ogólnego zastosowania (General-Purpose AI Model), np. GPT lub Claude, wykorzystywany jako podstawa różnych produktów i usług. Takie modele podlegają określonym obowiązkom dotyczącym przejrzystości.

EU AI Act

Wyjątek w prawie autorskim umożliwiający automatyczną analizę treści i danych. Przepisy dotyczące TDM różnią się między UE, USA i Wielką Brytanią.

Podmiot wdrażający

Organizacja (np. biblioteka), która wykorzystuje system AI w swojej działalności, ale nie jest jego twórcą ani dostawcą.

Podmiot wdrażający

Ocena skutków dla ochrony danych (Data Protection Impact Assessment) – proces wymagany przez RODO przed wdrożeniem systemów AI mogących stwarzać wysokie ryzyko dla praw i wolności osób.

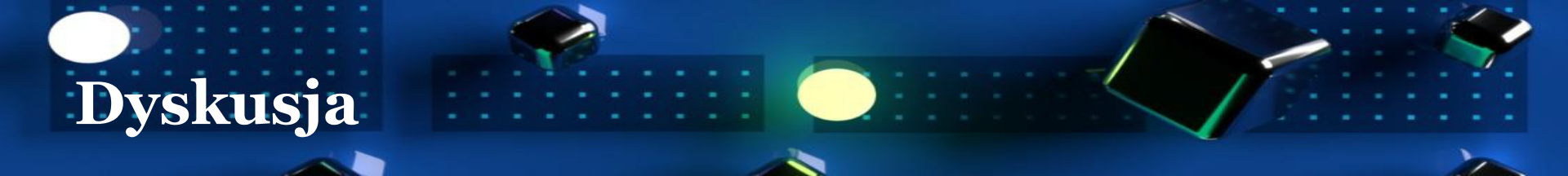
Podmiot wdrażający

Klauzula umowna, w której jedna strona zobowiązuje się pokryć odpowiedzialność prawną lub straty finansowe poniesione przez drugą stronę.

Ćwiczenie – analiza zgodności

- Przypadek 1: Biblioteka korzysta z chatbota AI rekomendującego książki. System przypadkowo zapisuje historię rozmów użytkowników wraz z ich preferencjami.
- Przypadek 2: Proponowane jest wykorzystanie rozpoznawania twarzy do celów bezpieczeństwa. Czy EU AI Act na to pozwala? Jakie zabezpieczenia byłyby konieczne?
- Przypadek 3: Student generuje esej przy użyciu ChatGPT. Szkoła prosi bibliotekę o udostępnienie historii wyszukiwania studenta.

W grupach przeanalizujcie przypadek dotyczący AI, prywatności danych i zgodności z prawem, aby określić najlepszy sposób działania zgodny z RODO oraz EU AI Act.



Dyskusja

P1 Czy Wasza instytucja posiada politykę zakupu i wdrażania narzędzi AI?
Kto analizuje zgodność umów z dostawcami pod względem prawnym?

P2 Czy korzystaliście z AI do tworzenia treści, takich jak rekordy, opisy czy podsumowania?
Kto posiada prawa do tych treści?

P3 Jak wyjaśnilibyście klasyfikację ryzyka w EU AI Act osobie, która nigdy wcześniej o niej nie słyszała?

P4 Jaki problem prawny związany z AI wydaje się dziś najważniejszy w Waszej bibliotece?