Prywatność w AI

Katarzyna Hajduk

Politechnika Wrocławska, Wrocław, Polska
259189@student.pwr.edu.pl

Streszczenie W miarę jak sztuczna inteligencja staje się coraz bardziej zaawansowana i wszechobecna w różnych aspektach naszego życia, ludzie częściej zaczynają się martwić o swoją prywatność. Chociaż AI może znacząco poprawić nasze życie, oferując nowe możliwości, istnieje także obawa, że może być źródłem nadużyć i stanowić zagrożenie dla danych. Niniejszy raport bada, w jaki sposób rozwój AI wpływa na prywatność, identyfikuje główne wyzwania w tej dziedzinie i proponuje strategie mające na celu zwiększenie ochrony danych osobowych.

Keywords: Prywatność · Sztuczna inteligencja · Ochrona danych · RODO · AI Act

1 Wstęp

1.1 Źródło problemu

Sztuczna inteligencja, coraz bardziej obecna w codziennym życiu, od smartfonów po opiekę zdrowotną i działania nadzorcze rządów, zwraca uwagę na pilną potrzebę wprowadzenia rygorystycznych środków ochrony prywatności. Technologie AI przetwarzają znaczące ilości danych osobowych, często bez wyraźnej zgody lub pełnej świadomości użytkowników, co rodzi poważne obawy dotyczące prywatności. Potencjał AI do zbierania, analizowania i interpretowania danych osobowych na ogromną skalę wprowadza wyzwania dla ochrony prywatności, zmuszając do znalezienia równowagi między korzyściami płynącymi z innowacji a ochroną danych osobowych [6]. Rozwój AI wpłynął na transformację wielu sektorów, w tym medycyny, transportu, edukacji i rozrywki, ale rosnąca integracja AI z życiem codziennym podkreśla obawy związane z prywatnością i bezpieczeństwem danych.

1.2 Cel pracy

Poniższy raport ma na celu zbadanie wpływu sztucznej inteligencji na prywatność, zidentyfikowanie głównych wyzwań i zagrożeń dla ochrony danych osobowych oraz zaproponowanie realnych rozwiązań. Jego celem jest przegląd obecnych ram prawnych i zasugerowanie możliwych podejść w celu zapewnienia prywatności w erze sztucznej inteligencji.

2 Kluczowe pojęcia

- Sztuczna inteligencja (SI/AI): Zdolność maszyn do wykazywania ludzkich umiejętności, takich jak rozumowanie, uczenie się, planowanie i kreatywność [2].
- Prywatność: Zdolność jednostki do kontrolowania rozpowszechniania danych osobowych [4].
- Ochrona danych: Strategia i procesy bezpieczeństwa, które pomagają chronić poufne dane przed uszkodzeniem, naruszeniem zabezpieczeń i utratą [1].

3 Wpływ AI na Prywatność

3.1 AI w życiu codziennym

Technologie takie jak rozpoznawanie twarzy w monitoringu publicznym, personalizowane reklamy tworzone na podstawie danych użytkowników, czy algorytmy polecające produkty to tylko niektóre przykłady wykorzystania sztucznej inteligencji, które budzą obawy związane z prywatnością [3]. Mimo że powyższe technologie mają potencjał do poprawy jakości życia czy bezpieczeństwa użytkowników, wiążą się również z ryzykiem nadmiernego nadzoru i profilowania osób bez jasnej zgody.

3.2 Zagrożenia i wyzwania

Ryzyka związane z technologiami AI obejmują nieuprawniony dostęp do danych, wykorzystywanie danych bez zgody, a także zagrożenie wyciekiem danych w wyniku ataków cybernetycznych [9]. Złożoność i nieprzejrzystość algorytmów nierzadko sprawiają, że trudno jest zrozumieć, w jaki sposób dane są przetwarzane i na jakich założeniach się opierają. To prowadzi do etycznych dylematów związanych z sztuczną inteligencją i ochroną prywatności, podkreślając istotę autonomii, świadomej zgody i zaufania. Istotne jest, by ludzie mieli możliwość kontroli nad swoimi danymi i byli świadomi, jak są one wykorzystywane. Przejrzyste procedury wyrażania zgody umożliwiają podejmowanie świadomych decyzji dotyczących danych. Kluczowe jest również budowanie zaufania do systemów AI przez wprowadzenie zabezpieczeń gwarantujących, że działają one z poszanowaniem prywatności i praw człowieka.

4 Ochrona Prywatności w AI

4.1 Aktualnie przyjęte strategie

Aktualnie, w celu ochrony prywatności wykorzystuje się różnorodne metody, takie jak anonimizacja i pseudonimizacja danych, oraz stosowanie zasady minimalizacji danych. Te strategie są kluczowe do zmniejszenia ryzyka wycieku danych osobowych. Ich efektywność zależy jednak od ciągłego doskonalenia i zdolności

do adaptacji, aby móc skutecznie przeciwstawiać się zaawansowanym zagrożeniom i technologicznym postępom. Skuteczne stosowanie tych metod wymaga nieustannego rozwijania strategii ochrony prywatności, by móc wyprzedzać potencjalne słabości w zabezpieczeniach.

4.2 Regulacje prawne

RODO [8] Rozporządzenie Ogólne o Ochronie Danych (RODO) jest kluczowym aktem prawnym chroniącym prywatność w dobie rozwijającej się sztucznej inteligencji, które ustanawia standardy dotyczące ochrony danych osobowych. Wymaga od organizacji uzyskania wyraźnej zgody na przetwarzanie danych osobowych i zapewnia osobom większą kontrolę nad ich informacjami. RODO nakłada obowiązek legalnego, uczciwego i transparentnego przetwarzania danych, co oznacza informowanie osób, których dane są przetwarzane, w jasny i zrozumiały sposób. Przetwarzanie danych w systemach AI musi również przestrzegać zasady minimalizacji danych, ograniczając je do niezbędnego minimum i stosując odpowiednie środki bezpieczeństwa, aby zminimalizować ryzyko naruszenia prywatności.

AI Act [7] Oprócz RODO, opracowano także ustawę o sztucznej inteligencji (AI Act). AI Act wprowadza zasady zapewniające przejrzystość, odpowiedzialność oraz ochronę praw podstawowych przez wymóg oceny ryzyka i ujawnienia informacji o działaniu systemów AI. AI Act zakazuje szeregu nieetycznych zastosowań AI, w tym systemów kategoryzacji biometrycznej wykorzystujących dane wrażliwe, manipulowania ludzkim zachowaniem, tworzenia baz danych do rozpoznawania twarzy z obrazów internetowych lub CCTV i rozpoznawania emocji w pracy i edukacji.

5 Rekomendacje na przyszłość [5]

- Wprowadzenie systemów takich jak App Tracking Transparency od Apple, wymagających zgody użytkownika przed zbieraniem danych.
- Wbudowanie w przeglądarki internetowe funkcji, które automatycznie umożliwiają rezygnację ze śledzenia przez strony trzecie.
- Projektowanie systemów AI tak, aby wykluczały one wykorzystanie danych osobowych zarówno w procesach szkoleniowych, jak i w generowanych wynikach.
- Przejście od podejścia skupionego na ochronie indywidualnych praw do danych, ku kompleksowym strategiom ochrony prywatności, gdzie pośrednicy danych prowadzą negocjacje w imieniu konsumentów.

6 Podsumowanie

Podsumowując, choć sztuczna inteligencja ma ogromny potencjał do przyspieszenia rozwoju społecznego, niezbędne jest rozwiązanie problemów prywatności,

które pojawiają się wraz z jej rozwojem. Aby w pełni wykorzystać zalety AI, zachowując przy tym ochronę prywatności, kluczowe będzie zastosowanie zrównoważonego podejścia, które połączy regulacje prawne, postępy technologiczne oraz podnoszenie świadomości społecznej.

Literatura

1. Czym jest ochrona danych? Microsoft. Dostęp: Kwiecień 08, 2024.
2. Sztuczna inteligencja: co to jest i jakie ma zastosowania? Parlament Europejski, Wrzesień 2020. Dostęp: Kwiecień 08, 2024.
3. C.F. Kerry. Protecting privacy in an ai-driven world, Luty 2020.
4. E. Kuczma. *Generalny inspektor ochrony danych osobowych jako organ ochrony prawa do prywatności*. PhD thesis, Uniwersytet w Białymstoku, Białystok, Polska, 2016.
5. K. Miller. Privacy in an ai era: How do we protect our personal information?, Marzec 2024.
6. B. Murdoch. Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics*, 22:122, 2021.
7. Redakcja. Osiągnięto porozumienie w sprawie ai act. GDPR, Grudzień 2023. Dostęp: Kwiecień 08, 2024.
8. K. Smolarek-Wietrzychowska. Czy ochrona prywatności i sztuczna inteligencja idą w parze? Deloitte Polska, Styczeń 2021.
9. M. van Rijmenam and CSP. Privacy in the age of ai: Risks, challenges and solutions, Luty 2023.