ROCZNIKI NAUK PRAWNYCH
Tom XXXV, numer 1 – 2025
DOI: https://doi.org/10.18290/rnp25351.2

PATRYK PIENIĄŻEK
Uniwersytet im. Adama Mickiewicza w Poznaniu
patryk.pieniazek@amu.edu.pl
ORCID: https://orcid.org/0000-0002-3015-337X

SZTUCZNA INTELIGENCJA I OCHRONA DANYCH OSOBOWYCH. ZARYS PROBLEMU

ARTIFICIAL INTELLIGENCE AND PERSONAL DATA PROTECTION. AN OUTLINE OF THE PROBLEM

Abstract. The aim of this article is the analyze the risks to the protection of personal data arising from their processing by AI systems and to identify solutions to minimize these risks. The study uses a dogmatic-legal method, based on an analysis of existing regulations and literature on the subject. The results of the study indicate significant gaps in the regulations and the need to implement protective measures, such as data anonymization and algorithm audits. The findings can form the basis for further research and legislative action on data protection in AI systems.

Keywords: artificial intelligence; data protection; privacy; recommendations; risks

WPROWADZENIE

W ostatnich latach trwa dyskusja na temat relacji zachodzących pomiędzy prawem ochrony danych osobowych a sztuczną inteligencją (dalej: AI). Z pewnością pojawia się wiele wątpliwości dotyczących przetwarzania danych osobowych przez systemy AI, które wynikają z różnic w celach i metodach działania obu tych obszarów. Przykładowo AI będzie wymagała dużej ilości danych osobowych do trenowania swoich modeli, czy chociażby do udoskonalania algorytmów, co wiązać się będzie z gromadzeniem danych osobowych z różnych źródeł, w różnych miejscach. Z kolei przepisy zawarte w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO)[1] wymagają minimalizacji danych osobowych oraz przetwarzania ich wyłącznie w jasno określonych i zgodnych z prawem celach. Stanowić to może ograniczenie dla firm i organizacji, które z jednej strony muszą spełniać wysokie standardy dotyczące ochrony danych osobowych, a z drugiej strony wykorzystywać możliwości oferowane przez AI.

Celem niniejszego artykułu jest omówienie potencjalnych zagrożeń dla ochrony danych osobowych wynikających z ich przetwarzania przez systemy AI, a także zaproponowanie rozwiązań, których wdrożenie przez dostawców systemów AI może uchronić przed ewentualnymi zagrożeniami. W ramach niniejszego artykułu została wykorzystana metoda dogmatycznoprawna: przeprowadzono analizę istniejących uregulowań prawnych poprzez odwoływanie się do piśmiennictwa.

1. POJĘCIE I RODZAJE SYSTEMÓW SZTUCZNEJ INTELIGENCJI

W doktrynie wielokrotnie podejmowano próby zdefiniowania pojęcia „system AI", przez co w literaturze przedmiotu pojawia się mnogość definicji odnoszących się do tego zagadnienia. Zdaniem wielu teoretyków prawa, definicja przyjęta na gruncie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (dalej: AI Act)[2] miała oznaczać moment przełomowy, niemniej jednak również w tym przypadku pojawiają się liczne wątpliwości.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze zm.).

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).

W literaturze przedmiotu najczęściej używanymi definicjami, które nawiązują do systemów AI, są te, które zostały opracowane przez naukowców z Cambridge oraz Stanford. N.J. Nilsson (Cambridge) wskazuje, że

> sztuczna inteligencja to działanie mające na celu uczynienie maszyn inteligentnymi, a inteligencja to cecha, która umożliwia jednostce prawidłowe i przewidywalne funkcjonowanie w jej otoczeniu[3].

Definicja ta obejmuje różnorodne zdolności systemu AI, a mianowicie: uczenie się, rozumienie języka naturalnego, zdolność do identyfikowania wzorców i regularności danych, a także rozwiązywanie problemów. Te umiejętności powodują, że maszyny stają się inteligentne na wzór człowieka, przez co skutecznie mogą wykonywać określone zadania i spełniać wyznaczone cele, co powoduje, że działają w sposób spójny i przewidywalny w zmieniającym się środowisku.

Następnie warto przytoczyć definicje, którą stworzyli naukowcy ze Stanford, którzy przyjęli, że

> sztuczna inteligencja to nauka i zestaw technologii obliczeniowych, które są inspirowane – choć zazwyczaj działają inaczej – ludzkim układem nerwowym w zakresie, w jakim umożliwia on odczuwanie, uczenie się, rozumowanie i podejmowanie działań[4].

W ramach tego zdefiniowania uwaga została zwrócona na kwestie inspiracji ludzkim mózgiem, który jest zdolny do odczuwania, uczenia się, rozumowania, a następnie podejmowania działań. Kluczowe inspirowane aspekty obejmują: sieci neuronowe, procesy uczenia się oraz zdolność do adaptacji na podstawie doświadczeń. Pomimo to, chodź inspiracja ludzkim układem nerwowym jest wyraźna, AI może też działać w inny sposób. Przykładowo, jest w stanie wykorzystywać m.in. modele matematyczne do przetwarzania różnego rodzaju danych oraz na ich podstawie podejmować decyzje, których jednym z problemów może być dyskryminacja. Ponadto w porównaniu do ludzkiego mózgu AI może przetwarzać ogromne ilości danych w krótkim czasie,

[3] N.J. NILSSON, *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge 2010.

[4] P. STONE ET AL., *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, Stanford 2016, https://ai100.stanford.edu/2016-report/executive-summary [dostęp: 26.07.2024].

dzięki mocy współczesnych komputerów. Zatem należy wskazać, że AI to złożona i wieloaspektowa dziedzina, która mimo inspiracji biologicznym układem nerwowym rozwijać się będzie na podstawie unikalnych zasad oraz technologii obliczeniowych, dając warunki do tworzenia zaawansowanych systemów zdolnych do odczuwania, uczenia się, rozumowania i podejmowania decyzji.

12 lipca 2024 r. w Dzienniku Urzędowym Komisji Europejskiej został opublikowany AI Act – rozporządzenie, którego celem jest zapewnienie harmonizacji dotyczącej wykorzystywania systemów AI w Unii Europejskiej. Niniejszy akt reguluje m.in. kwestie dotyczące zakazu wykorzystywania systemów AI, czyli tzw. zakazane praktyki (art. 5), gdzie klasyfikuje systemy AI pod kątem potencjalnego zagrożenia dla zdrowia, życia, bezpieczeństwa ludzi i ich praw podstawowych[5]. Co jednak istotne, prawodawca unijny zdecydował się również na zdefiniowanie pojęcia systemu AI, które stanowi pierwszą definicję legalną tegoż sytemu. Art. 3 pkt 1 AI Act wskazuje, że

> 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.

Mając na uwadze niniejszą definicję należy wskazać, że system AI oparty jest na maszynie, która może wykazywać różny poziom autonomii, czyli zdolność do samodzielnego podejmowania decyzji i wykonywania działań bez bezpośredniego nadzoru człowieka. Jednak nie należy zapominać, że to właśnie człowiekowi (dostawcy systemu AI) będzie przypisywana odpowiedzialność za ewentualne naruszenia. Następną cechą systemu AI będzie zdolność adaptacyjna oznaczająca możliwość uczenia się na podstawie interakcji, jak i również możliwość poprawiania z czasem swoich działań. Jednak nie należy zapominać, że pomimo korzyści wynikających z autonomii systemów AI, tj. zwiększenie efektywności, redukcji błędów czy możliwości działania w trudnych i niebezpiecznych warunkach, może nieść za sobą wyzwania związane z bezpieczeństwem, odpowiedzialnością za decyzje podejmowane przez AI oraz z ich wpływem tychże systemów na społeczeństwo.

Warto jednak zwrócić uwagę na ogólność, a zarazem uniwersalność tejże definicji. Początkowo, na etapie projektowania była ona krytykowana przez

[5] D. FLISAK, *Akt w sprawie sztucznej inteligencji*, LEX/el. 2024.

przedstawicieli doktryny, jednak przyjęcie tego sposobu zdefiniowania jest celowym i przemyślanym zabiegiem, mającym na celu objęcie najszerszego zakresu technologii, a zarazem zapewnienie elastyczności i adaptacji regulacji do przyszłych zmian technologicznych. Należy zauważyć, że AI bez wątpienia rozwija się bardzo dynamicznie. Tworzenie szczegółowej definicji mogłoby spowodować ograniczenia przedmiotowe w obliczu nowych innowacji, a przyjęcie tego rozwiązania pozwala na objęcie wszystkich technologii oraz wykluczenie ciągłych zmian regulacyjnych.

Po zidentyfikowaniu kluczowych cech i funkcji systemu AI należy również wskazać jego rodzaje. F.A. Batarseh wyróżnia osiem podstawowych typów systemów AI, tj.: uczenie maszynowe, sieci neuronowe, algorytmy genetyczne, przetwarzanie języka naturalnego (NLP), systemy oparte na wiedzy (KBS), widzenie komputerowe (*Computer Vision*), robotyka oraz nauka o danych i zaawansowana analityka[6].

W ostatnich latach zauważamy dynamiczny rozwój uczenia maszynowego w kontekście analizy danych i obliczeń. Sam ten system umożliwia komputerom automatyczne uczenie się i doskonalenie na podstawie doświadczenia, bez konieczności wykorzystania specjalnego oprogramowania[7]. Co jednak istotne, jest jednym z fundamentalnych typów sztucznej inteligencji, który został uregulowany w AI Act.

Kolejnym typem AI są sieci neuronowe, które działają w sposób inspirujący się ludzkim mózgiem i systemem nerwowym. Wykorzystując te technologie, komputery mogą stymulować ludzkie zdolności poznawcze, takie jak rozumienie abstrakcyjnych pojęć, języków czy analizowanie znaczenia obrazów. Pozwala to na bardziej zaawansowaną interakcję z maszynami i przetwarzanie złożonych informacji w sposób przypominający ludzkie myślenie[8]. Chociaż nie są bezpośrednio objęte regulacjami AI Act, ich rozwój może stwarzać nowe wyzwania etyczne.

W kontekście algorytmów genetycznych pełnią rolę metod przeszukiwania, które bazują na zasadach doboru naturalnego i dziedziczenia. Wykorzystują ewolucyjną zasadę przetrwania najlepiej przystosowanych jednostek[9]. Algorytmy genetyczne są wykorzystywane w różnych dziedzinach ze względu na

[6] F.A. BATARSEH, *Artificial Intelligence*, [in:] *Encyclopedia of Big Data*, red. L.A. Schintler, C.L. McNeely, Cham 2022, s. 45-48.

[7] I.H. SARKER, *Machine Learning: Algorithms, Real-World Applications and Research Directions*, „SN Compututer Science" 2 (2021), artykuł 160, s. 159.

[8] O. KRAMER, *Machine Learning for Evolution Strategies*, Cham 2016.

[9] R. WINICZENKO, *Algorytmy genetyczne i ich zastosowania*, „Postępy Techniki Przetwórstwa Spożywczego" 2008, s. 107-110.

ich zdolność do znajdowania rozwiązań optymalnych, np. w inżynierii czy projektowaniu.

Przechodząc do przetwarzania języka naturalnego (NLP) należy wskazać, że jego podstawową funkcją jest zdolność do rozumienia i przetwarzania ludzkiego języka przez komputery. Dzięki dynamicznemu rozwojowi uczenia maszynowego NLP stało się jedną z kluczowych dziedzin AI, obejmującą także lingwistykę, informatykę oraz technologie informacyjne. NLP umożliwia maszynom analizowanie, interpretowanie i generowanie języka ludzkiego w sposób zbliżony do naturalnej komunikacji międzyludzkiej. Dzięki temu technologia ta znajduje szerokie zastosowanie w automatyzacji eksploracji danych, zaawansowanej analizie treści oraz optymalizacji procesów biznesowych. Przetwarzanie języka naturalnego wspomaga m.in. wyszukiwanie informacji, tłumaczenia maszynowe, analizę sentymentu, chatboty oraz systemy rekomendacyjne, usprawniając interakcję człowieka z technologią i poprawiając efektywność pracy w różnych sektorach gospodarki[10]. Jednak pomimo wielu korzyści jakie NLP oferuje, pojawiają się również obawy o prywatność i bezpieczeństwo danych osobowych, ze względu na wymagania dostępu do dużych ilości danych tekstowych, czego dowodem jest fakt, że chatboty mogą gromadzić i przechowywać dane wrażliwe bez zgody użytkowników.

Kolejno należy wspomnieć o systemach opartych na wiedzy (KBS), które działają poprzez wykorzystanie istniejącej bazy wiedzy do podejmowania decyzji. Co jednak ciekawe, KBS może być wyposażony w mechanizmy uczenia maszynowego, przez co będzie w stanie automatycznie dokonywać aktualizacji i gromadzić nowe dane. Choć zarówno same systemy KBS nie zostały bezpośrednio wymienione w AI Act, mogą one jednak podlegać pewnym regulacjom – szczególnie w przypadkach, gdy wpływają na istotne aspekty życia społecznego.

Istotnym rodzajem AI jest również widzenie komputerowe (*Computer Vision*), które dąży do nadania komputerom zdolności widzenia trójwymiarowego. W wizji komputerowej obrazy otaczającej nas rzeczywistości są interpretowane przez systemy komputerowe, poprzez analizę zawartości obrazów rzeczywistych obiektów przesyłanych do komputera[11]. Ciekawym przykładem zastosowania tej technologii są autonomiczne pojazdy. Samojezdne samochody używają kamer i algorytmów widzenia komputerowego do rozpoznawania znaków drogowych, pieszych, innych pojazdów i przeszkód na drodze.

[10] R. EGGER, E. GOKCE, *Natural Language Processing (NLP): An Introduction*, [w:] *Applied Data Science in Tourism. Tourism on the Verge*, red. R. Egger, Cham 2022, s. 307-308.

[11] A. KACZMAREK, *Widzenie komputerowe oparte na mnogości widoków*, „Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej" 36 (2013), s. 85-88.

Jednym z intrygujących tematów we współczesnych badaniach naukowych jest tworzenie robotów na wzór ludzi. Celem robotyki jest projektowanie, budowanie i operowanie maszynami. Same roboty są zdolne do wykonywania zadań automatycznie, często z duża precyzją i w warunkach, które mogą być niebezpieczne lub trudne do pokonania dla ludzi[12]. Niniejsza technologia znajduje zastosowanie w wielu dziedzinach, w tym w przemyśle (roboty przemysłowe), medycynie (roboty chirurgiczne), wojsku, eksploracji kosmicznej. Pomimo postępów w tej dziedzinie AI, nadal pojawiają się kwestie trudne do rozwiązania. Roboty, zaprojektowane na podobieństwo ludzi, mają nawet zdolność do popełnienia samobójstwa. To Korea Południowa jest przykładem kraju, który doświadczył takich okoliczności. Robot, którego praca rozpoczęła się w sierpniu 2023 r., był jednym z pierwszych w kraju robotem-urzędnikiem, którego wykorzystywano do pracy w administracji publicznej. W okolicznościach, które nie zostały wyjaśnione, spadł ze schodów i uległ ciężkiemu uszkodzeniu. Dlatego, pomimo że robotyka stanowi spektakularną dziedzinę AI, wymaga ona rozważenia etycznego i prawnego.

Ostatnim rodzajem AI, który zostanie omówiony w ramach niniejszego artykułu, jest nauka o danych i zaawansowana analityka. Dziedziny te związane są bezpośrednio z analizą i interpretacją dużych zbiorów danych m.in. w celu wspierania procesów decyzyjnych. Ponadto nauka o danych pozwala na lepsze zrozumienie i wykorzystanie informacji do podejmowania bardziej świadomych decyzji. Jej zastosowanie możemy zauważyć w różnych obszarach działalności, tj.: biznesie, opiece zdrowotnej, marketingu, a także w sektorze publicznym.

W ujęciu końcowym definicja systemów AI, która została przyjęta w ramach AI Act, pomimo swojej ogólności, stanowi elastyczne rozwiązanie, które ogranicza się do konkretnych typów systemów. Taka konstrukcja prawna pozostawia możliwość uwzględnienia przyszłych technologii, umożliwiając dostosowywanie się do dynamicznego obszaru AI. Dzięki takiemu rozwiązaniu regulacje zawarte w AI Act zachowują swoją skuteczność i aktualność, pozwalając na dostosowanie prawa do zmieniającego się ekosystemu AI.

[12] C. ZIELIŃSKI, *Robotyka: techniki, funkcje, rola społeczna Cz. 1. Techniczne podstawy inteligencji i bezpieczeństwa robotów*, „Pomiary Automatyka Robotyka" 26 (2022), nr 4, s. 5-26.

2. PRAWNE ZAGROŻENIA DLA OCHRONY DANYCH OSOBOWYCH W KONTEKŚCIE ICH PRZETWARZANIA PRZEZ SYSTEMY AI

W związku z coraz powszechniejszym wykorzystywaniem AI w różnych dziedzinach pojawia się wiele wątpliwości dotyczących przetwarzania danych osobowych przez systemy AI, które jak już wspomniano we wstępie, wynikają z różnic w celach i metodach działania obu tych obszarów. Główne wyzwania wynikają przede wszystkim z realizacji zasad dotyczących przetwarzania danych osobowych, a także zaspokojenia praw jednostek do dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania czy też prawa do sprzeciwu.

Istotne jest aby zaznaczyć, że AI Act w swoich regulacjach nie będzie odnosił się do ochrony danych osobowych. Jego ustanowienie ma zupełnie inny zakres przedmiotowy – dotyczy tworzenia, rozwoju i wykorzystywania systemów AI, które masowo przetwarzają dane osobowe, w tym dane wrażliwe. Motyw 10 zawarty w preambule AI Act określa, że RODO będzie niezmiennie podstawowym aktem regulującym ochronę danych osobowych w UE. Implikuje to, że wszelkie działania związane z wykorzystaniem danych osobowych w systemach AI muszą być jednocześnie zgodne z normami określonymi w AI Act oraz RODO.

Największe obawy pojawiają się w przypadku realizacji zasady dotyczącej minimalizacji danych, która została ustanowiona w art. 5 ust. 1 lit. c RODO. Wskazuje ona na zapewnienie przy przetwarzaniu danych osobowych ograniczonej do minimum ilości i treści danych osobowych adekwatnie do tego, co niezbędne przy przetwarzaniu[13]. Warto zaznaczyć, że to administrator danych osobowych w myśl art. 25 ust. 2 RODO jest odpowiedzialny za wprowadzanie odpowiednich środków, które pozwolą na przetwarzanie danych osobowych wyłącznie w rozumieniu sprecyzowanego celu, dla którego zostały one zgromadzone. Co istotne, AI będzie wymagało dużych ilości danych (imię, nazwisko, dane kontaktowe), a także tych, które prawodawca unijny ujął w kategorii szczególnych danych osobowych (art. 9 ust. 1 RODO), obejmujących m.in. dane dotyczące zdrowia, przekonań religijnych czy pochodzenia etnicznego. Niemniej jednak konieczność przetwarzania tak szerokiego zakresu danych osobowych przez systemy AI nie jest uniwersalna i zależy od konkretnego zastosowania technologii. Przykładowo, AI wykorzystywana w personalizacji usług cyfrowych, takich jak rekomendacje treści w serwisach

[13] M. KRZYSZTOFEK, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.

streamingowych czy automatyczne dostosowywanie ofert zakupowych, opiera się głównie na analizie preferencji użytkowników, a nie na ich wrażliwych danych osobowych. Z kolei w systemach AI stosowanych w medycynie, np. w diagnostyce chorób na podstawie obrazowania medycznego czy analizy historii leczenia, przetwarzanie danych zdrowotnych jest niezbędne.

W kontekście ochrony danych osobowych często wskazuje się, że dobrym rozwiązaniem mogłoby być zastosowanie procesu anonimizacji danych jako formy zabezpieczenia danych osobowych[14]. Jednak warto zauważyć, że pojęcie „anonimizacja" nie posiada definicji legalnej, co może prowadzić do wątpliwości w zakresie jej skuteczności i zgodności z obowiązującymi regulacjami. Przyjmuje się, że stanowić ona będzie o instrumencie w zakresie ochrony prywatności, który ma na celu trwałe i nieodwracalne usunięcie powiązań między danymi osobowymi a osobami, których one dotyczą. Jak wskazuje treść motywu 52 dyrektywy 2019/2014[15], informacje anonimowe nie będą odnosiły się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, gdyż cel tego procesu służyć ma temu, by dane osoby były przedstawiane w sposób, który zapewni zachowanie pełnej anonimowości. Jednak i w tym przypadku zastosowanie anonimizacji może spowodować ograniczenie działania AI, które często wymaga dostępu do szczegółowych danych, by skutecznie działać, co może kolidować z wymaganiami dotyczącymi prywatności.

Kolejnym przypadkiem sporu, który może wystąpić podczas przetwarzania danych osobowych przez systemy AI jest możliwość niezgodnego z prawem wykorzystania danych. Zasada określona w art. 5 ust. 1 lit. a RODO stanowi o zgodności z prawem, rzetelności i przejrzystości przetwarzania danych osobowych. Prawodawca unijny wskazuje, że proces przetwarzania danych osobowych powinien oparty być na obowiązujących przepisach prawa, tak by zapewnić rzetelność i przejrzystość dla osoby, której dane dotyczą. Bez wątpienia należy wskazać, że systemy AI często wykorzystują duże ilości danych osobowych, takich jak: dane dotyczące tożsamości, preferencji, nawyków zakupowych i zdrowotnych. Istnieje ryzyko, że dane te będą wykorzystywane niezgodnie z prawem lub wbrew zamiarom użytkownika, co może prowadzić do naruszenia jego prywatności. Dodatkowo, zanonimizowane dane mogą zostać przekształcone w dane osobowe, w tym dane szczególnych kategorii.

[14] M. GUMULARZ, T. IZODORCZYK (red.), *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, Warszawa 2021, s. 110-111.

[15] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L z 2019 r. Nr 172, s. 56).

Rozpatrywany problem będzie odnosił się również do kolejnej zasady, a mianowicie ograniczonego celu (art. 5 ust. 1 lit. b RODO), który wyznacza, że przetwarzanie danych osobowych powinno nastąpić jedynie w konkretnych oraz prawnie uzasadnionych celach, za zgodą osoby, której dane dotyczą. To kolejno będzie powiązane z obowiązkiem informacyjnym dostawcy systemu AI, który może jednocześnie pełnić funkcję administratora danych, w przypadku gdy decyduje o celach i środkach przetwarzania tych danych. W odniesieniu do tego, dostawca systemu AI w razie wystąpienia naruszenia ochrony danych osobowych jest zobowiązany dowieść, że dane osobowe są przetwarzane zgodnie z prawem oraz że przestrzega spoczywających na nim obowiązków wynikających z AI Act i RODO. Nie należy zapomnieć, iż sama zasada rozliczalności ma zastosowanie podczas całego przebiegu procesu przetwarzania danych osobowych, a nie tylko na etapie wstępnym, jakim jest gromadzenie danych.

Na zakończenie istotne jest odniesienie do praw osób, których dane są wykorzystywane, gdyż i w tym zakresie pojawiają się kolejne wyzwania, które będą wynikały ze specyfiki działania systemów AI. Może być to następstwem braku transparentności, zwłaszcza w przypadku algorytmów opartych na uczeniu maszynowym, które są trudne do zrozumienia i interpretacji nawet przez samych twórców. W wyniku tego dochodzi do tzw. efektu czarnej skrzynki, czyli pojawiają się trudności w interpretacji, w jaki sposób dane są przetwarzane i jakie decyzje są podejmowane. Najczęstsze wątpliwości pojawiają się w przypadku stronniczości algorytmów i możliwości podejmowania przez nie dyskryminujących decyzji. Bezspornie jednym z najważniejszych problemów etycznych związanych z AI jest jej zdolność do dyskryminacji łączącej się z utrwaleniem uprzedzeń i pogłębieniem występujących już nierówności.

Już w preambule prawodawca unijny odnosi się do tej kwestii, wskazując m.in. w motywie 31 na zjawisko *scoringu* społecznego, który jest powszechnie obowiązujący w Chinach[16]. System ten polega na monitorowaniu i ocenianiu zachowań obywateli na podstawie wielu danych dotyczących ich zachowań społecznych w różnych kontekstach, a także na podstawie znanych, wywnioskowanych lub przewidywanych cech osobistych lub cech osobowości w określonych okresach. Co jednak ważne, niniejsze rozwiązanie zostało skrytykowane przez prawodawcę unijnego na gruncie AI Act i w ten sposób stanowi jedną z niedozwolonych praktyk.

[16] M. GÓRSKI, *Chiński system kredytu społecznego. Antecedencje, konteksty i konsekwencje*, [w:] *Prawo sztucznej inteligencji i nowych technologii 3*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2023, LEX/el.

Pisząc o dyskryminacji, wydawać się może, że nie należy wiązać tej kwestii z prywatnością, ponieważ dotyczy problemów społecznych występujących bez gromadzenia i wykorzystywania danych osobowych. Jednak nie sposób pominąć informacji, że dyskryminacja będzie dotyczyła cech ludzkich m.in. koloru skóry, tożsamości seksualnej czy też pochodzenia narodowego, które to niezaprzeczalnie podlegają ochronie jako dane osobowe.

3. REKOMENDACJE

Twórcy systemów AI, aby sprostać powyższym wyzwaniom i zapewnić ochronę danych osobowych, są zobowiązani do zrozumienia znaczenia trudności, które występują już na etapie ich projektowania. Systemy AI powinny od samego początku być projektowane na podstawie regulacji dotyczących ochrony danych osobowych. Istotne jest zapewnienie osobom, których dane są przetwarzane, prawa do dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania czy też prawa do sprzeciwu. Odnosić się to będzie jednocześnie do świadomości, że dany proces odbywa się przy działaniu AI, a jednostki mają prawo do kwestionowania decyzji, które zapadają w ramach tych systemów, w łatwy i dostępny sposób.

Dodatkowo systemy AI powinny być projektowane i implementowane na podstawie minimalizacji danych, ograniczenia celu, dokładności, integralności i poufności, które są niezbędne do prawidłowego wdrożenia AI. Można domniemywać, że w kontekście AI nie ma miejsca na zasadę minimalizacji danych, jednakże dostawcy będący administratorami danych osobowych mają obowiązek ograniczyć gromadzenie i inne formy przetwarzania danych osobowych do tego, co jest niezbędne do celów przetwarzania, unikając masowego przetwarzania tych danych. Obowiązek ten powinien objąć cały cykl systemu, łącznie z fazami testowania, akceptacji i dopuszczenia do produkcji. Nie należy gromadzić i przetwarzać danych osobowych w sposób masowy, a w przypadku danych szczególnej kategorii przetwarzanie powinno zachodzić pod warunkiem stosowania odpowiednich zabezpieczeń w zakresie podstawowych praw i wolności osób fizycznych określonych w art. 10 ust. 5 AI Act. Istotna jest w tym również edukacja osób obsługujących systemy AI dotycząca dostępnych procedur technicznych mających na celu zminimalizowanie wykorzystania danych osobowych oraz uwzględniania ich na wszystkich etapach opracowywania.

W kontekście integralności danych oznacza to, że dane nie powinny być modyfikowane, usuwane ani uszkadzane w sposób nieautoryzowany, co zapewni ich wiarygodność i użyteczność. Integralność danych jest kluczowym aspektem bezpieczeństwa informacji oraz zarządzania danymi. Niedopuszczalne jest, aby procesy te zachodziły bez odpowiednich środków technicznych, a tym samym systemy AI dopuszczały do ataków cybernetycznych czy chociażby niekontrolowanych błędów ludzkich. Jednostki muszą mieć zagwarantowane, że ich dane osobowe są gromadzone i przechowywane zgodnie z wymogami bezpieczeństwa i ochrony prywatności, a także powinny posiadać szeroki zakres uprawnień do zarządzania i kontrolowania swoich danych. Należy jednak zauważyć, że w przypadku, gdy administratorem danych jest organ władzy publicznej przetwarzający dane w związku z realizacją zadań publicznych, zakres tych uprawnień może podlegać pewnym ograniczeniom. W takich sytuacjach – mimo spełnienia wszystkich wymogów dotyczących ochrony i bezpieczeństwa danych – nie zawsze będzie możliwe pełne zarządzanie danymi, na przykład poprzez żądanie ich usunięcia lub całkowitego zaprzestania ich przetwarzania, jeśli wynika to z obowiązujących przepisów prawa.

Ostatnią kwestią, jaka powinna być rekomendowana, to odpowiednie polityki prywatności danych przetwarzanych przez systemy AI uwzględniające zasadę przejrzystości działania tychże systemów. Polityka prywatności to zbiór zasad, procedur i praktyk, które określają sposób, w jaki administrator danych gromadzi, przechowuje, używa i udostępnia dane osobowe użytkowników. Jest to dokument opisujący zasady ochrony prywatności oraz sposób postępowania w zakresie danych osobowych, mający na celu zapewnienie bezpieczeństwa i prywatności danych, zgodnie z obowiązującymi przepisami prawnymi i normami etycznymi. Polityka prywatności informuje użytkowników o ich prawach, o celach zbierania danych, sposobach ich przetwarzania oraz udostępniania, a także zapewnia wytyczne dotyczące sposobu, w jaki osoby fizyczne mogą zarządzać swoimi danymi osobowymi. Niniejsze rozwiązanie może pomóc w ograniczeniu ryzyka dla osób fizycznych i zapewnieniu zgodności z wymogami AI Act i RODO, w szczególności poprzez dostarczanie szczegółowych informacji na temat tego, w jaki sposób, kiedy i w jakim celu przetwarzane są dane osobowe w ramach systemów AI.

PODSUMOWANIE

W świetle przeprowadzonej analizy należy stwierdzić, że może występować konflikt między AI a ochroną danych osobowych. Pojawia się wiele obszarów, na które należy zwrócić szczególną uwagę podczas przetwarzania danych osobowych przez systemy AI. Problem ten może wynikać nie tyle z odmienności regulacji obu dziedzin – co samo w sobie jest uzasadnione – lecz raczej z faktu, że przepisy dotyczące AI i ochrony danych osobowych nie są w pełni do siebie dostosowane. Kluczowe elementy, takie jak zasada minimalizacji danych, prawo do bycia zapomnianym oraz wymóg uzyskania świadomej zgody na przetwarzanie danych, które mają na celu ochronę praw osób fizycznych, stawiają przed systemami AI oraz ich dostawcami duże wyzwania. Pomimo tego, wdrożenie w praktyce rekomendacji organów nadzorczych zapewni zwiększenie poziomu bezpieczeństwa i ochrony prywatności danych osobowych przetwarzanych przez systemy AI, a także znacząco obniży ryzyko nałożenia administracyjnych kar pieniężnych za naruszenia przepisów o ochronie danych osobowych.

BIBILIOGRAFIA

BATARSEH Feras A., *Artificial Intelligence*, [w:] *Encyclopedia of Big Data*, red. L.A. Schintler, C.L. McNeely, Cham 2022, s. 45-48.

EGGER R., GOKCE E., *Natural Language Processing (NLP)*, [w:] *Applied Data Science in Tourism. Tourism on the Verge*, red. R. Egger, Cham 2022, s. 307-334.

FLISAK Damian, *Akt w sprawie sztucznej inteligencji*, LEX/el. 2024.

GÓRSKI Marcin, *Chiński system kredytu społecznego. Antecedencje, konteksty i konsekwencje*, [w:] *Prawo sztucznej inteligencji i nowych technologii 3*, red. B. Fischer, A. Pązik, Świerczyński M., Warszawa 2023, LEX/el.

GUMULARZ Mirosław, IZODORCZYK Tomasz (red.), *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, Warszawa 2021.

KACZMAREK Adam, *Widzenie komputerowe oparte na mnogości widoków*, „Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej" 36 (2013), s. 85-88.

KRAMER Oliver, *Machine Learning for Evolution Strategies*, Cham 2016.

KRZYSZTOFEK Mariusz, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.

NILSSON Nils J., *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge 2010.

SARKER Iqbal H., *Machine Learning: Algorithms, Real-World Applications and Research Directions*, „SN Compututer Science" 2 (2021), artykuł 160.

STONE Peter et al., *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, Stanford 2016.

WINICZENKO Radosław, *Algorytmy genetyczne i ich zastosowania*, „Postępy Techniki Przetwórstwa Spożywczego" 2008, s. 107-110.

ZIELIŃSKI Cezary, *Robotyka: techniki, funkcje, rola społeczna Cz. 1. Techniczne podstawy inteligencji i bezpieczeństwa robotów*, „Pomiary Automatyka Robotyka" 26 (2022), nr 4, s. 5-26.

SZTUCZNA INTELIGENCJA I OCHRONA DANYCH OSOBOWYCH ZARYS PROBLEMU

STRESZCZENIE

W ostatnich latach trwa dyskusja na temat relacji zachodzących pomiędzy prawem ochrony danych osobowych a sztuczną inteligencją. Z pewnością pojawia się wiele wątpliwości dotyczących przetwarzania danych osobowych przez systemy AI, które wynikają z różnic w celach i metodach działania obu tych obszarów. W ramach niniejszego artykułu zostały przedstawione potencjalne zagrożenia dla ochrony danych osobowych wynikających z ich przetwarzania przez systemy AI, a także zaproponowane rozwiązania, których wdrożenie przez dostawców systemów AI może uchronić przed owymi zagrożeniami.

Słowa kluczowe: ochrona danych osobowych; prywatność; rekomendacje; sztuczna inteligencja; zagrożenia