

AI w sporcie – wyzwania prawne

Aleksandra Maciejewicz

Pomysł na dzisiejszą prezentację:

- Zebrać rozproszone elementy wykorzystania AI w sporcie w jednym miejscu
- Dać związkom sportowym „helicopter view” kluczowych wyzwań prawnych
- Pokazać, że znajomość choćby zarysu problemów jest konieczna, aby móc je później skutecznie adresować w swojej organizacji
- Ułatwić pokazanie innym uczestnikom branży, jak praktycznie podchodzić do AI i prawa w sporcie

How AI Is Revolutionizing Professional Sports

By [Kathleen Walch](#), Contributor. © Kathleen...

Follow Author

Published Aug 16, 2024, 08:25am EDT

Share Save Comment



AI is being adopted in all areas of sports to enhance the game and fan experiences alike.

GETTY

- **Analiza ruchu** zawodników przez kamery AI, np. system Hawk-Eye w tenisie i krykiecie do śledzenia trajektorii piłki i oceny decyzji sędziowskich.
- **Monitorowanie obciążeń treningowych** przez sensory GPS i akcelerometry w kamizelkach Catapult Vector, aby optymalizować intensywność wysiłku piłkarzy czy rugbystów.
- **Predykcja ryzyka kontuzji** poprzez algorytmy analizujące zmiany w danych o dystansach, sprintach i regeneracji, co pozwala trenerom modyfikować plan obciążeń.
- Tworzenie **spersonalizowanych planów treningowych** dzięki AI analizującej szybkość, technikę biegu i wytrzymałość sportowca.
- **Wsparcie sędziowania** – np. system Fujitsu Judging Support System w gimnastyce analizuje ruchy w 3D i generuje oceny zgodne z kryteriami trudności i wykonania.
- Generowanie **spersonalizowanych powtórek i highlightów dla kibiców** podczas igrzysk olimpijskich w Paryżu 2024, dopasowanych do preferencji odbiorców.
- **Wirtualna rzeczywistość** wspierana przez AI (np. Rezzil, BeYourBest) pozwala piłkarzom trenować rzuty karne i decyzje w symulowanych warunkach meczowych.



PRO

PRO

W ramach działalności związku sportowego dzieją się:

- procesy kadrowe (rekrutacja pracowników, analiza wyników pracy)
- współpraca z podwykonawcami (agencje, freelancerzy, firmy IT)
- zamówienia usług i narzędzi (strony internetowe, analiza danych, materiały promocyjne)
- realizacja szkoleń, grantów, materiałów edukacyjnych,

- a w ramach każdego tych obszarów może wykorzystywać sztuczną inteligencję – zarówno w tle, jak i wprost jako narzędzie wykonawcze

Rewolucja w sporcie. Jak AI wspiera sportowców, trenerów i sędziów?

Sztuczna inteligencja coraz śmielej wkracza w świat sportu, zmieniając sposób treningu, analizowania rozgrywek i zarządzania drużynami. Pozwala tworzyć spersonalizowane programy treningowe i wspomaga sędziów sportowych.

Publikacja: 12.01.2025 05:11



Akty prawne dotyczące AI:

AI Act (a za jakiś czas ustawa)

RODO

Ustawa o prawie autorskim / inne dotyczące własności intelektualnej

Kodeks cywilny

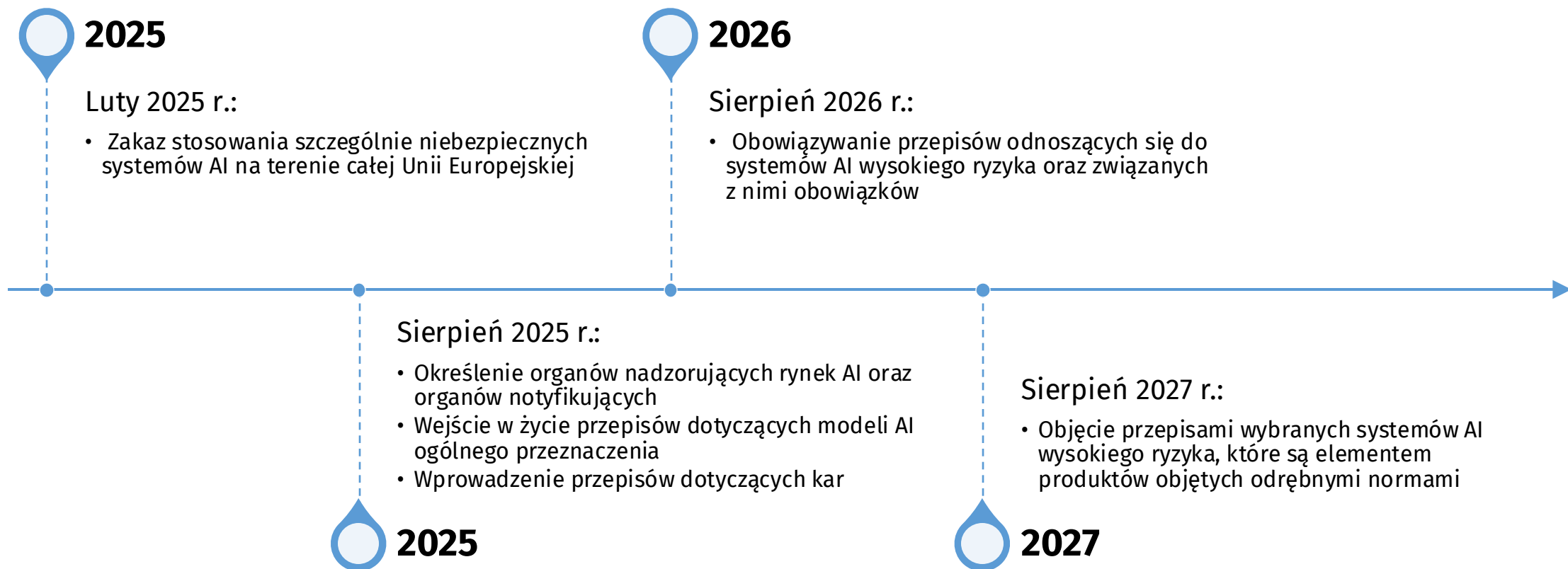
Ustawa o zwalczaniu nieuczciwej konkurencji

Kodeks pracy

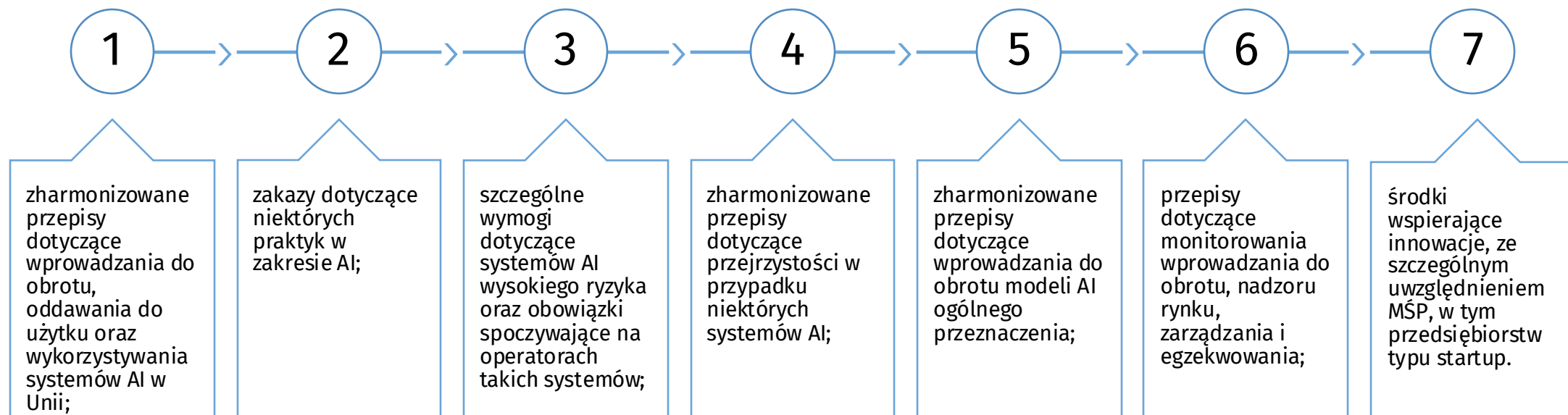
Ustawa o świadczeniu usług drogą elektroniczną

i inne.

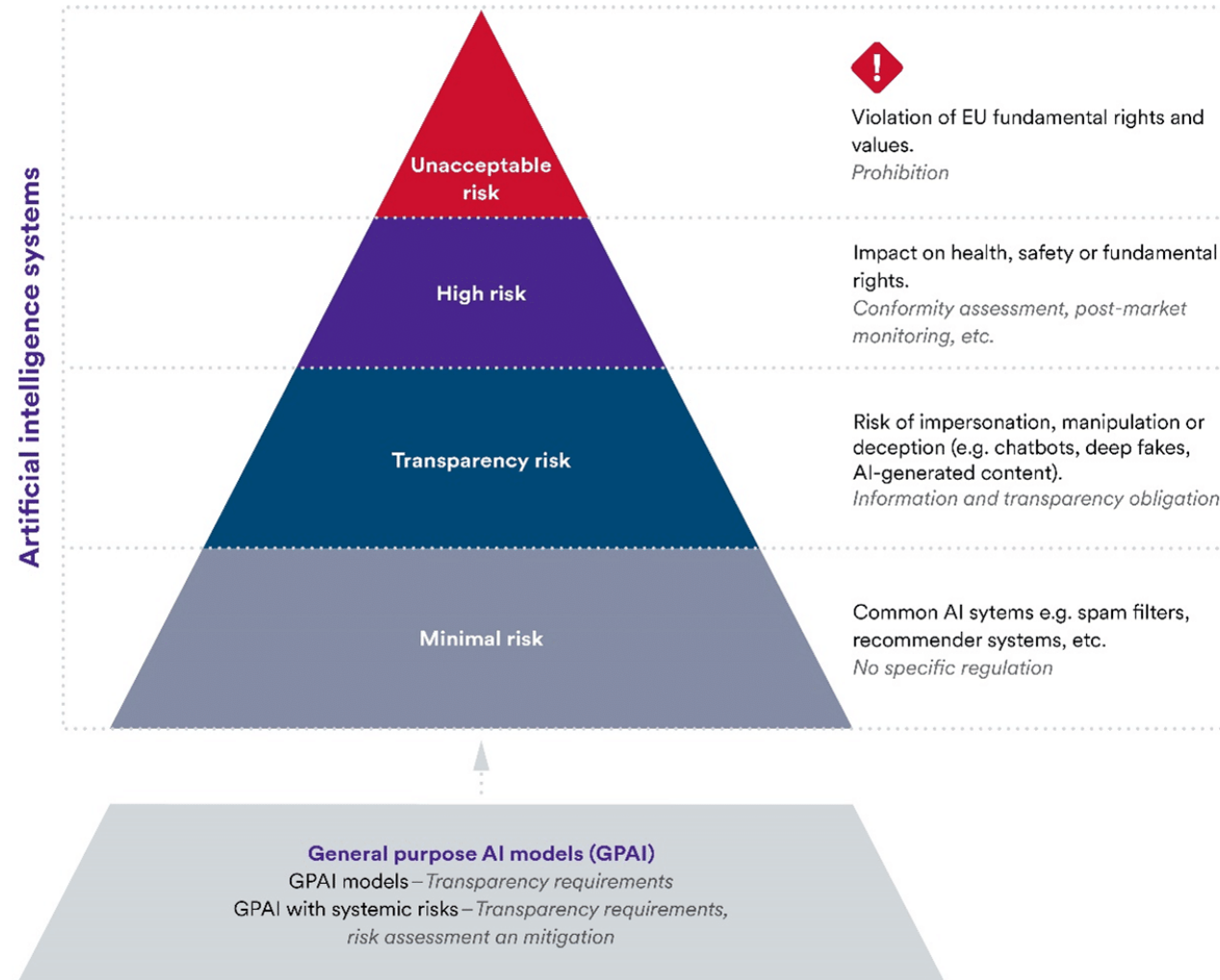
AI Act – harmonogram:



AI Act ustanawia:



EU AI-Act: Risk-based Approach



Zakazane praktyki w zakresie AI: czego nie wolno

W skrócie:

- AI + celowe techniki manipulacyjne lub wprowadzające w błąd o określonym skutku.
- AI wykorzystuje słabości osoby fizycznej lub określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną - z określonym skutkiem.
- Scoring społeczny prowadzący do nieuzasadnionego/nieproporcjonalnego krzywdzącego traktowania lub poza pierwotnym kontekstem pozyskania danych.
- Biometryczna kategoryzacja wrażliwych danych (pochodzenie, orientacja itd.).
- Zdalna biometryczna identyfikacja w czasie rzeczywistym w przestrzeni publicznej – z wyjątkami.

Zakazane praktyki: ale uwaga na uproszczenia

Rozpoznawanie emocji

Na przykład:

- spostrzeżenie, że dana osoba jest uśmiechnięta, nie stanowi rozpoznawania emocji;
- określenie, czy dana osoba jest chora, nie stanowi rozpoznawania emocji.

Zakresem zakazu nie są objęte:

- systemy AI wnioskuje emocje i nastroje na podstawie danych innych niż biometryczne,
- systemy AI wnioskuje stany fizyczne, takie jak ból i zmęczenie.

Np. korzystanie przez centrum telefoniczne z systemów rozpoznawania głosu do śledzenia emocji klientów (np. gniew, zniecierpliwienie – w celu pomocy pracownikom w radzeniu sobie ze zdenerwowanymi klientami) nie jest zakazane na mocy art. 5 ust. 1 lit. f) aktu w sprawie sztucznej inteligencji.

Manipulowanie

Perswazja – polega na przedstawianiu argumentów lub informacji w sposób, który odwołuje się do rozumu i emocji, ale wyjaśnia cele i funkcjonowanie systemu AI, dostarcza istotnych i dokładnych informacji z myślą o zapewnieniu świadomego podejmowania decyzji oraz wspiera zdolność jednostki do oceny informacji i dokonywania wolnych i autonomicznych wyborów.

Na przykład system AI wykorzystujący spersonalizowane zalecenia oparte na przejrzystych algorytmach oraz preferencjach i kontroli użytkowników wykorzystuje perswazję.

Scoring społeczny

Ukierunkowana reklama handlowa wspomagana AI nie wchodzi w zakres stosowania, jeżeli opiera się na odpowiednich danych (np. preferencjach użytkowników), odbywa się zgodnie z prawem UE dot. ochrony konsumentów, ochrony danych i usług cyfrowych oraz nie prowadzi do szkodliwego lub nieproporcjonalnego traktowania (np. wyzysk, nieuczciwe różnicowanie cen).

Systemy AI wysokiego ryzyka

- **Biometria** (w zakresie dozwolonym przez prawo UE lub krajowe):
 - systemy zdalnej identyfikacji biometrycznej,
 - systemy kategoryzacji biometrycznej według wrażliwych lub chronionych atrybutów (np. rasa, płeć, niepełnosprawność),
 - systemy rozpoznawania emocji (poza wyjątkami medycznymi i bezpieczeństwa).
- **Infrastruktura krytyczna** :
 - systemy AI stosowane jako elementy bezpieczeństwa w zarządzaniu krytyczną infrastrukturą cyfrową, ruchem drogowym, dostawach wody, gazu, ciepła, energii elektrycznej.
- **Kształcenie i szkolenie zawodowe** :
 - systemy decydujące o dostępie/przyjęciu do szkół i programów edukacyjnych,
 - systemy oceny wyników nauki lub przydzielania do ścieżek edukacyjnych,
 - systemy monitorowania i wykrywania niedozwolonych zachowań podczas egzaminów.
- **Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia** :
 - systemy wspierające rekrutację, selekcję kandydatów, ocenę, awanse, rozwiązanie umowy,
 - systemy do spersonalizowanego przydzielania zadań i monitorowania pracowników.
- **Dostęp do usług prywatnych i publicznych** :
 - systemy używane do ustalania prawa do świadczeń i usług publicznych,
 - systemy scoringu kredytowego i oceny zdolności kredytowej osób fizycznych,
 - systemy oceny ryzyka i ustalania cen ubezpieczeń zdrowotnych i na życie,
 - systemy oceny i klasyfikowania zgłoszeń alarmowych oraz priorytetyzacji wysyłania służb ratunkowych.

Z życia wzięte:

Czy zastosowanie AI w procesie wysokiego ryzyka, takim jak preselekcja CV, pozostaje objęte kategorią wysokiego ryzyka, jeśli decyzje podejmowane są również przez człowieka, a wyniki AI nie są ostateczne?

- [...] Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia;
- systemy AI przeznaczone do wykorzystywania **do celów rekrutacji** lub wyboru osób fizycznych, w szczególności do celów umieszczania ukierunkowanych ogłoszeń o pracę, analizowania i **filtrowania podań o pracę** oraz do oceny kandydatów;
- systemy AI przeznaczone do wykorzystywania do celów **podejmowania decyzji wpływających na warunki stosunków pracy**, decyzji o awansie lub rozwiązaniu umownego stosunku pracy, przydzielania zadań w oparciu o indywidualne zachowanie lub cechy osobowości lub charakter lub do monitorowania lub oceny wydajności i zachowania osób pozostających w takich stosunkach. [...]

Co bym sprawdziła, czy nie jest system AI wysokiego ryzyka:

Obszar działalności	Potencjalne zastosowanie AI	Przepis Aktu AI
Selekcja zawodników, trenerów, pracowników administracyjnych	Automatyczne systemy rekrutacji, oceny, awansów, przydzielania zadań, monitorowania wyników	Załącznik III pkt 4 – „Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia”
Bezpieczeństwo podczas zawodów i imprez sportowych	Monitoring z użyciem rozpoznawania twarzy, identyfikacji biometrycznej lub rozpoznawania emocji uczestników	Załącznik III pkt 1 – „Biometria”
Postępowania dyscyplinarne wobec zawodników i sędziów	AI analizująca dane o zachowaniach, naruszeniach, incydentach; systemy wspierające ocenę wiarygodności dowodów	Załącznik III pkt 4 lit. b i c – „Zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia”
Opieka medyczna nad zawodnikami	Systemy AI zintegrowane z wyrobami medycznymi (np. urządzenia do monitorowania parametrów zdrowotnych sportowców, diagnostyka kontuzji)	Art. 6 ust. 1 – systemy AI jak element związany z bezpieczeństwem lub samym wyrobem medycznym, a wyrób podlega ocenie zgodności przez jednostkę notyfikowaną.

AI Act ma zastosowanie do:

“ZE WZGLĘDU NA SWÓJ CYFROWY CHARAKTER NIEKTÓRE SYSTEMY AI POWINNY ZOSTAĆ OBJĘTE ZAKRESEM STOSOWANIA NINIEJSZEGO ROZPORZĄDZENIA, **NAWET JEŚLI NIE** ZOSTAŁY WPROWADZANE DO OBROTU, ODDANE DO UŻYTKU ANI SĄ WYKORZYSTYWANE W UNII.”

- dostawców wprowadzających do obrotu lub oddających do użytku systemy AI lub wprowadzających do obrotu modele AI ogólnego przeznaczenia w Unii, niezależnie od tego, czy dostawcy ci mają siedzibę lub znajdują się w Unii czy w państwie trzecim;
- podmiotów stosujących systemy AI, które to podmioty mają siedzibę lub znajdują się w Unii;
- dostawców systemów AI i podmiotów stosujących systemy AI, którzy mają siedzibę lub znajdują się w państwie trzecim, w przypadku gdy wyniki wytworzone przez system AI są wykorzystywane w Unii;
- importerów i dystrybutorów systemów AI;
- producentów produktu, którzy pod własną nazwą lub znakiem towarowym oraz wraz ze swoim produktem wprowadzają do obrotu lub oddają do użytku system AI;
- upoważnionych przedstawicieli dostawców niemających siedziby w Unii;
- osób, na które AI ma wpływ i które znajdują się w Unii.

Podmiot stosujący

- Podmiotem stosującym może być:
 - Osoba fizyczna
 - Osoba prawna
 - Rodzaje osób prawnych: organ publiczny, agencja, inny podmiot
- Warunki wykorzystania systemu AI przez podmiot stosujący:
 - Kontrola nad systemem AI
 - Podmiot stosujący musi sprawować kontrolę nad systemem AI
- Wyjątek:
 - Wykorzystywanie systemu AI w ramach osobistej działalności pozazawodowej
 - Nie kwalifikuje się jako podmiot stosujący.

Pytania pomocnicze:

1. Czy rozwijasz system AI lub model AI ogólnego przeznaczenia?

- Jeśli tak, możesz być dostawcą systemu AI. Dostawca jest odpowiedzialny za rozwój systemu AI lub zlecenie jego rozwoju, a następnie wprowadzanie go na rynek pod własną nazwą lub znakiem towarowym.

2. Czy wykorzystujesz system AI, nad którym sprawujesz kontrolę, w swojej działalności?

- Jeśli tak, możesz być podmiotem stosującym. Podmiot stosujący to osoba lub organizacja, która używa systemu AI w swojej działalności zawodowej (nie w celach osobistych).

3. Czy masz siedzibę w Unii Europejskiej i działasz na podstawie pełnomocnictwa dostawcy systemu AI, aby spełniać jego obowiązki?

- Jeśli tak, możesz być upoważnionym przedstawicielem. Upoważniony przedstawiciel działa w imieniu dostawcy, który może znajdować się poza UE, aby spełniać wymogi regulacyjne w UE.

4. Czy masz siedzibę w UE i wprowadzasz do obrotu system AI pochodzący od dostawcy mającego siedzibę w państwie trzecim (poza UE)?

- Jeśli tak, możesz być importerem. Importer wprowadza na rynek unijny system AI opracowany przez dostawcę spoza UE.

5. Czy udostępniasz system AI na rynku UE, ale nie jesteś dostawcą, importerem ani upoważnionym przedstawicielem?

- Jeśli tak, możesz być dystrybutorem. Dystrybutor udostępnia system AI na rynku, ale nie bierze udziału w jego produkcji, rozwoju ani imporcie.

* Czy pełnisz jakąkolwiek z powyższych ról?

- Jeśli tak, jesteś operatorem. Operator to ogólna kategoria, która obejmuje dostawców, podmioty stosujące, upoważnionych przedstawicieli, importerów i dystrybutorów.

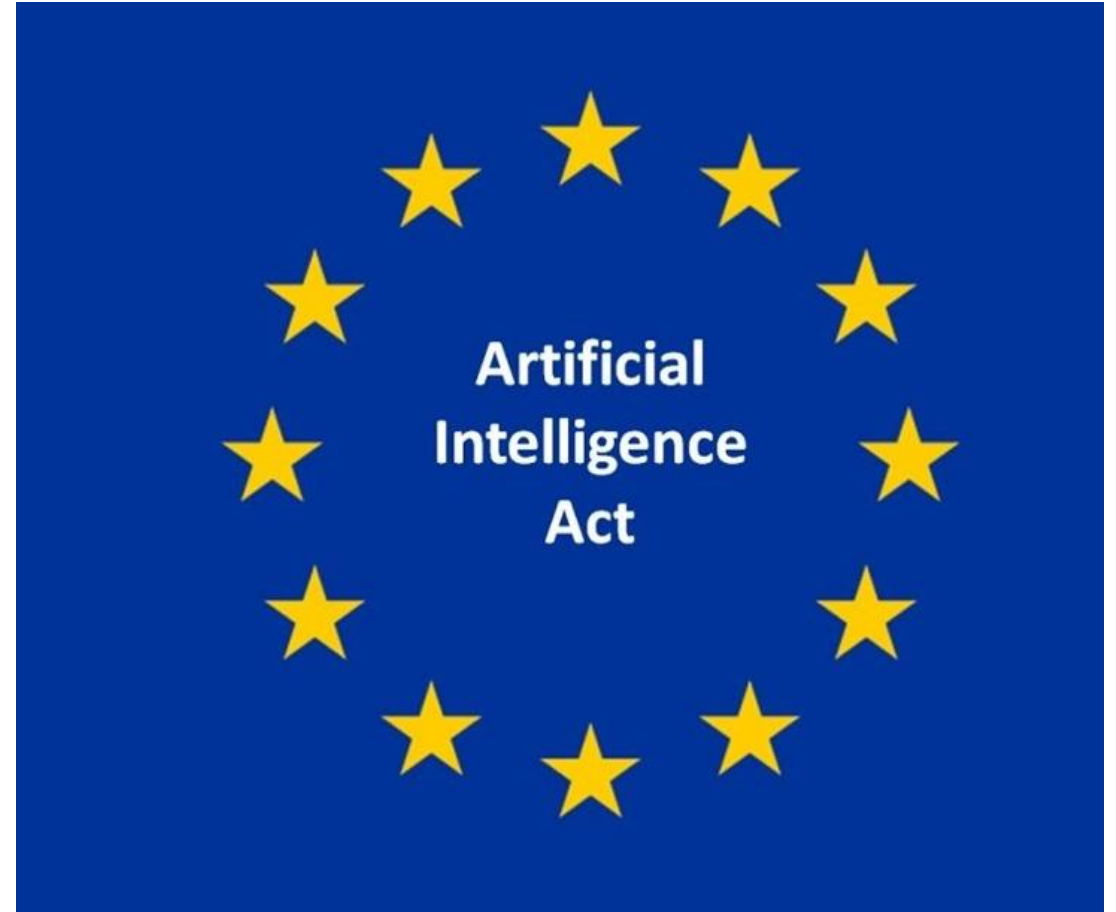
Podmioty stosujące systemy AI wysokiego ryzyka

Są zobowiązane między innymi do (art. 26 AI Act):

- zapewnienie zgodności z instrukcją obsługi;
- nadzór człowieka sprawowany przez przeszkolone osoby;
- odpowiedzialność za jakość danych wejściowych;
- monitoring działania systemu i zgłaszanie incydentów;
- obowiązek przechowywania logów przez min. 6 miesięcy;
- obowiązek informowania pracowników o wdrożeniu systemu w miejscu pracy;
- rejestracja systemu w bazie UE (dla podmiotów publicznych);
- wykorzystanie informacji od dostawcy do celów RODO (DPIA);
- obowiązek uzyskania zgody sądu na użycie AI do identyfikacji biometrycznej post factum;
- obowiązek informowania osób fizycznych o użyciu systemu, jeśli decyzja ich dotyczy;
- współpraca z organami nadzorczymi.

Dostawcy systemów sztucznej inteligencji wysokiego ryzyka:

- ustanawiają, wdrażają, dokumentuje i utrzymuje system zarządzania ryzykiem w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka;
- sporządzają dokumentację techniczną systemu sztucznej inteligencji wysokiego ryzyka;
- przechowują rejestry zdarzeń generowane automatycznie przez ich systemy sztucznej inteligencji wysokiego ryzyka, jeżeli znajdują się one pod ich kontrolą;
- zapewniają, aby system sztucznej inteligencji wysokiego ryzyka poddano odpowiedniej procedurze oceny zgodności przed wprowadzeniem go do obrotu lub oddaniem go do użytku;
- wypełniają obowiązki rejestracyjne;
- podejmują niezbędne działania naprawcze, jeżeli system sztucznej inteligencji wysokiego ryzyka nie spełnia wymogów;
- informują właściwe organy krajowe państw członkowskich, w których udostępnił lub oddał do użytku system sztucznej inteligencji, oraz, w stosownych przypadkach, jednostkę notyfikowaną o niezgodności z wymogami i o wszelkich podjętych działaniach naprawczych;
- wykazują, na żądanie właściwego organu krajowego, zgodność systemu sztucznej inteligencji wysokiego ryzyka z wymogami ustanowionymi w rozdziale 2 niniejszego tytułu.



Pan R. pyta: Założmy, że dostawca oferuje narzędzie mające jako jedną z opcji użycie AI i ja chcę takie narzędzie uruchomić w organizacji ...

Zagadnienie:

Po czyjej stronie jest odpowiedzialność za spełnienie AI ACT - dostawcy rozwiązania czy użytkownika końcowego?

Jeśli tak, to jako użytkownik takiego rozwiązania (ogólnodostępnego z półki) - jakie ciążą na mnie jako kliencie obowiązki prawne?

Czy istnieją jakieś certyfikaty, którymi dostawca rozwiązania może się okazać co do zgodności z EU AI ACT po których można uznać, że klient (i/lub dostawca) jest w pełni zgodny z prawem?

Jeśli nie - to czy istnieje jakaś checklista, po której pozytywnym przejściu z dostawcą mogę uznać, że jesteśmy zgodni z AI ACT

Jakie ma znaczenie to o czym czatujemy z AI (specyfikacje projektów/produktów, specyficzne dane)

Możliwe wyjaśnienie z AI Act:

Po stronie obu.

Zależy z jakiego aktu prawnego.

Tak, certyfikaty wydane przez jednostki notyfikowane, deklaracja zgodności UE.

Bez 100-procentowej gwarancji, ale np. wytyczne CNIL (lipiec 2025).

W kontekście AI Act - najczęściej w połączeniu z przeznaczeniem.

Niektóre “ryzyka” transparentności:

Kategoria systemu AI	Obowiązek informacyjny	Podmiot odpowiedzialny
Systemy do interakcji z ludźmi (np. chatboty , awatary)	Należy poinformować osobę fizyczną, że wchodzi w interakcję z systemem AI, chyba że jest to w sposób oczywisty widoczne z kontekstu.	Dostawca i podmiot stosujący
Systemy rozpoznawania emocji lub kategoryzacji biometrycznej	Należy poinformować osoby fizyczne, które są narażone na działanie systemu, o jego funkcjonowaniu.	Podmiot stosujący
"Deepfake" – treści wideo, audio i obrazy	Należy ujawnić, że treść została sztucznie wygenerowana lub przetworzona. Wyjątki (np. dzieła artystyczne, satyra) nie zwalniają z obowiązku, choć oznaczenie może być dyskretne.	Podmiot stosujący
Generowanie lub manipulacja tekstem	W przypadku publikacji tekstu o znaczeniu publicznym, należy oznaczyć go jako sztucznie wygenerowany. Obowiązek nie ma zastosowania, jeśli treść podlegała ludzkiej weryfikacji i kontroli redakcyjnej.	Podmiot stosujący
System AI wysokiego ryzyka w miejscu pracy	Informuje się przedstawicieli pracowników i pracowników, których to dotyczy, że będzie w stosunku do nich wykorzystywany system AI wysokiego ryzyka.	Podmiot stosujący (będący pracodawcą)

Z życia wzięte:

Czy jeśli - przykładowo - wprowadzimy do organizacji **narzędzie do wypełniania umów**, które uczy się na dotychczas wykonywanych zadaniach (np. proponuje nam wysokość kary umownej, mając na względzie wcześniej sporządzane umowy - tak jak choćby czyni to autokorekta), to czy mamy już do czynienia z systemem AI?

→ Nawet jeżeli zgodnie z definicją legalną z AI Act to jest system sztucznej inteligencji*, to po prostu nie musimy się przejmować tym rozporządzeniem.

*"system AI" oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem **autonomii** po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który - na potrzeby wyraźnych lub dorozumianych celów - **wnioskuje**, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne

WŁASNOŚĆ INTELEKTUALNA – W AI I SPORCIE

Case studies własność intelektualna: AI w sporcie

01

Przykład 1: AI generujące taktyczne schematy gry na podstawie analizy setek meczów – kto jest właścicielem praw do tak opracowanej strategii? Klub, trener czy dostawca systemu?

02

Przykład 2: AI projektujące nowe stroje sportowe z uwzględnieniem ergonomii i trendów – czy prawa autorskie do wzoru należą do projektanta, klubu, czy producenta algorytmu?

03

Przykład 3: AI tworzące cyfrowe awatary zawodników do gier i transmisji VR – kto posiada prawa do wizerunku i generowanych treści? Sam zawodnik, organizacja czy firma technologiczna?

WŁASNOŚĆ INTELEKTUALNA

```
graph TD; A[WŁASNOŚĆ INTELEKTUALNA] --> B[PRAWO AUTORSKIE]; A --> C[BAZY DANYCH]; A --> D[WŁASNOŚĆ PRZEMYSŁOWA]; A --> E[KNOW HOW];
```

PRAWO AUTORSKIE

utwory
przedmioty praw
pokrewnych

*wizerunek

BAZY DANYCH

WŁASNOŚĆ PRZEMYSŁOWA

znaki towarowe
wynałazki
wzory użytkowe
wzory przemysłowe

KNOW HOW

poufne informacje
techniczne,
technologiczne,
organizacyjne,
gospodarcze

Działalność związku a ryzyko praw autorskich

- **Pytanie 1**

AI generujące materiały promujące związek (np. kampanie rekrutacyjne, storytelling o danej dziedzinie sportu)

– czy to związek jest „autorem”, czy AI?

- **Pytanie 2**

Własność treści w systemach e-learningowych trenerów i sędziów

– kto posiada prawa do treści szkoleniowych tworzonych przez AI?

- **Pytanie 3**

Możliwe naruszenie praw autorskich w raporcie

– jaką mamy gwarancję, że w outpucie nie pojawi się plagiat?

- **Pytanie 4**

Kto ponosi odpowiedzialność za potencjalne naruszenia praw autorskich?

– związek, indywidualny pracownik, dostawca AI, a może nikt?

- **Pytanie 5**

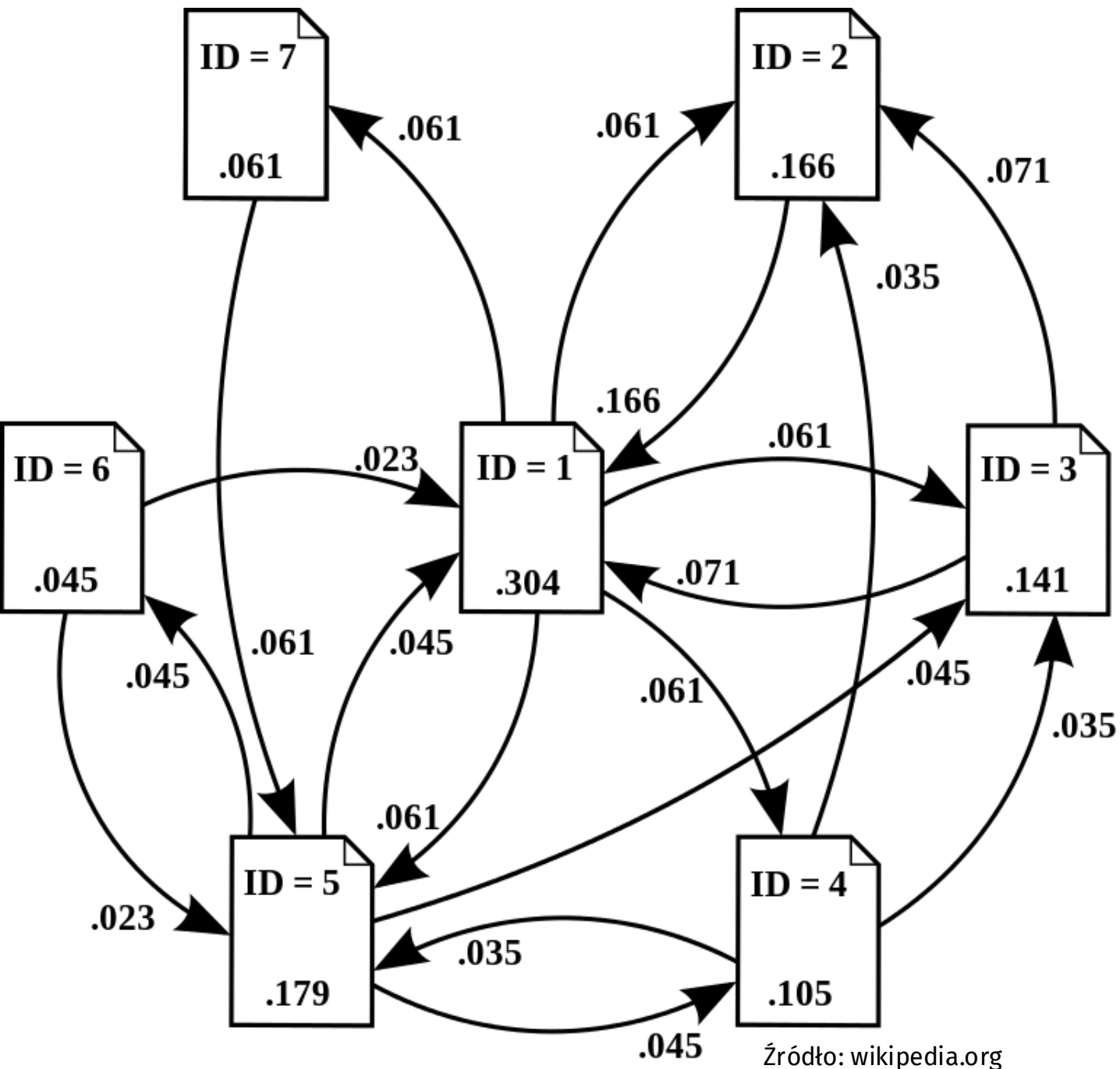
Dalsza dystrybucja

– czy treści wygenerowane przez AI mogą być sprzedawane lub licencjonowane?

Ochroną objęty może być wyłącznie
sposób wyrażenia;

→ **nie są objęte ochroną** odkrycia,
idee, procedury, metody i zasady
działania oraz koncepcje
matematyczne

(art. 1 ust. 2 [1] ustawy o prawie autorskim i prawach pokrewnych)



ALGORYTMY

LAW MORE

Sport ball motion monitoring methods and systems - US12023564B2

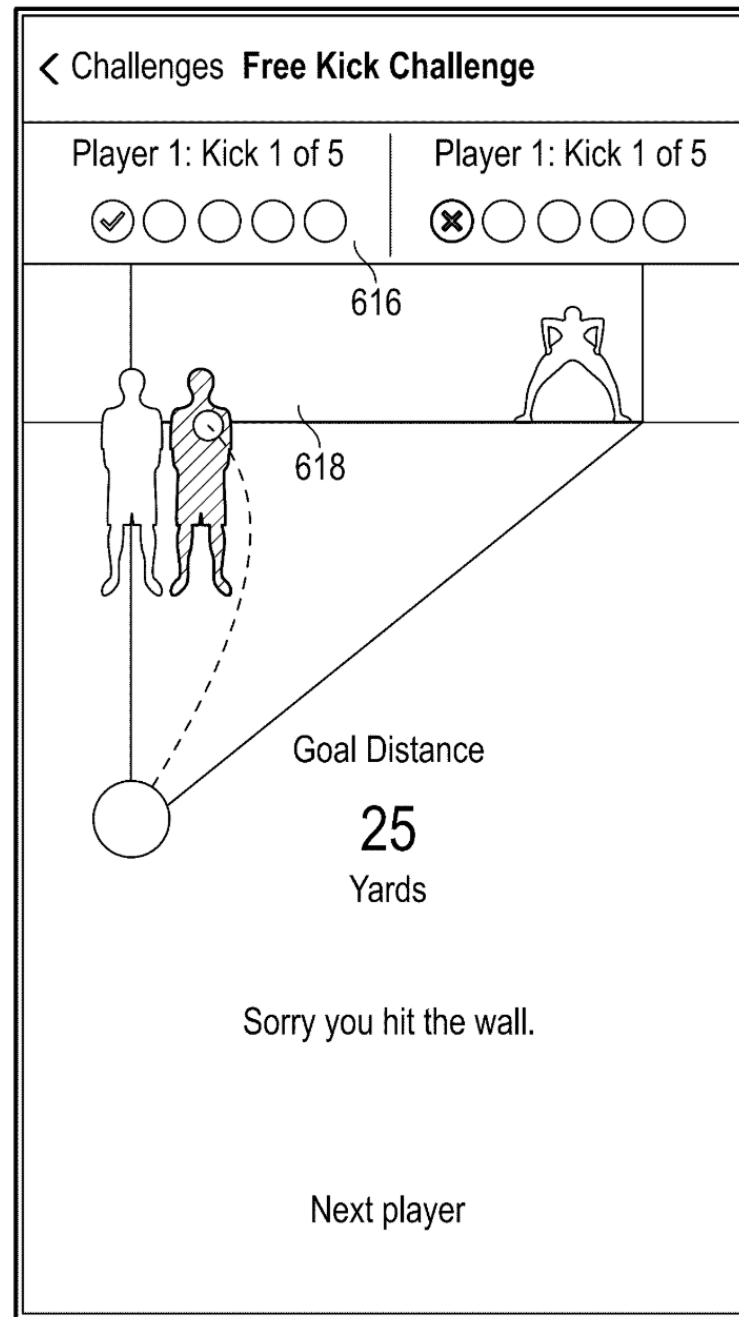


FIG. 42

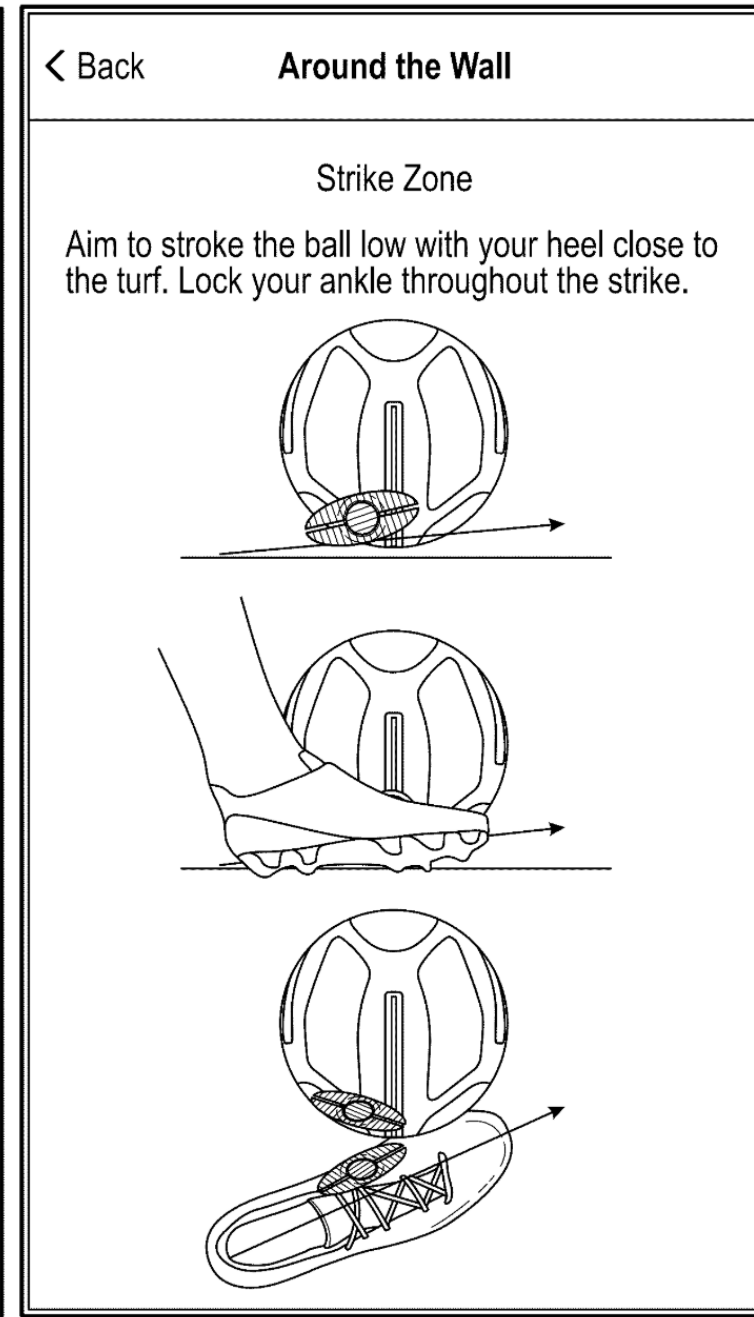


FIG. 35



LUDZIE I PROMPTY

- AI nie może być uznane za autora – prawo autorskie chroni wyłącznie utwory stworzone przez ludzi.
- Prompty to polecenia lub pomysły na obiekt (tekst lub obraz), a prawo autorskie chroni wyłącznie wyrażenie idei, nie samą ideę.
- Zaawansowany, szczegółowy prompt (dokładne parametry dotyczące stylu, kolorów, nastroju) → Potencjalnie może być chroniony, ale tylko jako utwór literacki, a nie finalny obraz.
- Problem „czarnej skrzynki” AI – nawet przy tym samym promptcie AI może generować różne wyniki, co podważa argument o pełnej kontroli twórczej użytkownika.



Jako sztuczna inteligencja, nie posiadam praw autorskich ani żadnych innych praw. Prawa autorskie są przyznawane twórcom lub autorom, którzy są ludźmi. Sztuczna inteligencja, tak jak ja, jest narzędziem, które wykonuje zadania na podstawie algorytmów i danych, ale nie ma zdolności do tworzenia praw autorskich.



Jeśli chodzi o prawa autorskie do treści wytworzonych przez sztuczną inteligencję, zazwyczaj przypisuje się je osobie lub podmiotowi, który ją uruchomił lub kontroluje. Na przykład, jeśli sztuczna inteligencja została stworzona przez programistę lub firmę, to zazwyczaj to oni posiadają prawa autorskie do wytworzonej przez nią treści.

Tak więc:

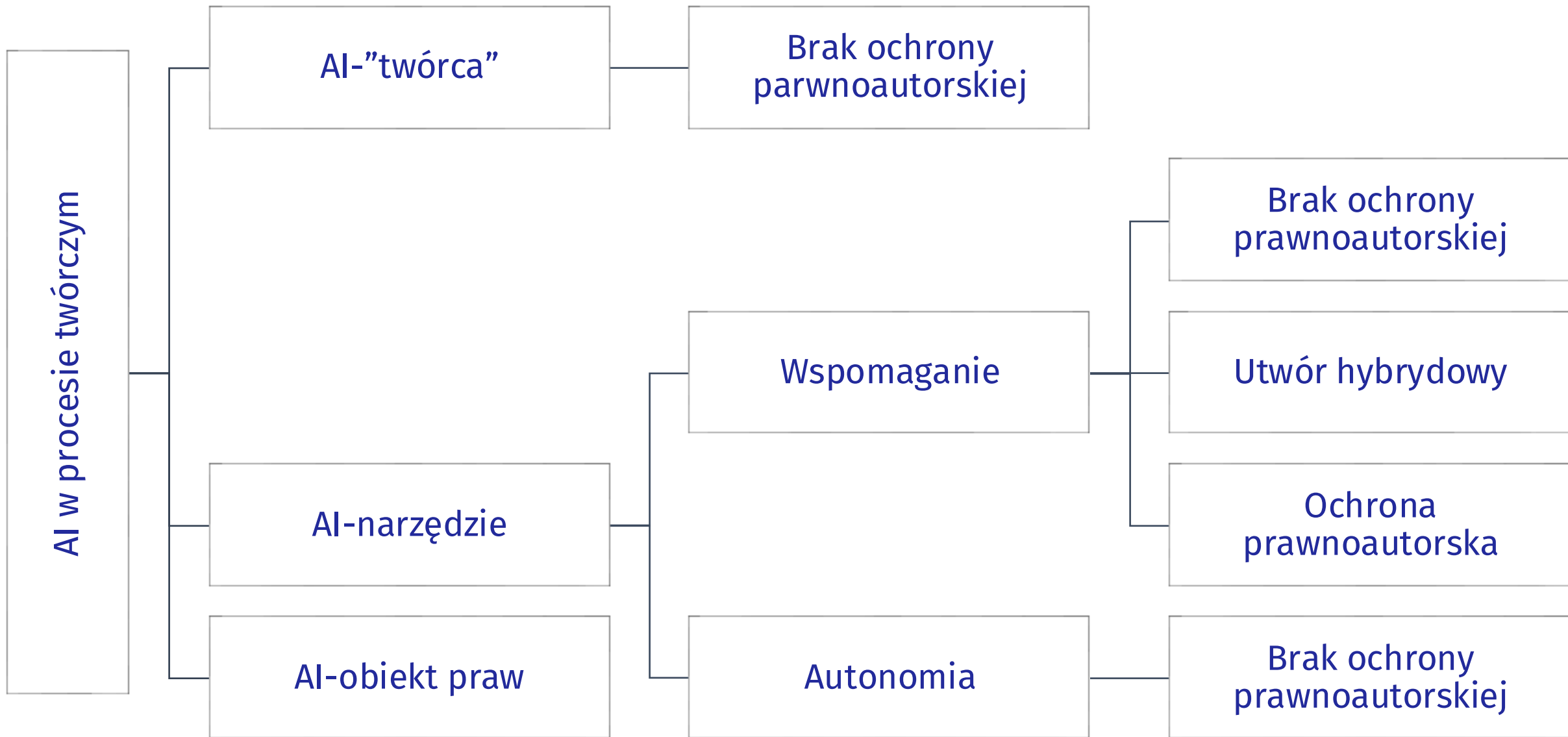
- czy prawa autorskie należą do maszyny, która stworzyła dzieło,
- czy prawa autorskie należą do twórcy algorytmu (programisty),
- czy prawa autorskie należą do użytkownika programu,
- a może jest to utwór współautorski lub niemający autora?

Ile utworu w utworze?

wygenerowanie dzieła całkowicie przez AI,
zainicjowane przez prompt

oś prawnautorska

człowiek tworzy utwór, wprowadzając do
procesu twórczego drobne elementy
automatyzmu AI



Różne poziomy wkładu człowieka a własność prawnoautorska

AI jako techniczna część większego dzieła stworzonego przez człowieka → pełna ochrona praw autorskich (np. AI generuje analizę, ale trener redaguje, strukturyzuje i uzupełnia treść).

- **Samo wpisanie prostego promptu → brak praw autorskich**
(np. „Stwórz profesjonalny plan ćwiczeń tygodniowych zawodnika”).
- **Zaawansowane inżynierowanie promptów → potencjalna ochrona, ale bardzo niepewna**
(np. iteracyjna modyfikacja wyników AI).
- **Twórcza selekcja i edycja wyników AI → możliwa ochrona prawna**
(np. ręczna poprawa, dodanie oryginalnych treści).

Checklista: Bezpieczne korzystanie z AI w kontekście prawa autorskiego

Rozumienie prawa autorskiego:

- ☒ Znam podstawowe zasady praw autorskich dotyczące AI.
- ☒ Podpisuję odpowiednie umowy ze swoimi podwykonawcami.

Licencjonowanie i uprawnienia:

- ☒ Korzystam tylko z narzędzi AI, które posiadają jasne licencje na użycie danych.
- ☒ Upewniam się, że umowy licencyjne obejmują odpowiednie prawa do użytku, modyfikacji i dystrybucji.

Weryfikacja źródła danych:

- ☒ Używam danych do treningu AI, które są wolne od praw autorskich lub do których posiadam prawa.
- ☒ Unikam wykorzystywania danych chronionych bez odpowiedniej zgody.

Dokumentacja i atrybucja:

- ☒ Dokładnie dokumentuję proces twórczy i użyte narzędzi AI.
- ☒ Przypisuję autorstwo tam, gdzie jest to wymagane.

Czy mam zatem jakieś
możliwości ochrony?

Art. 13 USTAWY O ZWALCZNIU NIEUCZCIWEJ KONKURENCJI

Czynem nieuczciwej konkurencji jest **naśladowanie gotowego produktu**, polegające na tym, że za pomocą technicznych środków reprodukcji jest kopiowana zewnętrzna postać produktu, jeżeli może wprowadzić klientów w błąd co do tożsamości producenta lub produktu.

Art. 3 WW. USTAWY

Przypadkiem konkurencji pasożytniczej jest również sięganie do cudzego miejsca rynkowego w celu wykorzystania go do budowy własnej pozycji bądź dla jej polepszenia. Służy temu np. **nawiązanie do** cudzego znaku towarowego, firmy, **konceptji**, reklamy, wyglądu czy kolorystyki produktu, który cieszy się znajomością i uznaniem nabywców (por. IACa1744/14, VCSK311/06).

Art. 23 KODEKSU CYWILNEGO

Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, **twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska**, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

Ochrona baz danych tworzonych przez AI – reżim ustawy o ochronie baz danych

- Ustawa o ochronie baz danych przewiduje *prawo sui generis* dla producenta bazy, niezależnie od ochrony autorskiej
- Baza danych: uporządkowany zbiór elementów, dostępnych indywidualnie, wymagający istotnego nakładu inwestycyjnego w stworzenie, weryfikację lub prezentację
- Prawo *sui generis* chroni inwestycję, a nie twórczość – w przeciwieństwie do prawa autorskiego, które wymaga „oryginalności” i „twórczego układu” danych
- W przypadku baz danych generowanych przez AI brak wkładu twórczego człowieka wyklucza ochronę prawnoautorską, ale *nie wyklucza* ochrony *sui generis*, jeśli udokumentowany jest istotny nakład inwestycyjny w ich stworzenie, weryfikację czy prezentację
- Zakres prawa *sui generis*: wyłączne prawo do pobierania i wtórnego wykorzystania całości lub istotnej części bazy

Case study – wyrok TSUE w sprawie Football Dataco vs. Sportradar (C-173/11)

- Przedmiot sporu: baza „Football Live” – dane o przebiegu meczów piłkarskich (wyniki, kartki, zmiany). Producent (Football Dataco) poniósł znaczny nakład inwestycyjny
- Pozwani (Sportradar) kopiowali i rozpowszechniali dane w internecie, udostępniając je klientom bukmacherskim
- TSUE:
 - „Wtórne wykorzystanie” obejmuje każde publiczne udostępnienie całości lub części chronionej bazy, niezależnie od formy (również transmisja online)
 - Przesyłanie danych z serwera w jednym państwie do użytkowników w innym państwie jest również „wtórnym wykorzystaniem” i może naruszać prawo *sui generis* na terytorium państwa odbiorcy
- Wnioski dla AI w sporcie:
 - Bazy danych sportowych tworzone i weryfikowane z pomocą AI mogą korzystać z ochrony *sui generis*.
 - Wtórne wykorzystanie (np. agregacja i redystrybucja wyników przez zewnętrzne podmioty) bez zgody producenta narusza prawo.
 - Brak ochrony autorskiej nie oznacza braku ochrony – decyduje nakład inwestycyjny.

PATENTY

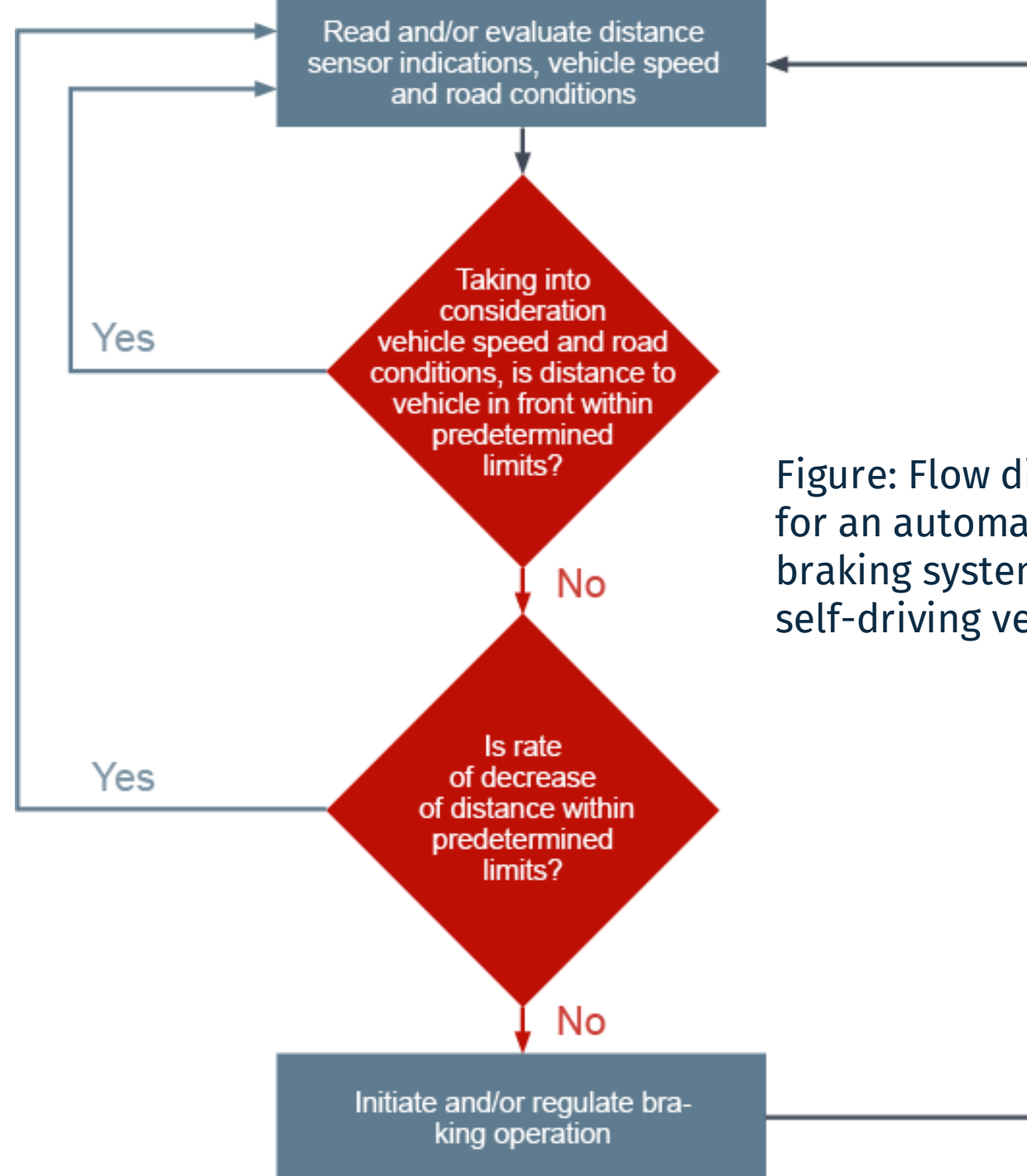
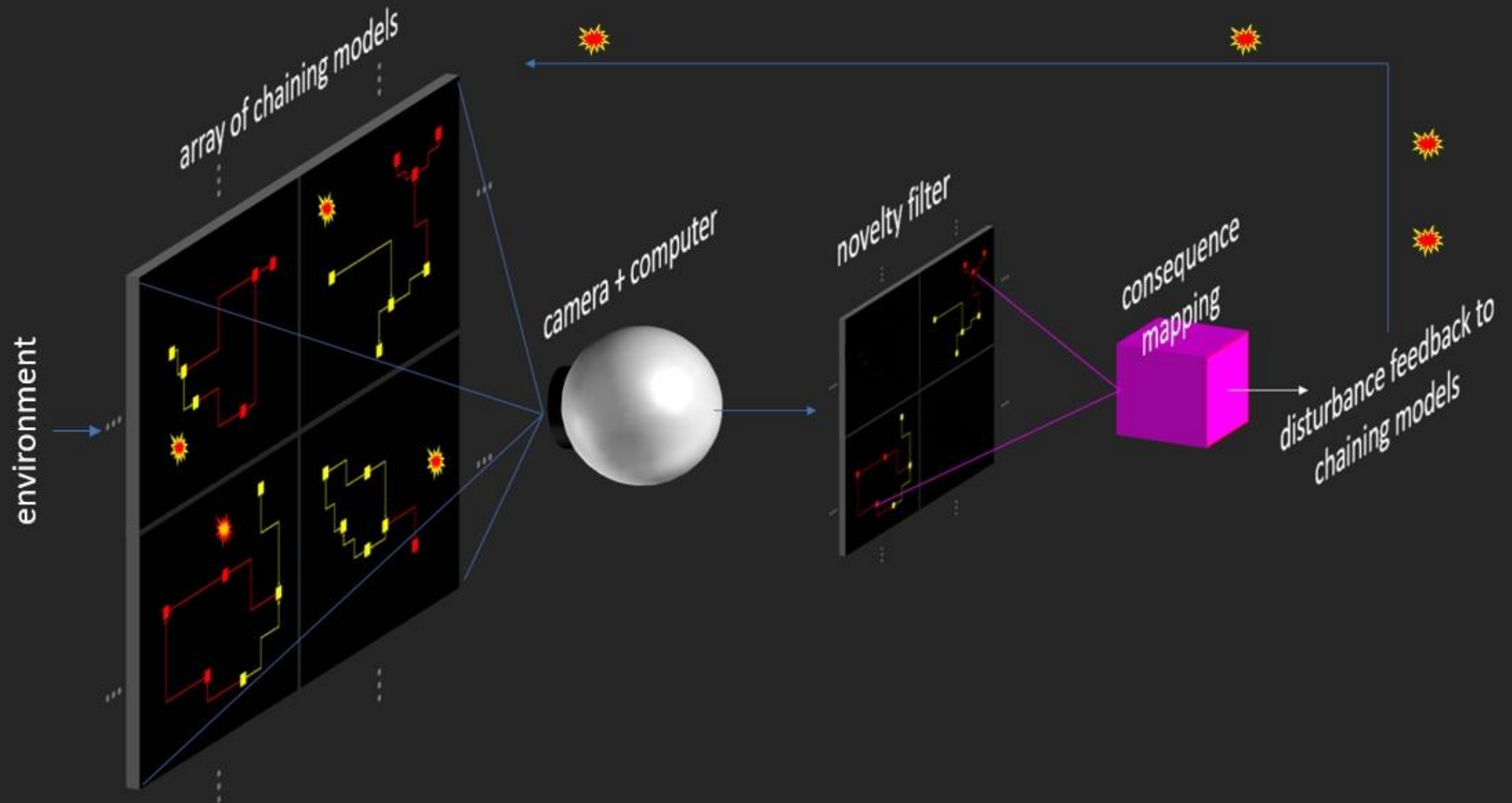


Figure: Flow diagram for an automatic braking system in a self-driving vehicle.

DABUS: EMBODIMENT 1



Własność

- As between the Company and you, the Company does not claim any ownership in Your Content / **Perplexity**
- As between you and **OpenAI**, and to the extent permitted by applicable law, you (a) retain your ownership rights in Input and (b) own the Output. We hereby assign to you all our right, title, and interest, if any, in and to Output.
- As between you and **Anthropic**, and to the extent permitted by applicable law, you retain any right, title, and interest that you have in such Inputs. Subject to your compliance with our Terms, we assign to you all our right, title, and interest (if any) in Outputs.

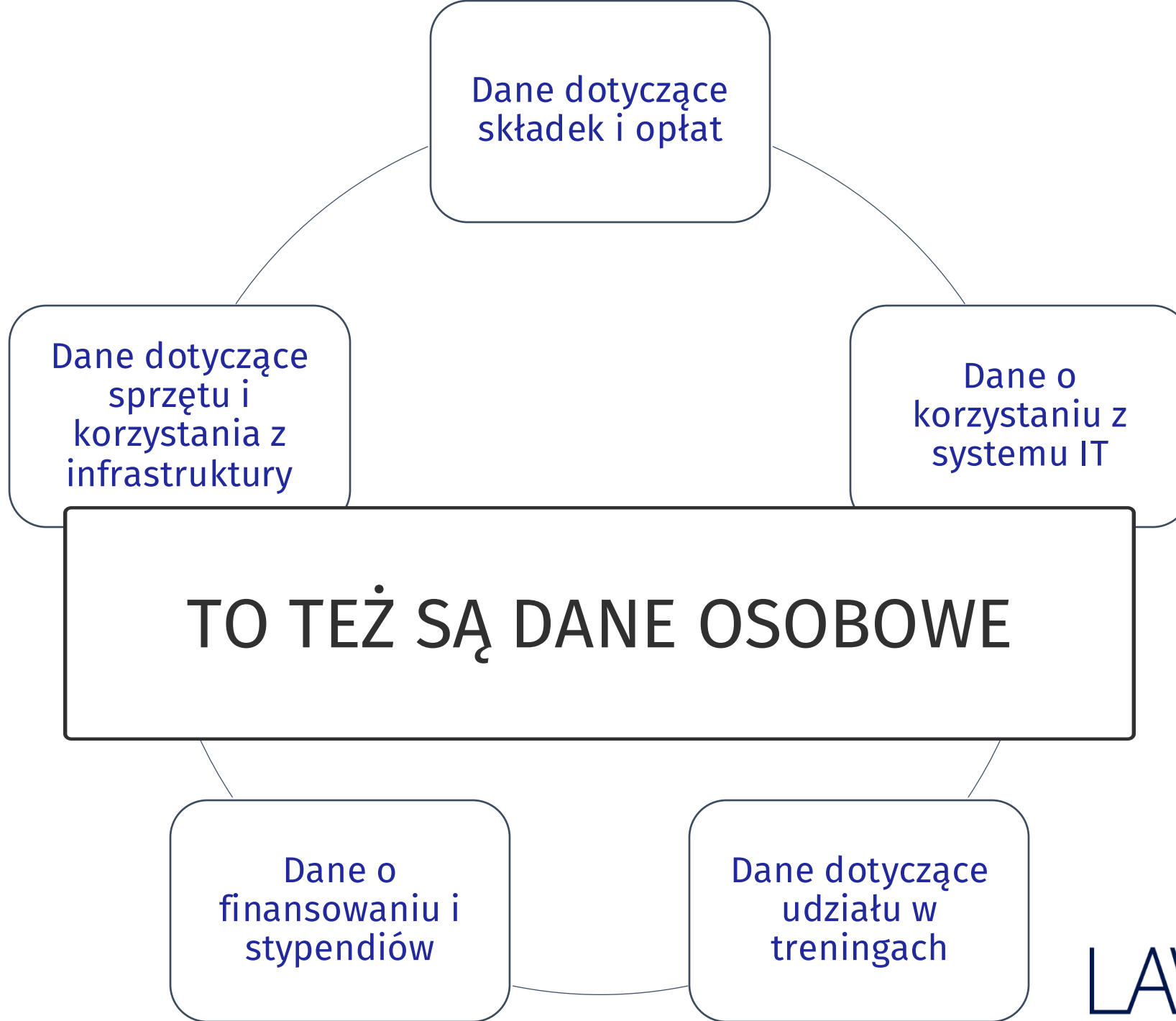
RODO I POUFNOŠĆ

Case studies o danych osobowych i poufności: AI w sporcie

Przykład 1: AI analizujące wyniki testów wydolnościowych, psychometrycznych i stanu zdrowia – kto ma dostęp do danych?

Przykład 2: Związek sportowy wykorzystuje AI do profilowania młodych zawodników na podstawie danych z testów fizycznych i wyników treningowych?

Przykład 3: AI uczące się na materiałach szkoleniowych i planach treningowych klubów - czy to utrata poufności?



✓ Dane osobowe

- oznaczają **wszelkie informacje** o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego 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
- przechowywanie / przeglądanie

„Przetwarzanie”

oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

Co može pójść źle?

- Ryzyko naruszenia art. 5 ust. 1 lit. a RODO
 - Zasada przejrzystości przetwarzania zakłada, że dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”).
- Ryzyko naruszenia art. 5 ust. 1 lit. c RODO
 - Zasada minimalizacji danych zakłada, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”).
- Ryzyko naruszenia art. 13 ust. 2 lit. f, art. 14 ust. 2 lit. g oraz art. 15 ust. 1 lit. h oraz art. 22 RODO
 - Uprawnienia osób przysługujące w przypadku zautomatyzowanego podejmowania decyzji: 1) prawo do istotnych informacji o zastosowaniu mechanizmów zautomatyzowanego podejmowania decyzji (w tym o profilowaniu) oraz o zasadach podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania; 2) prawo do zakwestionowania tej decyzji; 3) prawo do uzyskania interwencji ludzkiej; 4) prawo do wyrażenia własnego stanowiska
- Ryzyko naruszenia art. 28 RODO
 - Dostawcą rozwiązania jest podmiot zewnętrzny
- Ryzyko naruszenia art. 5 ust. 1 lit. b RODO
 - Zasada ograniczenia celu przetwarzania zakłada, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”).
 - W oparciu o dostarczoną strukturę wytrenowany zostanie własny model

Zgodność przepływu danych AI z RODO

Schemat 1: Cykl życia danych w AI

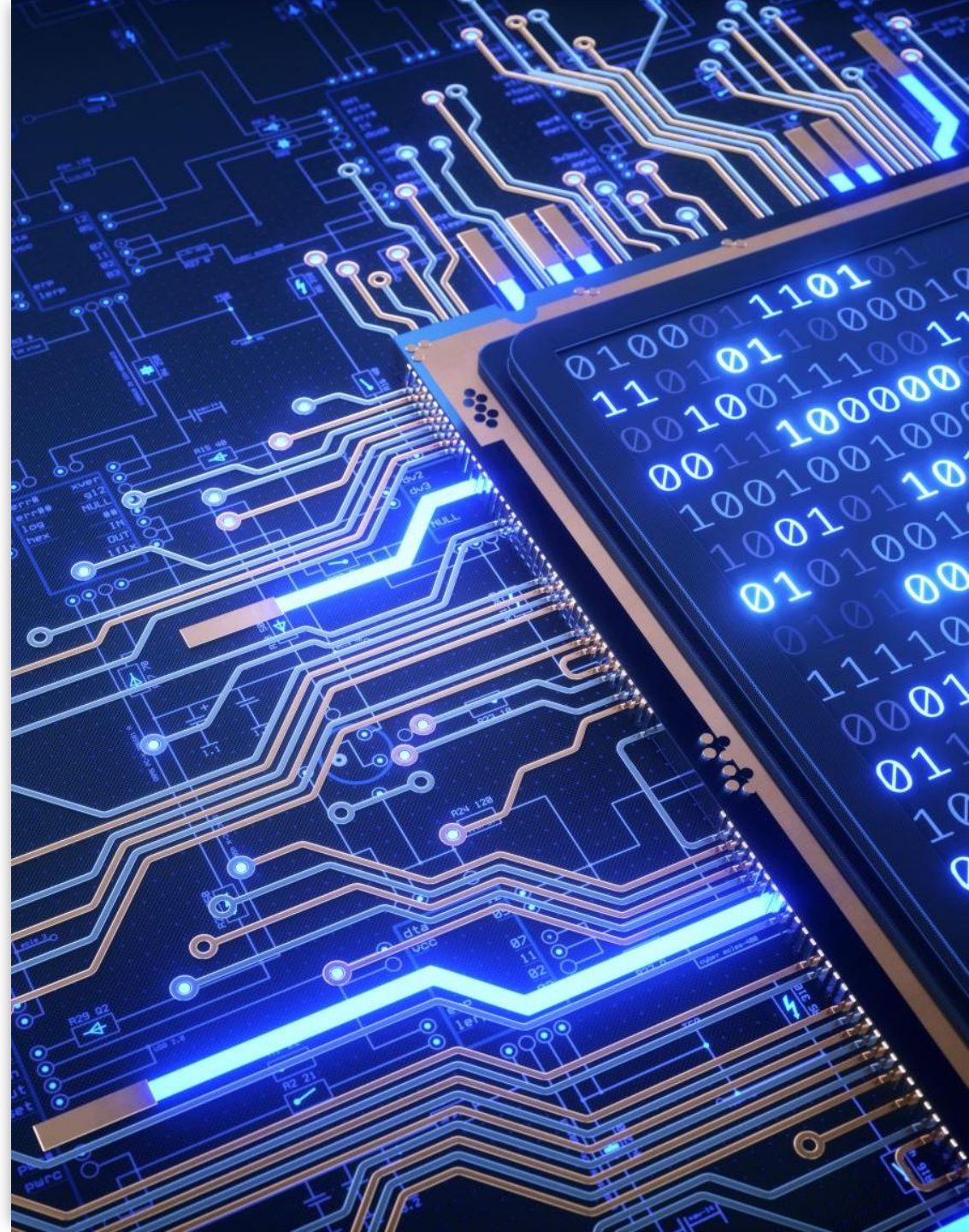
- Zbieranie danych → Przetwarzanie → Analiza → Wykorzystanie wyników

Schemat 2: Punkty kontroli RODO (przykłady)

- Zgoda na przetwarzanie danych (Art. 6 RODO)
- Prawo do bycia zapomnianym (Art. 17 RODO)
- Prawo do ograniczenia przetwarzania (Art. 18 RODO)
- Bezpieczeństwo danych (Art. 32 RODO).
- Obowiązek powiadomienia o naruszeniu danych (Art. 33 RODO).

Pomoc:

- <https://www.cnil.fr/en/take-data-protection-account-data-collection-and-management>
- <https://cyberpolicy.nask.pl/cyberbezpieczenstwo-ai-ai-w-cyberbezpieczenstwie/>



Z życia wzięte

Pani K. pyta:

- Czy wiadomości e-mail od interesariuszy, zawierające dane niepoddane anonimizacji, mogą być klasyfikowane przy użyciu lokalnie działającego modelu językowego (LLM)? Czy przed dokonaniem takiej klasyfikacji osoba kontaktująca się musi zostać poinformowana, że jej wiadomość będzie przetwarzana z wykorzystaniem narzędzi AI?

Jeśli przetwarzanie ma być realizowane na podstawie art. 6 ust. 1 lit. a albo f RODO, wówczas taka informacja powinna być podana, bo:

- w przypadku zgody fakt wykorzystywania LLM może być elementem decydującym o jej udzieleniu lub nie,
- w przypadku uzasadnionego interesu – korzystanie z LLM jest elementem istotnym dla złożenia sprzeciwu.

W pozostałych przypadkach (tj. realizacji umowy) – nie ma obowiązku podawania takiej informacji.

LICENCJE / UMOWY

ChatGPT – wyższy “plan” (również OpenAI for Nonprofits)

*14.2. Limitation on amount of liability. To the fullest extent permitted by law, except for: (a) a party’s gross negligence or willful misconduct, (b) a party’s indemnification obligations under this agreement, or (c) customer’s payment obligations, each party’s total liability under the agreement will not exceed the total amount customer paid to OpenAI during the **twelve months** immediately prior to the event giving rise to liability. the foregoing limitations apply despite any failure of essential purpose of any limited remedy.*

Our commitments provide you with ownership and control over your business data (inputs and outputs from ChatGPT Team, ChatGPT Enterprise, ChatGPT Edu, and our API Platform) and support for your compliance needs.

Ownership

You own and control your data

- ✓ We do not train our models on your business data by default
- ✓ You own your inputs and outputs (where allowed by law)
- ✓ You control how long your data is retained (ChatGPT Enterprise)

Control

You decide who has access within your organization

- ✓ Enterprise-level authentication through SAML SSO (ChatGPT Enterprise and API)
- ✓ Fine-grained control over access and available features
- ✓ Custom models are yours alone to use and are not shared with anyone else

Security

Comprehensive compliance

- ✓ Successfully completed a SOC 2 audit, confirming that our controls align with industry standards for security and confidentiality
- ✓ Data encryption at rest (AES-256) and in transit between our customers and us, and between us and our service providers (TLS 1.2+)
- ✓ Visit our Trust Portal to understand more about our security measures

W sporcie kluczowe jest podejście ostrożnościowe do AI:

Opracować politykę wewnętrzną dotyczącą ochrony danych i poufności – kto i jak może przetwarzać dane w organizacji.

Weryfikować umowy z dostawcami AI – kto ma jakie prawa do danych/treści.

Zapewnić transparentność decyzji AI, np. czy osoby ubiegające się o licencję są profilowane.

Opracować politykę wewnętrzną dotyczącą AI – kto i jak może korzystać z AI w organizacji.

Monitorować zmiany prawne – regulacje dotyczące AI i RODO dynamicznie się rozwijają.

**I kto za to wszystko ponosi
odpowiedzialność?**

Kto odpowiada za błędy AI – związek, dostawca technologii, personel, ktoś inny?

1

Dostawca technologii (producent AI) – ponosi odpowiedzialność za błędy wynikające z konstrukcji, oprogramowania i wad systemu AI. Jeśli błąd wynika z wadliwego działania algorytmów lub wad produktu, odpowiedzialność spada na ich twórców i dostawców technologii.

2

Związek sportowy – jako użytkownik systemu AI kontrolujący ryzyko związane z jego działaniem i czerpiący z niego korzyści, związek odpowiada za właściwe wykorzystanie AI oraz nadzór nad technologią. W przypadku niewłaściwego użycia lub braku należytej staranności w kontroli systemu, związek może ponieść odpowiedzialność za powstałe szkody.

3

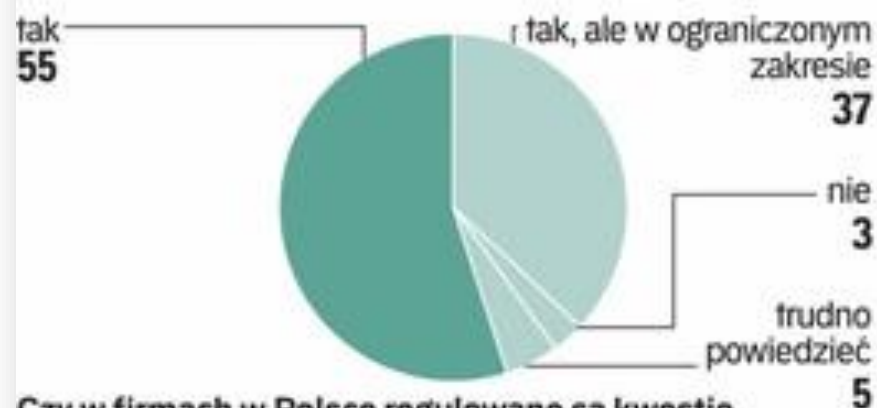
Personel – odpowiadają za decyzje podejmowane na podstawie danych AI oraz za prawidłowe interpretowanie jej wyników. Jeżeli działają niezgodnie z zasadami lub zaniedbują nadzór, mogą być współodpowiedzialni.

Odpowiedzialność związku sportowego i należyta staranność

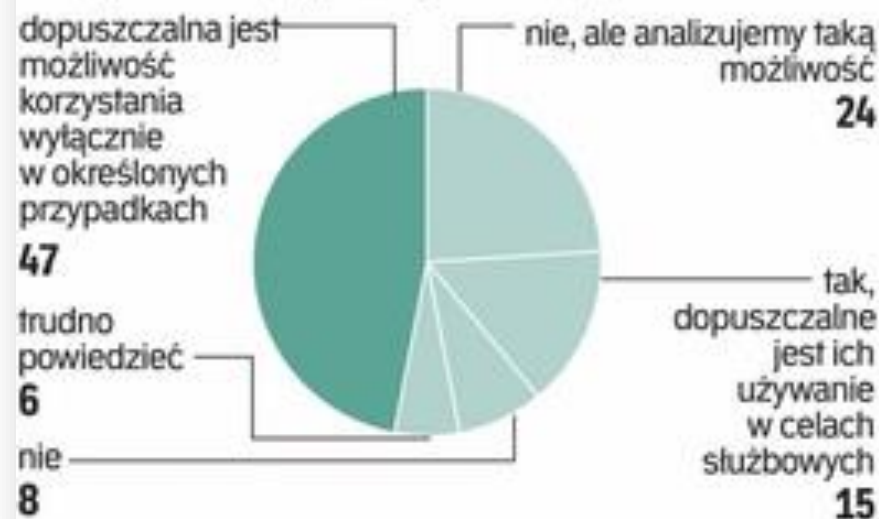
- **Rozproszenie odpowiedzialności** – odpowiedzialność może spoczywać na:
 - twórcy systemu (błędy w projektowaniu, brak zabezpieczeń),
 - integratorze (np. związek wdrażający system AI – odpowiedzialność organizacyjna i *culpa in eligendo*),
 - użytkownikach (np. trenerzy, działacze korzystający z narzędzi).
- **Czyn niedozwolony (art. 415 KC)** – odpowiedzialność powstaje, gdy działanie lub zaniechanie jest:
 - bezprawne,
 - zawinione (umyślność lub niedbalstwo),
 - powoduje szkodę i istnieje związek przyczynowy.
- **Należyta staranność (art. 355 KC)** – miernik: co zrobiłaby staranna i profesjonalna osoba w danej sytuacji (np. testy, procedury, zabezpieczenia, nadzór).
- **Ryzyka praktyczne:**
 - brak testów i audytów systemu,
 - brak regulaminów dot. AI,
 - brak monitorowania dostawców i kontraktów.
- **Kierunek UE** – możliwe przesunięcie ciężaru dowodu i wzmocnienie odpowiedzialności podmiotów wdrażających AI.
- **Black box AI** – ryzyko decyzji nieprzejrzystych i trudnych do wyjaśnienia; konieczność stosowania *Explainable AI* w ocenie np. zawodników i rekomendacjach dla klubów.

I co ja mam z tym wszystkim
zrobić?

Czy wdrażając narzędzia oparte na sztucznej inteligencji, firmy w Polsce analizują aspekt cyberbezpieczeństwa, w proc.



Czy w firmach w Polsce regulowane są kwestie dostępu m.in. do popularnych botów, w proc.



Czy firmy wdrażają szczególne zasady i procedury dotyczące używania systemów AI, w proc.



Źródło: EY

Wykorzystujesz AI w projekcie? Kilka pytań, które możesz sobie zadać:

- ✓ Odpowiedzialność: Kto jest odpowiedzialny, jeśli narzędzie AI popełni błąd, który spowoduje szkodę dla osoby trzeciej?
- ✓ Prawa autorskie: Czy w tym projekcie potrzebuję, aby powstały prawa autorskiego?
- ✓ Dane uczące: Czy dane treningowe (np. wyniki sportowe, nagrania wideo z zawodów) zostały pozyskane legalnie i zgodnie z regulacjami o ochronie danych?
- ✓ Ochrona danych: Jak organizacja chroni dane, kiedy AI je przetwarza?
- ✓ Poufność: Czy wykorzystywane algorytmy (np. systemy analizy techniki wioślarskiej) są poufne i czy mogę je wprowadzać do niewiarygodnego narzędzia AI?
- ✓ Transparentność: Jakie wymagania dotyczące informowania użytkowników o tym, jak działają algorytmy AI, są obligatoryjne?
- ✓ Audytowanie i ocena: Czy konieczna jest regularna ocena i audyt działania narzędzi AI?
- ✓ Aktualizacje: Czy dostawcy narzędzi AI mają prawo do jednostronnych zmian w użytkowaniu i regulaminach?
- ✓ Odporność na ataki: Czy organizacja jest zobowiązana do zapewnienia, że narzędzia AI z których korzysta, są odporne na ataki z zewnątrz?
- ✓ Zakres licencji: Jakie są ograniczenia w zakresie korzystania z narzędzi AI w ramach licencji, jakie są konsekwencje ich naruszenia?
- ✓ Wykorzystanie wyników: Czy organizacja ma prawo do komercyjnego wykorzystania wyników uzyskanych dzięki narzędziom AI? Dodatkowo, czy dostawca narzędzia ma jakieś prawa do nich?
- ✓ Biases (uprzedzenia) w AI: Jak organizacja radzi sobie z problemem uprzedzeń w algorytmach AI, które mogą prowadzić do nierównego traktowania?

Polecane:

Proaktywne monitorowanie zmian prawnych:

- Utrzymuj aktualność: Regularnie aktualizuj wiedzę o nowych przepisach.
- Wykorzystaj technologię: Implementuj narzędzia do monitorowania zmian prawnych.
- Dostosuj produkty i usługi: Regularnie przeglądaj działania organizacji pod kątem zgodności z najnowszymi przepisami.

Nie działaj sam:

- Szkolenia i edukacja pracowników: Organizuj regularne szkolenia dla pracowników dotyczące istotnych aspektów prawnych i regulacyjnych.
- Sieciowanie i współpraca: Możesz uczestniczyć w branżowych spotkaniach i grupach dyskusyjnych, aby dzielić się wiedzą i korzystać z doświadczeń innych organizacji.

Planowanie scenariuszy i zarządzanie ryzykiem:

- Scenariusze: Możesz w połączeniu z innymi podobnie działającym organizacjami przeprowadzać analizy potencjalnych skutków zmian prawnych na działalność organizacji.
- Strategie zarządzania ryzykiem: Opracujcie wspólnie strategie zarządzania ryzykiem, aby minimalizować potencjalne negatywne skutki zmian prawnych.

**Dziękuję
i zapraszam do kontaktu.**

aleksandra.maciejewicz@lawmore.pl

LAW MORE