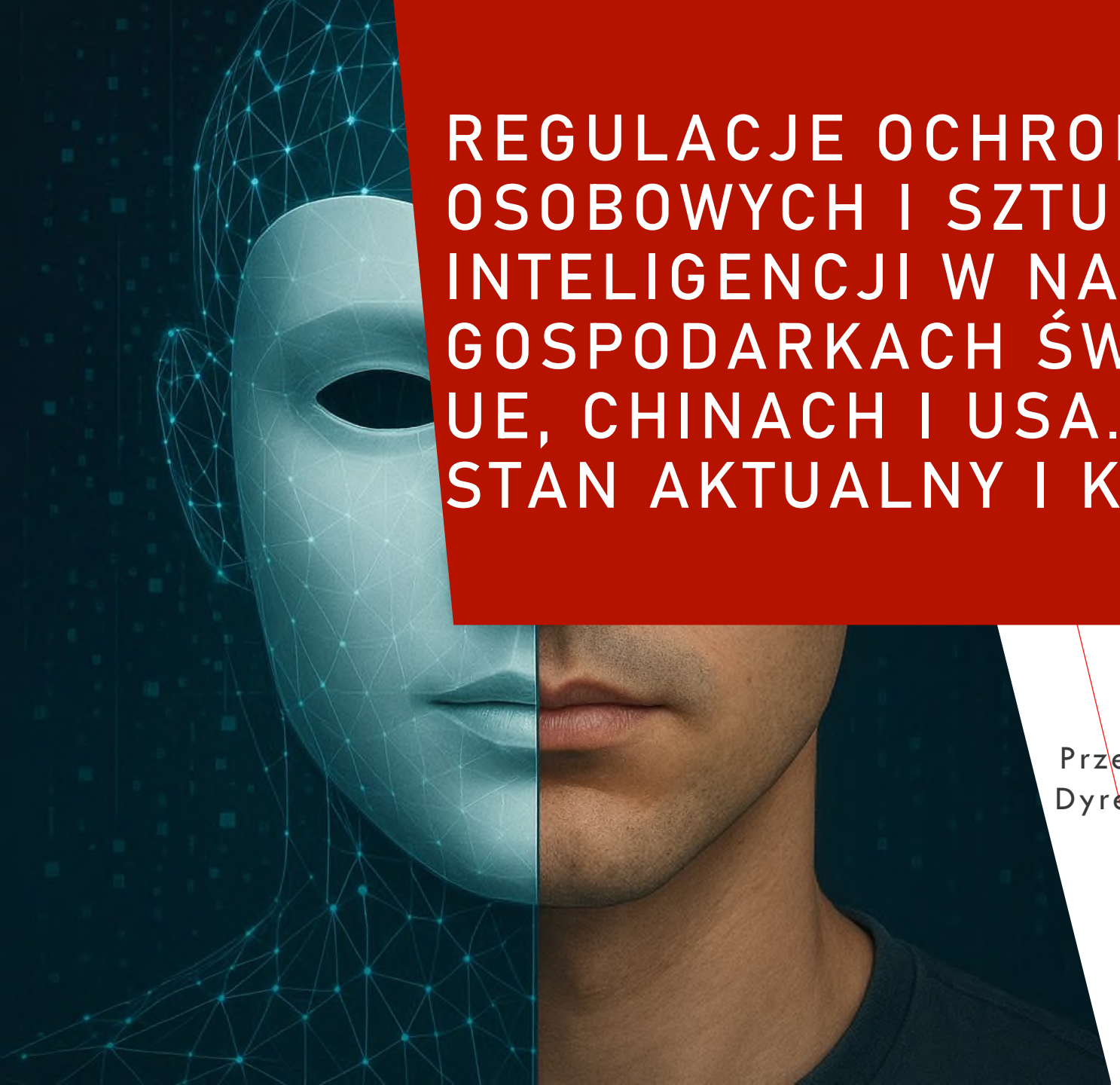

REGULACJE OCHRONY DANYCH OSOBOWYCH I SZTUCZNEJ INTELIGENCJI W NAJWIĘKSZYCH GOSPODARKACH ŚWIATA: UE, CHINACH I USA. STAN AKTUALNY I KIERUNKI ROZWOJU

prof. AKP, dr hab. Mariusz Krzysztofek

Przewodniczący Rady Dyscypliny Nauki Prawne AKP,
Dyrektor Centrum Prawa Ochrony Danych i Sztucznej Inteligencji

Privacy Director EMEA, Global DPO, Herbalife

REGULACJE SZTUCZNEJ INTELIGENCJI W USA

- Dotychczas brak ustawy federalnej o AI ale liczne rozproszone regulacje
- Podejście sektorowe oraz ustawy na poziomie stanów

- Prezydenckie Rozporządzenia Wykonawcze (Executive Orders) - określenie polityki i strategii władz federalnych wobec AI
  - Executive Order 13859 - Maintaining American Leadership in Artificial Intelligence" z 11.2.2019, cel: utrzymanie przez USA pozycji globalnego lidera w dziedzinie AI + godna zaufania AI, niedyskryminacja, prywatność
  - Executive Order 13960 - Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government z 3.12.2020 agencje federalne)

- podejście sektorowe, np. sektor finansowy – zastosowanie The Equal Credit Opportunity Act (ECOA) z 1974 r.

- niewiążące wytyczne na szczeblu federalnym: Ramy zarządzania ryzykiem AI („AI Risk Management Framework" (AI RMF 1.0)), National Institute of Standards and Technology (NIST) 2023 r.

REGULACJE SZTUCZNEJ INTELIGENCJI W USA

- Na koniec 2025 r. ogólne ustawy o AI w: Kalifornii, Utah, Kolorado i Teksasie (ale ustaw sektorowych o AI - kilkadziesiąt i w około połowie stanów).

Najbardziej kompleksowa ustawa: Kolorado (Colorado Senate Bill 24-205, Consumer Protections for Artificial Intelligence, Colorado AI Act), od 1 lutego 2026 r.

Poza ustawami ustanawiający ogólne ramy regulacyjne dla AI - kilkadziesiąt ustaw sektorowych regulujących zastosowania AI, np. w obszarze opieki zdrowotnej.

- Rozporządzenie wykonawcze „One Rule Executive Order", 11 grudnia 2025 r.

Cel: utrzymanie przewagi w wyścigu z Chinami.

Nie uchyla obowiązujących ustaw stanowych ani nie pozbawia stanów kompetencji do uchwalania przyszłych regulacji. Wyznacza kierunek działań organów federalnych oraz ma na celu ograniczenie fragmentacji regulacyjnej. Ewentualna przyszła federalna ustawa o sztucznej inteligencji mogłaby wywołać skutek preempcji wobec prawa stanowego.

CCPA: DEFINICJA DANYCH OSOBOWYCH

Podstawa zbliżona do RODO
ale

- konsument (mieszkaniec Kalifornii)
- komponent „gospodarstwa domowego” (dane osobowe to informacje, które identyfikują lub które można powiązać z konsumentem lub gospodarstwem domowym); jednak definicja nie wskazuje kryterium odróżniającego osobę w gospodarstwie domowym od konsumenta w definicji danych osobowych; CPRA household jako zidentyfikowana grupa konsumentów mieszkająca pod tym samym adresem i wspólnie użytkująca wspólne urządzenia lub usługi;
- natomiast wyłączenie prawa do usunięcia, korekty i dostępu do danych wobec danych gospodarstw domowych.

CCPA: DEFINICJA DANYCH OSOBOWYCH

Definicja danych osobowych w CCPA nie obejmuje informacji publicznie dostępnych ani uzyskanych zgodnie z prawem prawdziwych informacji, które stanowią przedmiot zainteresowania opinii publicznej (*publicly available information or lawfully obtained, truthful information that is a matter of public concern*). „Publicznie dostępne” informacje - udostępnione zgodnie z prawem z rejestrów władz federalnych, stanowych lub lokalnych, lub informacje, co do których administrator ma uzasadnione podstawy sądzić, że zostały zgodnie z prawem udostępnione ogółowi społeczeństwa przez konsumenta lub media o szerokim zasięgu, lub informacje udostępnione przez osobę, której konsument je ujawnił, jeżeli konsument nie ograniczył ich do określonego grona odbiorców.

ZAKRES MATERIALNY I ADMINISTRATOR DANYCH

Administrator danych [1798.140(d)(1) CCPA] – *business*), działalność komercyjna (np. nie organizacje non-profit ani organy administracji publicznej), działalności dla zysku lub korzyści finansowej swoich akcjonariuszy lub innych właścicieli, zbieranie (przetwarzanie) danych konsumentów, progi kwotowe i inne, poniżej których ustawa nie ma do administratora zastosowania

1) roczne przychody brutto – przekraczające 25 mln USD w poprzednim roku kalendarzowym;
2) liczba danych osobowych konsumentów lub gospodarstw domowych – 100 tys. lub więcej – które samodzielnie lub wspólnie, corocznie kupuje, sprzedaje lub udostępnia;
3) co najmniej 50% rocznych przychodów uzyskiwanych ze sprzedaży lub udostępniania danych osobowych konsumentów.

REGULACJE SZTUCZNEJ INTELIGENCJI W CHINACH

- ustawy Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych – brak kompleksowej ustawy o AI

ale plany prac legislacyjnych Rady Państwa i Stałego Komitetu Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych oraz projekty ustawy opracowane przez środowiska eksperckie i akademickie
przepisy sektorowe - w dziedzinach takich jak ruch drogowy, ekologia, szkolnictwo wyższe

- rozporządzenia administracyjne Rady Państwa

np. dotyczące uzależnienia algorytmicznego (w art. 19) rozporządzenie administracyjne Rady Państwa w sprawie ochrony małoletnich w środowisku internetowym przyjęte 20 września 2023 r. i obowiązujące od 1 stycznia 2024 r.

- szczególne znaczenie - Chińska Administracja Cyberprzestrzeni (Cyberspace Administration of China, CAC) – resortowe / normatywne

rozporządzenia administracyjne dotyczące: algorytmów rekomendacji (rejestr generatywnych narzędzi AI), algorytmów głębokiej syntezy (deepfake) i generatywnej AI
Measures for the Labeling of AI-Generated Synthetic Content

- standardy i normy – obligatoryjne / rekomendowane

np. Data Annotation Security Specification – dotyczący bezpieczeństwa procesu oznaczania danych treningowych oraz wymagań dla zbiorów danych wykorzystywanych w treningu i dostrajaniu modeli, National Technical Committee 260 on Cybersecurity of Standardization Administration of China (TC260)

- pilotaże, etapowe wdrażanie przepisów

OCHRONA DZIECI W CYBERPRZESTRZENI

- RODO - 16 / 13 lat – brak ogólnego wymogu uzyskania zgody na przetwarzanie, próg wieku ale dla usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku i zgoda rodziców poniżej progu wieku
- PIPL - 14 lat – małoletni w wieku poniżej 14 lat – dane wrażliwe (art. 28 PIPL); zakaz grania w Internecie poniżej 18. roku ponad krótki limit czasowy - w weekendy i święta, w godzinach 20:00–21:00, system rejestracji z użyciem prawdziwych danych osobowych, automatyczne przerywanie gry po przekroczeniu dziennego limitu
- COPPA (Children's Online Privacy Protection Act) – dotyczy głównie komercyjnych witryn internetowych i usług online skierowanych do dzieci poniżej 13. roku życia; przeciwdziałanie komercjalizacji danych osobowych dzieci oraz „prurient interest", do których należą treści pornograficzne
- australijska Online Safety Amendment (Social Media Minimum Age) Bill 2024 (obowiązuje od grudnia 2025) – obowiązek dostawców usług mediów społecznościowych podejmowania „rozsądnych działań" aby uniemożliwić dostęp do nich użytkownikom poniżej 16. roku życia, zgoda rodziców bezprzedmiotowa;

  zakaz m.in.: Facebook, Instagram, Kick, Reddit, Snapchat, TikTok, Twitch, X, YouTube, poza zakazem m.in: Discord, GitHub, Messenger, Pinterest, Steam, WhatsApp.

Polska: w grupie 7–12 lat z serwisów społecznościowych i komunikatorów aktywnie korzysta 58% użytkowników, czyli prawie 1,5 mln dzieci. 32% tych dzieci z TikToka, a 1 z 10 najpopularniejszych serwisów (w grupie wiekowej 7–14 lat) - serwis pornograficzny (Instytut Cyfrowego Obywatelstwa, Raport „Internet dzieci")

DEEPFAKE'I I OBOWIĄZEK OZNACZANIA TREŚCI GENEROWANYCH PRZEZ AI

Measures for the Labeling of AI-Generated Synthetic Content, 四部门联合发布《人工智能生成合成内容标识办法》, 14 marca 2025 r., obowiązuje od 1 września 2025 r.

Obowiązek dostawców usług generatywnych AI (a więc m.in. generatorów tekstu, mowy lub wideo) wyraźnego oznaczania treści wygenerowanych przez sztuczną inteligencję (np. w formie symboli graficznych) lub w formie metadanych)

Obowiązek ten dotyczy także użytkowników, którzy publikują treści wygenerowane przez AI w celu wpływania na opinię publiczną, a więc np. o charakterze politycznym

Wspierane przez obowiązkowy standard krajowy: GB 45438-2025 Cybersecurity Technology – Labeling Method for Content Generated by Artificial Intelligence

zdjęcie reklamy z metra w Pekinie: napis w lewym dolnym rogu: 作品名称:《地铁奇妙之旅》本作品由AIGC生成, 不代表真实场景 obraz został wygenerowany przez AI (AI Generated Content)

DEEPFAKE'I I OBOWIĄZEK OZNACZANIA TREŚCI GENEROWANYCH PRZEZ AI

Ustawy głównie przeciwko niechcianym deep fake'om o charakterze seksualnym, w niektórych stanach szczególnie zawierającym wizerunki dzieci, oraz zmierzającym do manipulacji procesem wyborczym.

- Federalna ustawa „Take It Down Act", obowiązek objętych nią platform internetowych (od maja 2026 r.) usunięcia niechcianych intymnych materiałów (nonconsensual intimate images, NCII), nie tylko deep fake'ów, w ciągu 48 godzin od powiadomienia

- Przykłady na poziomie stanów ustaw
  - deepfake'i w kampaniach wyborczych:

Kalifornia, Assembly Bill 2655 (AB 2655, Defending Democracy from Deepfake Deception Act of 2024)
Kolorado, Candidate Election Deepfake Disclosures Act (HB 24-1147) 24 maja 2024 r. (oznaczanie)

  - Kalifornia, 1 stycznia 2025 r. SB 926 nowy typ przestępstwa - tworzenie i udostępnianie deepfake'ów przedstawiających istniejącą osobę w jednoznacznie seksualnym kontekście bez jej zgody, a SB 981 procedura usuwania takich treści przez platformy internetowe po potwierdzeniu zasadności zgłoszenia.

DEEPFAKE'I I OBOWIĄZEK OZNACZANIA TREŚCI GENEROWANYCH PRZEZ AI

Podmioty stosujące system AI, który generuje obrazy, treści audio lub wideo stanowiące deepfake lub który manipuluje takimi obrazami lub treściami, ujawniają to → wyjątek: wyraźnie artystyczny, twórczy, satyryczny, fikcyjny lub analogiczny charakter (Art. 50 ust. 4 AI Act)

European Commission, The General-Purpose AI Code of Practice, zatwierdzony przez KE i AI Board 1.08.2025, dobrowolnego porozumienie (m.in. Google, Microsoft i OpenAI), zobowiązanie do wprowadzania oznaczeń na wytworzonych przez ich modele AI materiałach udostępnianych publicznie, szczególnie w kontekście ochrony konsumentów i przeciwdziałania dezinformacji

DSA?

C2PA Coalition for Content Provenance and Authenticity

Realistyczne a nie artystyczne, satyryczne.
Miejsca parkingowe na powierzchni dla każdego?...

W Polsce fake powielany jako: "Potęga Unii Europejskiej na jednym zdjęciu"
Macron przedstawiony jako istota o czterech nogach, w tym dwóch kobiecych.

DZIĘKUJĘ
I ZAPRASZAM DO DYSKUSJI

prof. AKP dr hab. Mariusz Krzysztofek

Przewodniczący Rady Dyscypliny Nauki Prawne AKP,
Dyrektor Centrum Prawa Ochrony Danych i Sztucznej Inteligencji

Privacy Director EMEA, Global DPO, Herbalife