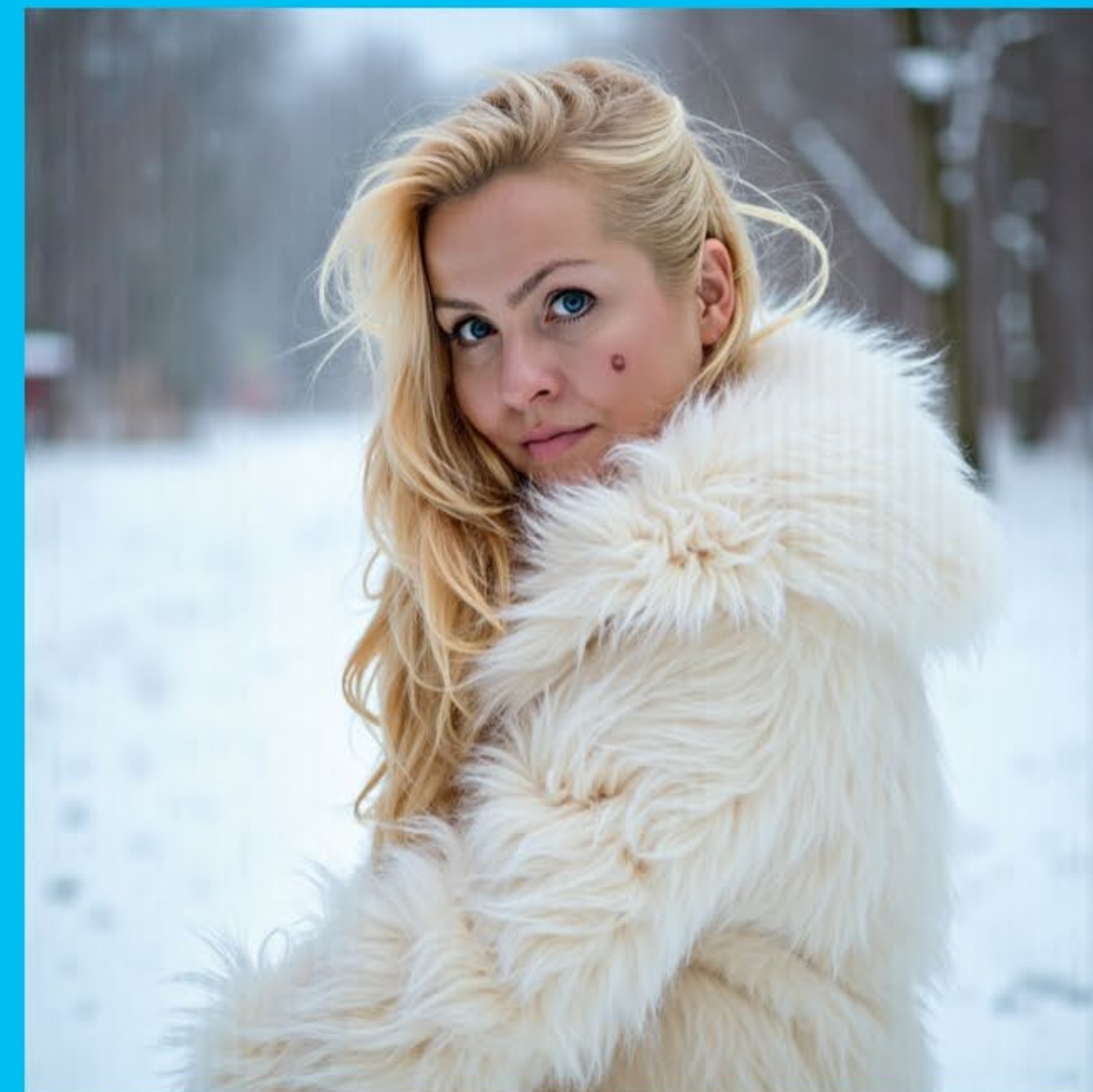


SZTUCZNA INTELIGENCJA. OBSZARY IMPLEMENTACJI

dr Ada Florentyna Pawlak, Uniwersytet SWPS



Rzeczpospolita
Polska

Sfinansowane przez
Unię Europejską
NextGenerationEU



Województwo
Śląskie

ASPEKTY PRAWNE AI

MIT Technology Review

CODING A MORAL MACHINE

How driverless cars mimic
human decisions using
computational models.

You Don't Need A
Blood Boy:
Why Transfusions Are
Overrated

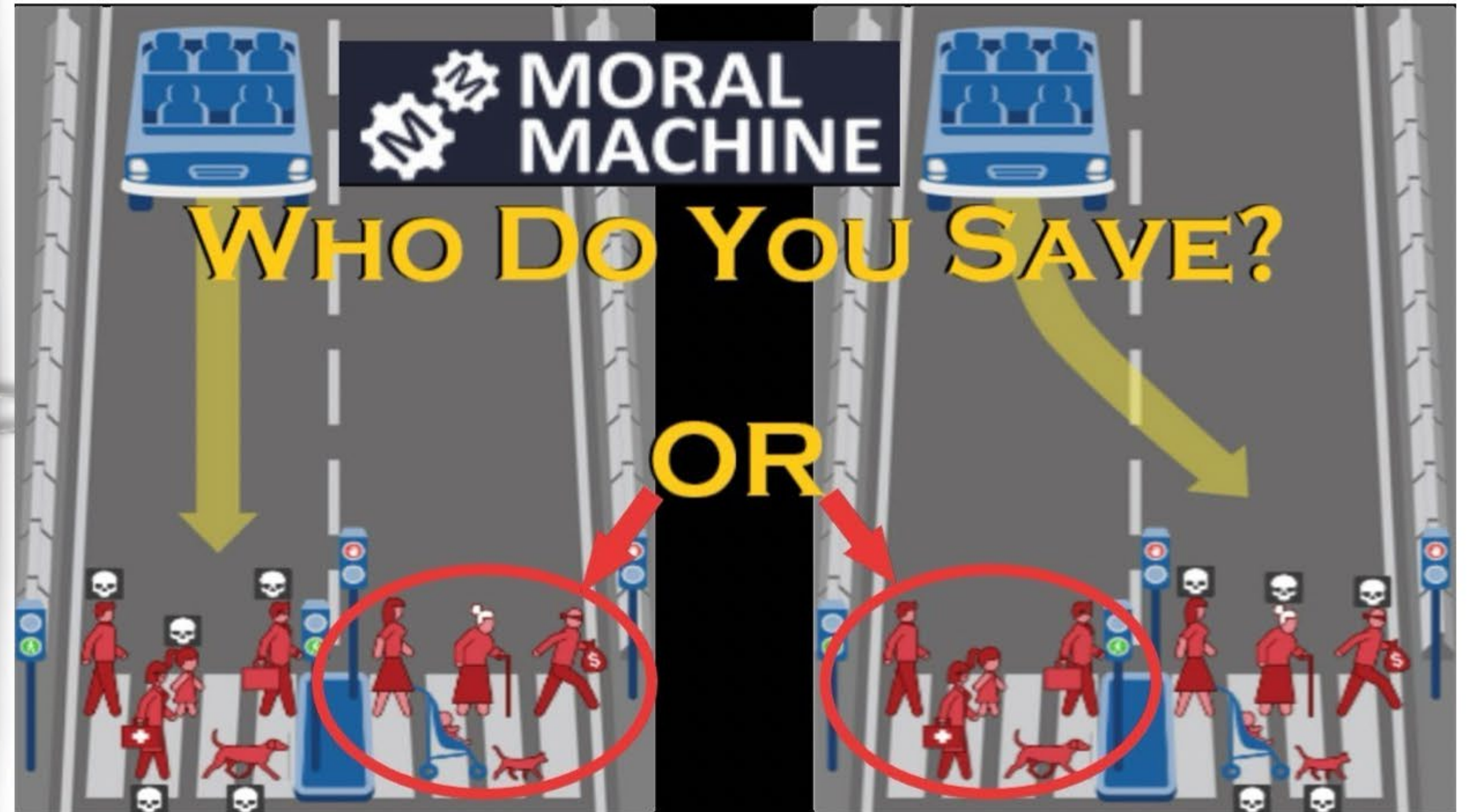
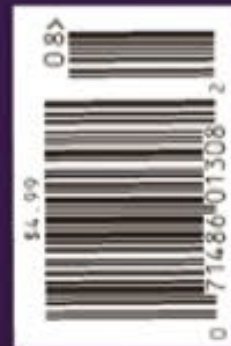
Review p.72

Surgery Simulation with
Laser Babies

Feature p.69

What You Didn't Know
About Antibiotics

Feature p.80





**STOP SHARING PERSONAL DETAILS WITH
CHAT GPT OR YOU MIGHT GET IN TROUBLE!!**



NEWS FLASH

**WHAT YOU SAY TO CHATGPT ISN'T AS
PRIVATE AS YOU THINK, EVEN DELETED
CHATS CAN BE ACCESSED, OPENAI CEO
SAM ALTMAN WARNS USERS.**

**TELL US IN THE COMMENTS BELOW AND
TAG YOUR BEST BUDDY TO LET THEM KNOW!!**

Typy gromadzonych danych

- Gromadzone dane:
 - o użytkownikach
 - o sposobach korzystania/ zachowaniach użytkowników
 - o relacjach między użytkownikami
 - o reakcjach (w schemacie eksperymentalnym)
- Problemy
 - gromadzenia danych – czy w ogóle są zapisywane?
 - jakości danych – jakie dane i w jaki sposób są zbierane?
 - wykorzystania danych – jak z nich skorzystać i w jakim celu?

Do kogo należą dane?

Services for individuals, such as ChatGPT and DALL·E

When you use our services for individuals such as ChatGPT or DALL·E, we may use your content to train our models.

You can opt out of training through our [privacy portal](#) by clicking on "do not train on my content," or to turn off training for your ChatGPT conversations, follow the instructions in our [Data Controls FAQ](#). Once you opt out, new conversations will not be used to train our models.

Services for businesses, such as ChatGPT Team, ChatGPT Enterprise, and our API Platform

We don't use content from our business offerings such as ChatGPT Team, ChatGPT Enterprise, and our API Platform to train our models. Please see our [Enterprise Privacy page](#) for information on how we handle business data.

How your data is used to improve model performance

<https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance>

Do kogo należą dane?

Ownership: You own and control your data

- We do not train on your business data (data from ChatGPT Team, ChatGPT Enterprise, or our API Platform)
- 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

- 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

- We've been audited for SOC 2 compliance (ChatGPT Enterprise and API)
- Data encryption at rest (AES-256) and in transit (TLS 1.2+)

Źródło: <https://openai.com/enterprise-privacy/>

Czy będziemy dzielić się naszymi danymi?

- Chcesz płacić mniej za ubezpieczenie zdrowotne?
- Chcesz płacić mniej za ubezpieczenie samochodu?
- Chcesz żebym udowodnił że będę dobrym, odpowiedzialnym pracownikiem?
- Podziel się danymi dotyczącymi zdrowia, aktywności fizycznej.
- Podziel się danymi z czarnej skrzynki swojego samochodu.
- Udostępnij dane o zawartości alkoholu we krwi albo statystyki produktywności z ostatnich 3 lat?

AI Act

Bruksela, dnia 21.4.2021 r. COM(2021) 206 final 2021/0106 (COD)

Artykuł 5

1. Zakazuje się następujących praktyk w zakresie sztucznej inteligencji:

a) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, **który stosuje techniki podprogowe** będące poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób, **który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną;**

b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, **który wykorzystuje dowolne słabości określonej grupy osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne** w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób, **który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;**

ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji **przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych** prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, kiedy to **punktowa ocena społeczna prowadzi do jednego lub obu z następujących skutków:**

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

ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

wykorzystywania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa, chyba że i w zakresie, w jakim takie wykorzystanie jest absolutnie niezbędne do jednego z następujących celów:

- (i) ukierunkowanego poszukiwania konkretnych potencjalnych ofiar przestępstw, w tym zaginionych dzieci;
- (ii) zapobiegnięcia konkretnemu, poważnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub atakowi terrorystycznemu;
- (iii) wykrywania, lokalizowania, identyfikowania lub ścigania sprawcy przestępstwa lub podejrzanego o popełnienie przestępstwa, o którym mowa w art. 2 ust. 2 decyzji ramowej Rady 2002/584/WSiSW i które w danym państwie członkowskim podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej trzy lata, zgodnie z prawem danego państwa członkowskiego.

ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

- **wymaga uzyskania uprzedniego zezwolenia** udzielonego przez organ sądowy lub niezależny organ administracyjny państwa członkowskiego, w którym ma nastąpić wykorzystanie, wydanego na uzasadniony wniosek i zgodnie ze szczegółowymi przepisami prawa krajowego

TYTUŁ III

SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

1. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 73 w celu aktualizacji wykazu zawartego w załączniku III poprzez dodanie systemów sztucznej inteligencji wysokiego ryzyka, jeżeli spełnione są oba poniższe **warunki**:
 - a) systemy sztucznej inteligencji są przeznaczone do wykorzystywania w którymkolwiek z obszarów wymienionych w załączniku III pkt 1–8;
 - b) **systemy sztucznej inteligencji stwarzają ryzyko szkody dla zdrowia i bezpieczeństwa lub ryzyko niekorzystnego wpływu na prawa podstawowe**, które pod względem dotkliwości i prawdopodobieństwa wystąpienia jest równoważne ryzyku szkody lub niekorzystnego wpływu, które stwarzają systemy sztucznej inteligencji wysokiego ryzyka wymienione już w załączniku III, lub jest od niego większe.

TYTUŁ III

SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

Komisja uwzględnia następujące kryteria:

- a) **przeznaczenie systemu** sztucznej inteligencji;
- b) **zakres**, w jakim system sztucznej inteligencji był wykorzystywany lub może być wykorzystywany;
- c) zakres, w jakim wykorzystywanie systemu sztucznej inteligencji spowodowało już szkodę dla zdrowia i bezpieczeństwa lub miało niekorzystny wpływ na prawa podstawowe lub wzbudziło istotne obawy co do możliwości wystąpienia takiej szkody lub niekorzystnego wpływu, czego potwierdzeniem są zgłoszenia lub udokumentowane zarzuty przedłożone właściwym organom krajowym;
- d) **potencjalny zakres takiej szkody lub takiego niekorzystnego wpływu**, w szczególności pod względem ich nasilenia i możliwości oddziaływania na wiele osób;
- e) zakres, w jakim osoby potencjalnie poszkodowane lub dotknięte niekorzystnym wpływem **są zależne od wyniku działania systemu sztucznej inteligencji**, w szczególności ze względu na fakt, że z przyczyn praktycznych lub prawnych nie jest możliwe zasadne zrezygnowanie z tego wyniku;
- f) zakres, w jakim osoby potencjalnie poszkodowane lub dotknięte niekorzystnym wpływem znajdują się **w słabszym położeniu względem użytkownika systemu** sztucznej inteligencji, w szczególności z powodu nierównego układu sił, wiedzy, sytuacji gospodarczej lub społecznej lub wieku;

TYTUŁ III

SYSTEMY SZTUCZNEJ INTELIGENCJI WYSOKIEGO RYZYKA

Komisja uwzględnia następujące kryteria:

- h) zakres, w jakim obowiązujące przepisy Unii przewidują:
- (i) **skuteczne środki dochodzenia roszczeń w związku z zagrożeniami** stwarzanymi przez system sztucznej inteligencji, z wyłączeniem roszczeń o odszkodowanie;
- (ii) **skuteczne środki zapobiegania temu ryzyku lub jego znacznego zminimalizowania.**

Obowiązek AI Literacy – nowe wyzwanie dla pracodawców

Zgodnie z art. 4 AI Act, od 2 lutego 2025 r. wszedł również obowiązek podnoszenia kompetencji pracowników w zakresie sztucznej inteligencji, tzw. AI Literacy.

Oznacza to, że zarówno dostawcy, jak i użytkownicy systemów AI muszą podjąć działania zmierzające do zapewnienia swoim pracownikom niezbędnej wiedzy oraz umiejętności umożliwiających efektywne i bezpieczne korzystanie z technologii AI.

Pracodawcy mają obowiązek przygotowania zespołów, biorąc pod uwagę m.in. aspekty techniczne, doświadczenie, wykształcenie oraz odpowiednie szkolenia, dostosowując je do specyfiki wykorzystywanych systemów i grup docelowych.

Kompetencje AI Literacy obejmują m.in.:

- **Wiedzę techniczną:** zrozumienie działania systemów AI.
- **Świadomość ryzyk:** rozpoznawanie potencjalnych zagrożeń związanych z AI.
- **Zgodność z przepisami:** znajomość wymogów prawnych dotyczących sztucznej inteligencji.
- **Umiejętności praktyczne i etyczne:** zdolność do odpowiedzialnego korzystania z systemów AI.

Warto pamiętać, że AI Literacy to nie jednorazowe szkolenie, ale ciągły proces dostosowywania się do dynamicznie rozwijającej się technologii. Firmy, które odpowiednio wcześniej zainwestują w kompetencje swoich pracowników, zyskają przewagę konkurencyjną i unikną potencjalnych problemów prawnych.

Jak przygotować się do nowych przepisów?

Przedsiębiorcy powinni już teraz podjąć działania, aby dostosować się do nowych wymogów. Kluczowe kroki to:

- 1 Mapowanie systemów AI:** zidentyfikowanie wszystkich systemów AI wykorzystywanych w firmie.
- 2 Analiza ryzyka:** określenie potencjalnych zagrożeń związanych z użyciem AI.
- 3 Audyt prawny:** ocena zgodności z obowiązującymi przepisami.
- 4 Szkolenia pracowników:** wdrożenie programów szkoleniowych, które podniosą kompetencje zespołu w zakresie AI.
- 5 Monitoring legislacyjny:** śledzenie wytycznych i rekomendacji dotyczących AI Act.