

# 2025: Rok Rewolucji Technologicznej w Ochronie Danych - Przewidywania na podstawie wniosków z najnowszego raportu TechSonar 2025

Posted on 2025-01-31

Technologia rozwija się w niesamowitym tempie, a rok 2024 był tego najlepszym dowodem. Świat doświadczył przełomów takich jak zastosowanie generatywnej sztucznej inteligencji w medycynie, dynamiczny rozwój kwantowej kryptografii oraz praktyczne wdrożenia cyfrowych bliźniaków w zarządzaniu miastami. Każda z tych innowacji wyznaczała nowe standardy, ale też prowokowała pytania o ich wpływ na prywatność i ochronę danych.

Czy tempo tych zmian utrzyma się, a nawet przyspieszy? Warto przyjrzeć się prognozom

zawartym w raporcie TechSonar 2025, który stanowi przewodnik po nadchodzących trendach i ich możliwym wpływie na ochronę danych.

# Czym jest TechSonar?

TechSonar to inicjatywa Europejskiego Inspektora Ochrony Danych (EIOD), która identyfikuje najważniejsze trendy technologiczne w kontekście ochrony danych osobowych. Raport ten ma na celu przewidywanie kierunków rozwoju technologii i ich wpływu na prywatność, umożliwiając podejmowanie działań prewencyjnych, zanim ryzyka związane z nowymi technologiami staną się realnym zagrożeniem. TechSonar 2025 wskazuje sześć kluczowych trendów technologicznych, które mogą zmienić sposób, w jaki chronimy dane osobowe. Niektóre technologie opisane w najnowszym raporcie TechSonar mogą pomóc w ograniczaniu ryzyka związanego z podstawowymi prawami jednostek. Z kolei inne, choć obiecują znaczące korzyści ekonomiczne, mogą stanowić poważne zagrożenie dla osób, jeśli nie będą właściwie zarządzane. Dlatego kluczowe stają się analizy ryzyka i wdrażanie solidnych środków ochronnych.

W kontekście sztucznej inteligencji, dostawcy i użytkownicy systemów AI muszą dokładnie oceniać ich wpływ, identyfikować potencjalne zagrożenia i podejmować działania zapobiegawcze, tym bardziej, że dynamiczny rozwój tej dziedziny, w połączeniu z możliwością wysokich zysków, napędza wyścig w obszarze sztucznej inteligencji, co sprawia, że systemy AI stają się coraz bardziej obecne w naszym codziennym życiu. Ponadto w raporcie przedstawiono scenariusze dotyczące każdego z sześciu trendów związanych ze sztuczną inteligencją. Opisujemy je poniżej. Warto podkreślić, że EIOD nie aprobuje tych przypadków użycia - ich jedynym celem jest zobrazowanie potencjalnych sytuacji, które mogą wynikać z zastosowania tych technologii. Scenariusze te mogą poruszać istotne kwestie związane z prawem do prywatności, ochroną danych osobowych, a także z szerszym wpływem na społeczeństwo.

# Najważniejsze trendy technologiczne na 2025 rok

## 1. Retrieval-Augmented Generation (RAG)

Modele generatywne takie jak ChatGPT, są wzbogacane o dostęp do zewnętrznych baz wiedzy. Dzięki temu mogą dostarczać bardziej precyzyjne i aktualne odpowiedzi, jednocześnie zmniejszając ryzyko generowania nieprawdziwych informacji. Należy jednak podkreślić, że systemy RAG wykorzystują dane zewnętrzne i zasoby informacji, które mogą zawierać dane osobowe. Jeśli zapytanie użytkownika jest bardzo szczegółowe, system RAG może przypadkowo pobrać i ujawnić takie dane, zwłaszcza jeśli znajdują się one w materiałach źródłowych lub w danych szkoleniowych. Takie ujawnienie stanowiłoby naruszenie ochrony danych osobowych, co jest szczególnie problematyczne w kontekście zgodności z przepisami RODO.

## 2. AI działające na urządzeniach (On-Device AI)

Dzięki edge computing możliwe jest lokalne przetwarzanie danych na urządzeniach użytkownika. To nie tylko przyspiesza działanie systemów, ale także minimalizuje konieczność przesyłania wrażliwych informacji do chmury, co zwiększa bezpieczeństwo. Chociaż przetwarzanie danych lokalnie może poprawić prywatność, jeśli urządzenie nie jest odpowiednio zabezpieczone (np. brak szyfrowania lub słabe hasła), to dane mogą być łatwiejszym celem dla atakujących.

## 3. AI multimodalna (MultimodalAI)

Nowe modele AI łączą dane różnych typów, takich jak tekst, obraz czy dźwięk, umożliwiając bardziej kompleksowe analizy i zastosowania. Tego rodzaju integracja może jednak

wymagać zaawansowanych mechanizmów ochrony danych, aby zapobiec nadużyciom. Systemy te mają tendencję do zbierania danych z wielu źródeł jednocześnie, co może prowadzić do nadmiernego gromadzenia informacji, nie zawsze niezbędnych do celów przetwarzania. W efekcie firmy mogą posiadać ogromne ilości danych osobowych, których zbieranie i przetwarzanie może być niezgodne z zasadami minimalizacji danych zgodnie z RODO.

#### 4. Skalowalny nadzór (Scalable Oversight)

Złożoność nowoczesnych systemów AI wymaga bardziej efektywnych metod monitorowania ich działania. Skalowalny nadzór pozwala na bieżące śledzenie zgodności z przepisami i zasadami etycznymi, co ma kluczowe znaczenie w kontekście dynamicznie rozwijających się technologii.

#### 5. Neuro-symboliczna sztuczna inteligencja (Neuro-Symbolic AI)

Połączenie sieci neuronowych z tradycyjną logiką symboliczną pozwala AI lepiej rozwiązywać złożone problemy. Może to zwiększyć efektywność systemów AI, ale jednocześnie stawia wyzwania związane z odpowiedzialnością za podejmowane decyzje.

#### 6. Oduczanie się maszyn (Machine Unlearning)

Jednym z najbardziej przełomowych osiągnięć przedstawionych w TechSonar 2025 jest bez wątpienia technologia „oduczania się maszyn”. Odgrywa kluczową rolę w kontekście wymagań stawianych przez RODO, w szczególności w zakresie prawa do bycia zapomnianym (art. 17 RODO). Zgodnie z tym przepisem, osoby fizyczne mają prawo żądać usunięcia swoich danych osobowych, jeśli dalsze ich przetwarzanie nie jest uzasadnione prawnie lub narusza ich prywatność. W przypadku sztucznej inteligencji, która opiera swoje działanie na dużych zbiorach danych, realizacja tego prawa może być wyzwaniem. Technologia „oduczania się maszyn” może okazać się rozwiązaniem tego problemu, umożliwiając efektywne zarządzanie danymi w zgodzie z regulacjami prawnymi.

# W kontekście RODO technologia ta pozwoli na:

- realizację prawa do bycia zapomnianym. Modele AI mogą usuwać wpływ konkretnych danych treningowych, co zapewni, że dane osoby, która żąda ich usunięcia, nie są już wykorzystywane w procesach decyzyjnych.
- zgodność z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO) poprzez redukcję zbiorów danych do tych, które są niezbędne, oraz eliminację danych, które nie powinny być już przetwarzane.
- zapobieganie naruszeniom bezpieczeństwa danych (art. 32 RODO), ponieważ usuwanie nieaktualnych lub nieautoryzowanych danych minimalizuje ryzyko błędnych lub niepożądanych decyzji modeli AI, które mogłyby prowadzić do naruszenia praw osób fizycznych.

Ponadto technologia „oduczania się maszyn” może wesprzeć przejrzystość działań przetwarzania danych (art. 12 RODO), umożliwiając użytkownikom lepsze zrozumienie, jak ich dane są przetwarzane i w jaki sposób mogą być usunięte z modeli AI. Dla administratorów danych staje się to cennym narzędziem, pozwalającym skuteczniej odpowiadać na żądania podmiotów danych oraz spełniać obowiązki wynikające z zasad ochrony prywatności w fazie projektowania (privacy by design) i domyślnej ochrony danych (privacy by default) zgodnie z art. 25 RODO. Podsumowując: nie wiemy, jakie nowe technologie przyniosą kolejne lata, ale jedno jest pewne: nadążanie za tymi zmianami i zapewnianie zgodności z przepisami to klucz do budowania zaufania w cyfrowym świecie.

TechSonar 2025 pokazuje, że odpowiedzialne podejście do innowacji może być fundamentem zrównoważonej przyszłości, w której technologia służy człowiekowi, a nie na

2025: Rok Rewolucji Technologicznej w Ochronie Danych -  
Przewidywania na podstawie wniosków z najnowszego raportu  
TechSonar 2025

odwrót. Niezwykle istotne jest nadążanie za zmianami poprzez edukację i budowanie świadomości zarówno wśród użytkowników, jak i w organizacjach. Kampanie społeczne, szkolenia i inwestowanie w kompetencje cyfrowe przyczyniają się do lepszego zrozumienia zagrożeń, ale także zwiększenia świadomości na temat ochrony danych. Rok 2025 może stać się rokiem, w którym odpowiedzialność za ochronę danych będzie naturalnym elementem korzystania z nowych technologii, a społeczeństwo zyska większą kontrolę nad swoją prywatnością w cyfrowym świecie.