ACTA IURIDICA RESOVIENSIA Nr 1(44)/2024

ISSN 2720-0574 DOI: 10.15584/actaires.2024.1.7

Gabriel Z. Kolasa

Uniwersytet Wrocławski
ORCID: 0009-0003-4591-6178

SZTUCZNA INTELIGENCJA (AI) VS. OCHRONA DANYCH OSOBOWYCH (RODO) – JAK ZAPEWNIĆ ZGODNOŚĆ ROZWIĄZAŃ AI Z PODSTAWOWYMI MECHANIZMAMI SYSTEMU OCHRONY DANYCH OSOBOWYCH W RAMACH UNII EUROPEJSKIEJ?

Wprowadzenie

Sztuczna inteligencja (a co najmniej systemy tak określane w odbiorze publicznym) szturmem weszła do powszechnego używania i coraz więcej można zauważyć zastosowań masowego przetwarzania danych za jej pomocą, w tym także danych osobowych. Wraz z rozwojem nowych technologii pojawiają się kolejne wyzwania związane z zapewnieniem jednolitej ochrony danych osobowych przewidzianej w europejskim rozporządzeniu o ochronie danych osobowych[1]. Jednym z często podnoszonych problemów jest zapewnienie zgodności rozwiązań AI z prawami podstawowymi gwarantowanymi w ramach Unii Europejskiej. W tym artykule pragnę przyjrzeć się zjawisku przetwarzania danych przez rozwiązania oparte na sztucznej inteligencji, przy prawie nieograniczonej ilości danych, oraz jakie może nieść to konsekwencje dla aktualnego systemu ochrony danych osobowych.

Sztuczna inteligencja – czy faktycznie jest to tak nowe?

Choć samo pojęcie *sztuczna inteligencja* (*artificial intelligence* – AI) dopiero od niedawna trafiło do zbiorowej świadomości coraz liczniejszych społeczno-

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, s. 1 ze zm.), dalej: RODO.

ści i opuściło już kuluary branży informatycznej, to technologia ta stosowana jest już od dawna. Implementowanie możliwości „uczenia się" algorytmów poprzez interpretację danych, zauważanie schematów czy przewidywanie zdarzeń lub zachowań pozwalało na utworzenie wielu potrzebnych i użytecznych narzędzi, z których korzysta niezliczona liczba osób, nawet o tym nie wiedząc. Przykładem zastosowania, w którym za cichego bohatera można uważać funkcjonalności tego rozwiązania, na pewno są funkcje usprawniające korzystanie ze skrzynek e-mail, oparte na analizie metadanych otrzymywanych wiadomości lub ich treści – np. filtry antyspamowe[2], czy systemy pozwalające na klasyfikacje treści – dziś wbudowane w rozwiązania dostępne ogólnie, jak np. algorytm Gmail dzielący wiadomości na różne kategorie, stosując do tego metody uczenia maszynowego[3].

Niektóre rozwiązania stały się na tyle powszechne, że nie zwracają już uwagi użytkowników internetu i są odbierane jako naturalna część pejzażu przeglądanych witryn w postaci reklam internetowych. Na tym polu wyścig reklamodawców i odbiorców treści marketingowych jest wspomagany przez rozwiązania pozwalające na dopasowanie wyświetlanych treści do profilu osoby przeglądającej treści. Decyduje o tym profil danego użytkownika sieci, do którego informacje są zbierane poprzez ciąg algorytmów i narzędzi, interpretowany na bieżąco ślad plików cookie oraz metadanych zbieranych po stronie mechanizmów zapełniających przestrzenie reklamowe[4]. Ten ślad pozwala dostawcom systemów reklamy internetowej na stosowanie odpowiednich algorytmów, które wspierane poprzez uczenie maszynowe[5] są w stanie jeszcze precyzyjniej docierać do osób wpisujących się w odgórnie ustalony profil reklamodawcy – a wszystko to rozstrzyga się w aukcjach trwających ułamki sekund (RTB). Ponowny wybuch po-

[2] „Such filters are generally also called Memory/Instance-based filters. This machine learning–based technique uses the data from the stored mails and classifies the new instance points in accordance with the similarities to the previous stored examples or the training set". *Artificial Intelligence and Data Mining Approaches in Security Frameworks*, red. N. Bhargava, R. Bhargava, P.S. Rathore, R. Agrawal John Wiley & Sons Incorporated 2021, s. 89.

[3] „Gmail tabs use a classification system that applies machine learning to determine where to put email based on a variety of signals. Signals include (but aren't limited to) who the email comes from, what type of content is in the message and how Gmail users have interacted with similar content". https://workspace.google.com/blog/productivity-collaboration/how-gmail-sorts-your-email-based-on-your-preferences (13.12.2023).

[4] „Concerns about impacts of profiling, which is usually performed without the consent, or even the knowledge of the person affected, relate to the fact that through profiling and data mining, data that could be considered as insignificant or trivial may be proved sensitive providing intimate knowledge about, e.g., life style or health risk 90. These concerns are fed also by the decreasing amount of human involvement to profiling, which increasingly is carried out by «machines»". L. Mitrou, *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, SSNR 2019, czerwiec, s. 21–22.

[5] *Putting machine learning into the hands of every advertiser – Google Ads Help*, https://support.google.com/google-ads/answer/9065075?hl=en (13.12.2023).

wszechności stosowania rozbudowanych mechanizmów uczenia maszynowego zapewniły rozwiązaniom opartych na sztucznej inteligencji modele językowe, które pozwalają na przełamanie bariery komunikacji człowiek–maszyna poprzez zastosowanie interfejsu tekstowego, do którego ludzie już zdążyli się przyzwyczaić wręcz od zarania istnienia komputerów. Dopiero komunikacja wręcz na poziomie zbliżonym do rozmowy z drugim człowiekiem, bez wtrętów w postaci komend, zmiennych, tablic i funkcji, rozpaliła wyobraźnię społeczeństwa i zrównała rozwiązania, tj. ChatGPT czy też Bing AI prawie do tej samej kategorii co kontakt z żywymi osobami[6], często przypisując im walory ekspertów[7]. Jednak pomimo zmiany sposobu interakcji na bardziej „ludzki" należy wciąż pamiętać, iż są to systemy i algorytmy, których funkcjonowanie polega na przetwarzaniu danych przez algorytmy uczenia maszynowego poprzez ich dopasowywanie czy też interpretację.

Nowe projekty zbudowane na ogromnych bazach danych (duża część informacji internetowych do 2021 r. w przypadku ChatGPT) czy też podłączanie ich do internetu sprawia, że coraz trudniej jest kontrolować ich funkcjonowanie. Dalszy postęp prac prowadzi do jeszcze głębszego przełamania barier wymiany informacji, ponieważ każde z liczących się obecnie rozwiązań wdraża do swoich modeli językowych funkcje pozwalające na rozpoznawanie mowy i zamianę jej na tekst oraz odpowiadanie poprzez wygenerowanie mowy z tekstu podanego przez system sztucznej inteligencji dzięki rozwiązaniom *Text-to-speech*. Takie udoskonalenie pozwoli na korzystanie z tych rozwiązań (a niejednokrotnie z całego zasobu treści internetowych) osobom, które mogą mieć problemy z obsługą standardowej przeglądarki internetowej bądź też do tej pory były przez swoje ułomności wykluczone cyfrowo.

Podstawa przetwarzania danych w projektach opartych na działaniu sztucznej inteligencji

Kluczową kwestią dla zgodnego z prawem przetwarzania danych osobowych jest, oprócz określenia celu takiego procesu, także zastosowanie odpowiedniej podstawy legalizującej zgodnie z zamkniętym katalogiem przedstawionym przez ustawodawcę europejskiego w art. 6 ust. 1 RODO oraz art. 9 ust. 2 RODO. Przy bliższym zapoznaniu się ze wspominanym katalogiem można zauważyć, że każda ze znajdujących się tam sześciu przesłanek może stanowić pod-

[6] T.H. Kung, M. Cheatham,A. Medenilla, C. Sillos, L. De Leon, C. Elepaño, M. Madriaga, R. Aggabao, G. Diaz-Candido, J. Maningo, V. Tseng, *Performance of ChatGPT on USMLE: Potential for AI-assisted medical education using large language models*.

[7] Artificial Intelligence Model Aces US Medical Licensing Exam, https://www.tasnimnews.com/en/news/2023/02/11/2851984/artificial-intelligence-model-aces-us-medical-licensing-exam (13.12.2023).

stawę do przetwarzania danych osobowych w rozwiązaniach znajdujących swoje zastosowanie w różnych rodzajach funkcjonalności.

Nie ulega wątpliwości, że rozwiązania AI produkujące treści lub realizujące usługi świetnie wpiszą się model, w którym dane do jej realizacji będą niezbędnie musiały być pobrane od osoby, której dane dotyczą – chociażby dla celu określenia wygenerowanej treści czy też realizacji płatności za nią. Przedstawiony model przetwarzania będzie służył realizacji przesłanki zawartej w art. 6 ust. 1 lit. b RODO. Podmiotowe ograniczenie wynikające z tej przesłanki dotyczy źródła pozyskania danych osobowych, a mianowicie od osoby będącej podmiotem tej relacji prawnej. Prowadzi to do niemożliwości zastosowania tego modelu do przetwarzania danych w projektach opierających się na danych zbieranych w ramach procesu agregowania informacji z powszechnie dostępnych zasobów internetu (czy to w formie ówcześnie zebranej bazy rekordów, czy też informacji zbieranej przez algorytm w momencie generowania odpowiedzi na przesłane zapytanie). Zastosowanie tej przesłanki może jedynie legalizować przetwarzanie danych osobowych podmiotów danych będących użytkownikami rozwiązań, w szczególności ponoszących opłaty i korzystających z płatnych wersji rozszerzonych poszczególnych aplikacji.

Często można spotkać też rozwiązania, które są projektowane *stricte* do ochrony żywotnych interesów osoby, tj. życia lub zdrowia. Duża liczba inteligentnych systemów zaczyna towarzyszyć człowiekowi w codziennym życiu i stąd stanowią dobre miejsce do zaimplementowania funkcjonalności, które poprzez szereg informacji zbieranych z otoczenia wykrywają sytuacje niebezpieczne, np. funkcje powiadamiające o wypadku (w zegarkach lub samochodach) czy też interpretujące stan psychofizyczny osoby (np. wczesne wykrywanie chorób serca[8]). Aktualnie coraz częstszym trendem pojawiającym się w przestrzeni przetwarzania danych o zdrowiu staje się telemedycyna pozwalająca na monitorowanie stanu zdrowia pacjenta w czasie rzeczywistym, co tworzy przestrzeń do wykorzystania systemów opartych na sztucznej inteligencji, które świetnie radzą sobie z interpretowaniem wielu zmiennych jednocześnie, co sprawia, że będą mogły skutecznie wcześnie przewidywać stany pogorszenia zdrowia pacjentów i notyfikować o tym odpowiednie jednostki medyczne.

Niewątpliwie przy spełnieniu dodatkowych warunków możliwe jest projektowanie systemów służących realizacji zadań publicznych lub pozwalających na realizację obowiązków wobec państwa nałożonych przez przepisy prawa. Agregowanie i intepretowanie danych na temat mieszkańców danej gminy poprzez odpowiednie systemy uczone maszynowo pozwoliłoby na wykorzystanie informacji na temat osób wymagających pomocy społecznej w celu zapewnienia im bardziej dopasowanych oraz łatwiej dostępnych procedur samorządowych lub

[8] M. Hutson, *Self-taught artificial intelligence beats doctors at predicting heart attacks*, https://www.science.org/content/article/self-taught-artificial-intelligence-beats-doctors-predicting-heart-attacks (13.12.2023).

państwowych reagujących na pojawiające się problemy społeczne. Jednak przed wdrożeniem tak nowoczesnych technologii wymagane jest zaplanowanie odpowiednich rozwiązań legislacyjnych oraz mechanizmów bezpieczeństwa w celu prawidłowego przetwarzania danych osób w ramach funkcjonowania tych systemów. Już dzisiaj coraz częściej można zobaczyć oswajanie technologii dla wygody obywatela, np. profil zaufany, portal podatkowy czy aplikacja mObywatel.

Kolejną z przesłanek legalizujących przetwarzanie danych osobowych jest niezbędność przetwarzania danych dla realizacji celów wynikających z prawnie uzasadnionych interesów administratora. Możliwe jest zastosowanie tej konstrukcji w przypadku, jeżeli nad takim przetwarzaniem nie mają charakteru nadrzędnego interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Wskazana przesłanka legalizacyjna ze względu na swoją elastyczność interpretacyjną może stanowić rozwiązanie pozwalające na odpowiednie modelowanie zbioru przetwarzanych danych oraz kształtowanie odpowiednich mechanizmów pozwalających na dopasowanie sposobu przetwarzania do rodzaju przetwarzanych danych osobowych. Dynamiczne zarządzanie treściami znajdującymi się w zbiorach danych systemów sztucznej inteligencji mogłoby zapewniać najbardziej skuteczną realizację praw i wolności osób, których dane są przetwarzane, bez ryzyka tworzenia zbyt sztywnych struktur relacyjnych pomiędzy dostawcą systemu a podmiotem, którego dane są przetwarzane, np. umowa, której jakakolwiek zmiana treści wymaga woli obu jej stron do zmiany, a także większego nakładu środków i czynności w celu wdrożenia tych zmian do już istniejących postanowień. Jednak nie sposób nie zauważyć dwoistej natury stosowania tego sposobu konstruowania systemu przetwarzania danych, który będzie wymagał reaktywnego dostosowania do zmieniających się warunków prawno-technologicznych. Może to powodować potrzebę ciągłego przemodelowywania procesu pod względem zakresu zbieranych danych oraz środków wykorzystywanych do ich przetwarzania. Zastosowanie tej przesłanki będzie się wiązało z dokonaniem oceny przez administratora wpływu na prawa i wolności osób, co w konsekwencji może prowadzić do nieprawidłowego przetwarzania skutkującego naruszeniem praw i wolności osób.

Zgoda jako najczęściej stosowana przesłanka legalizacyjna przetwarzania danych osobowych w projektach opartych na działaniu sztucznej inteligencji

Katalog modeli zgodnego z prawem ukonstytuowania procesu przetwarzania danych osobowych przez AI zamyka zgoda osób, których dane dotyczą. Przesłanka ta w niniejszym opracowaniu zasługuje na szersze omówienie ze względu

na uniwersalność i szerokie zastosowanie wobec podmiotów biorących udział w realizacji przetwarzania, połączone z szerokim zakresie uprawnień nadanych podmiotowi przetwarzania. Zastosowana konstrukcja posiada najmniej obostrzeń dla możliwości jej zastosowania, co sprawia, że pozwala na dynamiczne zarządzanie zasobem danych przetwarzanych przez oprogramowanie. Dzięki przekazaniu decyzyjności o momencie rozpoczęcia i zakończenia przetwarzania zapewnia najwyższy poziom kontroli nad przetwarzaniem danych samym zainteresowanym będącym jego podmiotami– co zostałoby zapewnione poprzez mechanizm wycofania oświadczenia woli zgodnie z art. 7 ust. 3 RODO. Nie ulega jednak wątpliwości, iż stosowanie tej przesłanki stanowi większe obciążenie dla administratora danych osobowych, który ze względu na zapewnienie zgodności z przyjętym przebiegiem procesu będzie zmuszony do ściślejszej obsługi przesyłanych zgłoszeń, a także do utrzymywania odpowiedniego zaplecza technicznego wyposażonego w funkcjonalności pozwalające na elastyczne zarządzanie treścią danych źródłowych dla systemów AI. Niezaniedbywalnym ryzykiem jest także niestabilność efektów, jakie oferowane przez niego oprogramowanie jest w stanie wygenerować w związku z fluktuacją posiadanych informacji. To w konsekwencji może prowadzić do destabilizacji wykorzystywanych algorytmów lub naruszenia integralności posiadanych danych.

Zaprojektowanie procesu opartego na zgodzie odbieranej od podmiotów, których dane mają być przetwarzane w systemie, implikuje, że dane do zasobów funkcjonalności będą zbierane w modelu opt-in (*optional in*). Oznacza to, że aby dane osoby fizycznej mogły pojawić się w zasobach oprogramowania, niezbędne jest uprzednie wyrażenie zgody przez osobę, której dane dotyczą. Należy zauważyć co najmniej dwa cele mogące wiązać się z danymi tej samej osoby fizycznej. Pierwszym celem, jaki można wyznaczyć, jest zaktualizowanie zagregowanych przez oprogramowanie danych o informacje zebrane (lub zebrane w przyszłości i wytworzone) na temat podmiotu wyrażającego zgodę. Drugim powodem przetwarzania jest funkcjonowanie konta użytkownika w platformie oferującej funkcjonalność (wraz z danymi związanymi z jego uwierzytelnieniem, a także historią zapytań i aktywności). Patrząc z tej perspektywy, należy przyjąć, że jedynie pierwszy z celów może opierać się na oświadczeniu podmiotu danych – mianowicie dodanie do bazy rekordów systemu[9]. Należy zauważyć, że uznanie zgody

[9] „Both the need for consent and the right withdraw consent threaten the development of AI because it could limit the amount of data available to learn from. Additionally, data subjects, in certain situations, can exercise a right to restrict the processing of their information. (…) Because AI continues to learn from past data, the issue becomes how to simultaneously stop AI's learning from this data, without impacting its prior development". M. Humerick, *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, „Santa Clara High Technology Law Journal" 2018, vol. 32 issue 4, art. 3, s. 406.

jako podstawy do założenia i funkcjonowania konta w oferowanym rozwiązaniu stałoby w sprzeczności z wymaganiami, jakie RODO stawia dla dobrowolności jej wyrażania w treści normy art. 7 ust. 4[10].

Sporną kwestią pozostaje możliwość świadomego wyrażenia zgody na przetwarzanie danych osobowych wobec danych wytworzonych lub skorelowanych dodatkowo przez algorytm. Należy zauważyć, że ustawodawca europejski wskazał sposób wykładni tej cechy w treści motywu 42 RODO: „Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych". Wart rozważenia jest zakres przedmiotowy, jaki obejmuje zaaprobowanie przetwarzania przez właściciela danych. Ze względu na specyfikę funkcjonowania systemów opartych na sztucznej inteligencji (także przy użyciu zaawansowanego uczenia maszynowego) oraz dynamiczne budowanie relacji pomiędzy informacjami będącymi w zasobach systemu AI niemożliwe jest określenie dokładnego celu i wskazania zamkniętego katalogu czynności, jakie mogą zostać dokonane na tych danych osobowych. Ograniczenie to wymaga od administratora odpowiedniego określenia celu już w treści klauzuli zgody, uwzględniającego również ten etap przetwarzania[11]. Niezbędne jest uświadomienie użytkownikowi, że wyrażana zgoda dotyczy także danych będących efektem przekształceń zebranych danych oraz danych znajdujących się już w bazie informacji wykorzystywanych przez oferowany system[12].

[10] „Od złożenia zgody nie należy uzależniać realizacji czy też nawiązania stosunku prawnego. Żądanie udzielenia zgody, np. na cele marketingowe, w zamian za wykonanie umowy przeczy idei dobrowolności zgody i jako takie jest niezgodne z art. 7 ust. 4 RODO. Zakazane będą więc wszelkiego rodzaju działania uzależniające dostęp do konkretnej usługi, np. strony internetowej, od tego, aby dana osoba wyraziła zgodę na przetwarzanie danych osobowych w celach marketingowych lub przesyłania newslettera". *Ogólne rozporządzenie o ochronie danych osobowych: Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 171.

[11] „It remains disputable if this legislative array will ensure that «users would review, rationally assess and deliberatively respond to that information when exercising their consent entitlements» as people are reluctant to read privacy notices. Even if policies and notices satisfy legal obligations, it is highly questionable if consent is adequate as legal ground. Technology and applications are changing steadily and rapidly having a serious impact on the foresee ability of the future uses of data based on consent submitted. The substantial increase in development of processing capabilities (storage, mining, crawling, matching profiles) may entirely transform the context and the conditions under which personal data are processed thus augmenting its informative value in an unpredictable way and increasing the potential adverse effects for individuals' rights". L. Mitrou, *Data Protection*…, s. 38–39.

[12] „If an organisation can identify potential benefits from using personal data in big data analytics, it should be able to explain these to users and seek consent, if that is the condition it chooses to rely on. It must find the point at which to explain the benefits of the analytics and present users with a meaningful choice – and then respect that choice when processing their personal data". ICO, *Big data, artificial intelligence, machine learning and data protection* v2.2, 2017.

Niezbędna do rozpatrzenia przez administratora jest sytuacja prawna danych osobowych, które mogą być treścią zapytania lub odpowiedzi odmownej. Zakres podmiotowy, który upoważnia do wyrażenia oświadczenia o zgodzie na przetwarzanie danych, dotyczy jedynie właściciela danych i znaczenia tego oświadczenia woli nie można stosować jako podstawy legalizującej przetwarzanie przez administratora innych danych osobowych. Prowadzi to w konsekwencji do możliwości wykorzystania w tworzonych treściach jedynie danych osobowych, których właściciele wyrazili podobne oświadczenie pozwalające na branie udziału w procesie. Dla odpowiedniego realizowania procesu wymagane jest od administratora pochylenie się nad kontrolą treści przetwarzanych danych na dwóch etapach działania algorytmów, tj. w momencie otrzymania i przechowywania treści zapytań, a także w chwili generowania treści odpowiedzi dla klientów. Nie ulega wątpliwości, że każda z tych kontroli będzie miała inny wymiar i zastosowanie. W pierwszym przypadku kontrola treści powinna mieć charakter pozwalający jedynie na realizację przetwarzania danych osobowych innych podmiotów, a więc możliwości powiadomienia podmiotów, które skorzystały z tych danych i posiadają je w swojej historii chatów (w szczególności jeżeli relacją przetwarzania pomiędzy klientem a dostawcą systemu jest powierzenie przetwarzania), niemożliwe jest jednak samodzielne usunięcie takich danych przez dostawcę systemu. W przypadku drugiej formy kontroli to na administratorze ciążyć będzie stworzenie sieci zasad pozwalających na wykrywanie oraz blokowanie wykorzystania treści związanych z oznaczonym zestawem danych osobowych. Obowiązek ten będzie aktualizował się za każdym razem, gdy właściciel danych postanowi wycofać swoje oświadczenie woli zgodnie z art. 7 ust. 3 RODO.

Ostatnim ważnym elementem dla legalizacji przetwarzania na podstawie wspominanej już podstawy prawnej jest potwierdzenie tożsamości podmiotu wyrażającego zgodę. Zgodnie z konstrukcją przyjętą przez prawodawcę europejskiego w art. 7 ust. 1 RODO to na administratorze danych osobowych spoczywa ciężar dowodowy prawidłowości jej odebrania[13]. Niezbędnym przymiotem takiego oświadczenia woli jest jego pochodzenie od osoby, której dane dotyczą. Brak możliwości wykazania przesłanek potwierdzających pochodzenie oświadczenia zgody będzie skutkował niespełnianiem przez administratora przesłanek zawartych w normie art. 6 ust. 1 lit. a RODO, co w konsekwencji może prowadzić do nielegalnego przetwarzania danych osobowych[14]. W przypadku tak roz-

[13] Wybór formy pozyskania zgody zależy od administratora, który, jak zostało to już powiedziane, zobowiązany jest fakt uzyskania zgody wykazać. Jednocześnie prawodawca unijny nie określa formy, która powinna być zachowana dla celów dowodowych. Zatem każdy środek, który będzie należycie udowadniał, że użytkownik udzielił zgodę, będzie wystarczający. M. Ciechomska, *E-usługi a RODO*, Warszawa 2021, s. 89.

[14] „Na podstawie art. 7 ust. 1 RODO w przypadku, gdy przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła

budowanego procesu przetwarzania należy przyłożyć szczególną wagę do potwierdzania tożsamości, gdyż nieprawidłowe zainicjowania przetwarzania danych osoby fizycznej może prowadzić do rozległego naruszania jej praw i wolności. Na etapie projektowania procesu administrator powinien ocenić ryzyko wystąpienia sytuacji podszywania się pod inną osobę fizyczną w celu zebrania o niej uzupełnianych za pomocą algorytmów oprogramowania danych. Nie ulega wątpliwości, że wystąpienie takiej sytuacji doprowadzi do nielegalnego przetwarzania danych osobowych, a w konsekwencji może skutkować powstaniem odpowiedzialności administracyjnej lub odszkodowawczej administratora. Biorąc pod uwagę poprzednie wnioski, należy wskazać, że charakter oraz rozległość procesu przetwarzania będą determinowały zastosowanie algorytmów powiązanych z potwierdzeniem tożsamości osoby poprzez usługi zewnętrzne – odpowiednio do kontekstu usługi: poprzez numer telefonu, za pomocą poczty e-mail lub wykorzystanie kont w portalach społecznościowych bądź przez dużych dostawców usług (w tym bankowych). Nadmiarowy charakter przetwarzania w związku z tym mechanizmem będą miały wszystkie oficjalne dane jednoznacznie identyfikujące osobę na poziomie administracyjnym, tj. numer dowodu osobistego, numer PESEL czy identyfikatory usług administracji elektronicznej.

Zapewnienie realizacji obowiązków informacyjnych na temat celów i sposobów przetwarzania danych osobowych z przepisów RODO – wybrane zagadnienia

Należy zastosować szczególne podejście do tematu możliwości udzielenia informacji o metodach i sposobach przetwarzania ze względu na dynamiczną i reaktywną charakterystykę działania rozwiązań opartych na sztucznej inteligencji. Wymiar odrębności jest tym większy, im bardziej rozległym zasobem informacji posługuje się algorytm i im częściej dostępna dla niego treść jest aktualizowana. Zgodnie z *ratio legis*[15] norm prawnych zobowiązujących admini-

zgodę na przetwarzanie swoich danych osobowych. Przepis przesądza zatem o rozkładzie ciężaru dowodu, który spoczywa na administratorze. Warto wskazać, że zgodnie z art. 6 KC ciężar dowodu określonego faktu spoczywa na stronie, która z tego faktu wywodzi skutki prawne, co ma znaczenie dla spraw sądowych dotyczących danych osobowych, w których administrator powoływałby się na fakt udzielenia zgody na przetwarzanie danych. (…) Ewentualny błąd lub inna nieprawidłowość zachodzące co do zakresu udzielonej zgody sprawią, że przetwarzanie nie będzie legalne". *Ogólne rozporządzenie o ochronie danych osobowych: Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 5.

[15] „Obowiązek ma charakter czynny, co oznacza, że administrator realizuje go z własnej inicjatywy, bez wniosku podmiotu danych. (…) jego funkcją pozostaje umożliwienie jednostce dostępu do dotyczących jej danych, a także informacji o istotnych okolicznościach, w jakich odbywa się przetwarzanie tych danych osobowych, oraz skorzystania z pozostałych praw wynikających

stratora danych do wyczerpującego i zrozumiałego przekazania informacji na temat przetwarzania danych osobowych należy priorytetowo traktować realizację wszelkich obowiązków informacyjnych[16]. Prawodawca europejski konstruuje obowiązek posiadania oraz udostępniania takich informacji w uprawnieniu podmiotu danych do uzyskania dostępu do treści swoich danych oraz informacji związanych z ich przetwarzaniem, zgodnie z normami zawartymi w art. 12–15 RODO. Legislator zadbał przy tym o wprowadzenie różnych trybów przekazywania informacji podmiotom danych, różniących się od siebie momentem realizacji tego obowiązku, ilością przekazywanych treści oraz wymogami co do zaktualizowania obowiązku administratora przetwarzającego dane osobowe. Zapewnia to, że osoba, której dane są przetwarzane, może w pełni świadomie zarządzać przetwarzaniem swoich danych i decydować o tym, czy chce podjąć przewidziane prawem środki, aby takie przetwarzanie przerwać.

Można zauważyć, że wskazane nakazy informowania podmiotu danych o celach i sposobach przetwarzania dzielą się na dwie kategorie co do czasu ich realizacji przez administratora. Zgodnie z brzmieniem art. 13 oraz 14 RODO można wyróżnić zobowiązanie do uprzedniego poinformowania osoby co najmniej o swojej tożsamości, danych umożliwiających nawiązanie z nim kontaktu, celach i podstawach prawnych przetwarzania, katalogu podmiotów stanowiących odbiorów danych oraz ich przekazywaniu, a w przypadku gdy dane pochodzą nie od osoby, której dotyczą – także o źródle ich pozyskania. Drugim trybem, który został przewidziany w przepisach prawa, jest udzielenie tożsamego katalogu informacji na podstawie wniosku podmiotu zgodnie z art. 15 RODO. Uprawnienie to pozwala na kontrolę prawidłowości przetwarzania realizowanego w procesach administratora. Zostało ono także wzmocnione przez wyposażenie podmiotu przetwarzania w możliwość żądania otrzymania kopii przetwarzanych danych zgodnie z art. 15 ust. 3 RODO. Trudności z rzetelnym i prawidłowym wykonaniem tego obowiązku przez administratora można podzielić na dwie zasadnicze kategorie: problem z oznaczeniem kategorii przetwarzanych danych osobowych lub problem z oznaczeniem sposobów przetwarzania posiadanych danych.

---

z rozdziału III RODO, jak również innych uprawnień, które zostały przewidziane w przepisach rozporządzenia". *Ibidem*.

[16] „W konkretnych przypadkach przedstawienie podmiotowi danych wystarczających informacji może się okazać trudne, głównie gdy sztuczna inteligencja oparta jest na głębokim uczeniu, nienadzorowanym lub jedynie częściowo nadzorowanym, gdy uczenie następuje nie na podstawie metod wykorzystujących symboliczne zasady rozumowania. Dobór metod, które mają być podstawą działania mechanizmów sztucznej inteligencji, z uwzględnieniem wymogu ich wyjaśnialności, jest w konsekwencji jednym z elementów oceny zgodności z zasadą przejrzystości. Chodzi bowiem o to, aby już w fazie projektowania przez dokonanie wyboru określonego rozwiązania technologicznego nie wykluczyć a priori możliwości realizacji tej zasady. Trudności technologiczne nie mogą bowiem zwalniać z obowiązku zachowania przejrzystości". B. Fischer, A. Pązik, M. Świerczyński *Prawo sztucznej inteligencji i nowych technologii 2*, Warszawa 2022, s. 438.

W pierwszym przypadku kluczowym aspektem będzie zasób informacji, jaki posiada aplikacja. W treści wspomnianych uprzednio przepisów wielokrotnie pojawia się obowiązek przekazania osobie treści jej przetwarzanych danych, informacji o kategoriach danych odnośnych, a także informacji o źródle, z którego zostały zebrane. Od administratora przygotowanie takich informacji wymaga posiadania odpowiednich funkcjonalności pozwalających systemowi na identyfikację oraz ewidencjonowanie posiadanych danych. W przypadku aktualizującej się dużej bazy informacji lub też wykorzystywania ogólnodostępnych źródeł informacji będzie to nastręczało dodatkowych problemów z potrzebą dynamicznego realizowania tych czynności, w czasie zbliżonym do ich pobierania[17]. Nie ulega wątpliwości, że automatyzacja tak dużego procesu będzie się wiązała z możliwością błędnego zakwalifikowania danych jako danych niebędących danymi osobowymi poprzez brak identyfikacji przez oprogramowanie odpowiedniej korelacji pomiędzy rekordami. Ponadto ocenie administratora będzie podlegać wskazanie granic realizacji uprawnień informacyjnych, w szczególności w przypadku danych pojawiających się w ramach przetwarzania przez algorytm przez krótki okres czy w przypadku dynamicznego zmieniania celu przetwarzanych danych. Nie istnieją w tekście prawnym wyrażone *stricte* możliwe do zastosowania w tych sytuacjach wyłączenia, gdyż chociażby nie powinno przyświecać przedsiębiorcy realizującemu swoją działalność powoływanie się na niewspółmierny wysiłek wobec celu i charakteru przetwarzania – nawet w przypadku, gdy generuje to koszty po jego stronie[18].

Jednak mając na uwadze wspomniane powyżej *ratio legis* przepisów konstytuujących, realizowane obowiązki informacyjne muszą zostać poddane ocenie administratora w ramach projektowania rozwiązania i jego obowiązkiem jest wyważenie informacji podawanych jego użytkownikom na podstawie faktycznego działania, jakiego dokonuje on przez swoje oprogramowanie. Biorąc pod uwagę modele funkcjonowania systemów opartych na sztucznej inteligencji i ich dynamiczny zakres przeglądania i zbierania danych, należałby w przypadku przyjęcia ścisłej wykładni językowej przesyłać do osoby fizycznej informacje na

[17] Odpowiedzialność za algorytmy nie może być statyczna. Należy na nią spoglądać w ujęciu dynamicznym, gdzie wiele czynników wpływających na bezpieczeństwo algorytmów nie jest stałych i podlega ciągłym zmianom, często nawet w czasie rzeczywistym. Przy określaniu odpowiedzialności konieczne jest uwzględnienie zmienności elementów czy też czynników wpływających na bezpieczeństwo, a co za tym idzie – odpowiedzialność za algorytmy. *Ibidem*, s. 126.

[18] Organ stwierdził, że rezygnację z bezpośredniego kontaktu tylko z powodu związanych z tym kosztów należy ocenić negatywnie, szczególnie że operacje na danych osobowych stanowią przedmiot podstawowej, czysto komercyjnej, profesjonalnej, wieloletniej działalności spółki. Organ zwrócił uwagę, że znaczenie mają także konsekwencje niespełniania tego obowiązku, jakimi są: niewiedza osób, których dane dotyczą, o procesach przetwarzania ich danych oraz o możliwości skorzystania z przysługujących im praw zagwarantowanych przepisami rozporządzenia 2016/679. Wyrok WSA w Warszawie z dnia 11 grudnia 2019 r., sygn. II SA/Wa 1030/19.

temat przetwarzania jej danych osobowych zgodnie z normą art. 14 RODO. Nie ulega jednak wątpliwości, że w przytłaczającej większości przypadków będzie stanowiło to mechaniczne zrealizowanie nakazanego prawem zachowania, które jednak nie przynosi żadnych korzyści dla żadnej ze stron tego stosunku. Dla lepszego wyjaśnienia sprawy posłużmy się modelem, w którym dane po wstępnym „przeczytaniu" przez algorytm są natychmiast usuwane, gdy podejmie on decyzję o ich nieprzydatności do realizowanego zadania. Trwające sekundy przetwarzania przez algorytm związane z zapoznaniem się z treścią tych danych powodowałby za każdym razem skierowanie do podmiotu danych komunikatu o przetwarzaniu danych, jednak nie będzie on miał żadnej możliwości wpłynąć na żaden z aspektów dokonanego już i zakończonego przetwarzania. Może to prowadzić do naruszenia przez administratora innych praw tych osób, np. prywatności, w dobrej wierze i z przekonaniem o realizacji obowiązków prawa. Można wyobrazić sobie, że przesyłanie informacji do częściej pojawiających się w zapytaniach osób mogłoby prowadzić do praktyki podobnej do przesyłania spamerskich kampanii marketingowych, co w rezultacie może skutkować obniżeniem skuteczności uwrażliwienia właścicieli danych na temat ich bezpieczeństwa i w rezultacie obniżyć poziom kontroli nad nimi.

Przy drugim aspekcie procesu przetwarzania kluczowe będzie zidentyfikowanie i oznaczenie sposobu przetwarzania danych osobowych w formie, która będzie możliwa do prześledzenia oraz zrozumienia przez podmioty danych. W zależności od zastosowanego algorytmu sztucznej inteligencji, a także metodologii, za pomocą której był on nauczany (w tym również w jakim stopniu były nadzorowane jego działania), może to determinować różne formy możliwego zrealizowania. W szczególności problemy mogą pojawić się w momencie pozostawienia „luzów decyzyjnych" w postaci pozostawienia wyboru działania samemu algorytmowi lub też niewprowadzania ograniczeń co do możliwości zachowań oprogramowania. Może to prowadzić do zaburzenia integralności i poprawności przetwarzanych danych, co mogłoby mieć przełożenie np. na dobra osobiste osób w postaci naruszenia dobrego imienia lub prywatności bądź też zaburzenia w sposobach analizowania i wyświetlania treści, co także poprzez dyskryminujące lub cenzurujące działania algorytmu może prowadzić do naruszenia ochrony danych osobowych. Wspomniane zjawisko z dużym prawdopodobieństwem może też eskalować wraz z postępującym samodzielnym uczeniem się algorytmu poprzez interakcje, na które został wystawiony. Będzie to miało poważne konsekwencje w przypadku systemów dopuszczonych do powszechnego używania przez nieokreśloną liczbę osób.

Podsumowując, konieczne wydaje się wprowadzenie odpowiednich regulacji prawnych oraz mechanizmów umożliwiających skuteczne ograniczanie szczegółowości przetwarzanych informacji czy też zakresu wiadomości obowiązkowych do przekazania w ramach wykonywania prawa dostępu do danych

osobowych w przypadku rozwiązań opartych na sztucznej inteligencji i uczeniu maszynowym. Istnieje kilka propozycji rozwiązania wspomnianych problemów, w tym m.in. pomocne może okazać się:

1. Wprowadzenie obowiązku informowania w sposób uproszczony o metodach działania algorytmów sztucznej inteligencji i uczenia maszynowego oraz o sposobie przetwarzania danych przez te systemy poprzez zawarcie odpowiedniej informacji w miejscu łatwo dostępnym dla osób, których dane dotyczą.
2. Opracowanie jednolitych metodologii oraz sposobów umożliwiających skuteczne wykonywanie prawa dostępu do takich danych, jak dedykowane formularze odpowiedzi na realizację prawa czy też na otrzymanie kopii danych przetwarzanych przez algorytm z objaśnieniem systemów postępującego procesu uszczuplania informacji do wersji podanej w komunikacie końcowym.
3. Stworzenie i wdrożenie jednolitego systemu wykrywania i zarządzania treściami o charakterze osobistym, naruszającym prywatność osoby, lub też informacjami mogącymi stanowić dane szczególne (w myśl katalogu zawartego w art. 9 ust. 1 RODO), a możliwe że także danych dotyczących wyroków skazujących i naruszeń prawa (art. 10 RODO). System powinien posiadać możliwość odwołania się od wskazań algorytmu i cechy realizujące obowiązki stawiane wobec algorytmów dotyczących zautomatyzowanego podejmowania decyzji.

Otoczenie innych aktów prawa unijnego oraz procedowane projekty

RODO nie jest jedynym aktem prawa europejskiego, który dotyczy poruszanych w treści artykułu problemów i uwag. Można chociażby zauważyć potrzebę dostosowania korzystania z systemów opartych na modelach sztucznej inteligencji w obszarze przetwarzania danych osobowych w ramach działania organów ścigania oraz organów wymiaru sprawiedliwości, które posiada odrębną dyrektywę[19] regulującą ten rodzaj przetwarzania informacji o osobach fizycznych. Trudno jednak w takim przypadku mówić o zwiększaniu kontroli nad treścią i sposobami przetwarzania danych przez osoby, których dane dotyczą – w tym zakresie wiodącą rolę będą musiały odegrać poszczególne podmioty wspólnotowe oraz krajowe, ustalając zakres ograniczenia oraz ingerencji w prawa podmio-

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. UE L z 2016 r., nr 119, s. 89 ze zm.).

tów danych oraz projektując akty prawne decydujące o kształcie przetwarzania danych osobowych.

Mocniej zbliżonym aktem prawnym do RODO jest rozporządzenie dotyczące przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii[20], co charakterystycznie pokazuje tożsamy katalog podstawy prawnych przetwarzania danych osobowych znajdujący w art. 5 tego rozporządzenia – pozbawiony jedynie przesłanki prawnej uzasadnionego interesu administratora danych. Tak ukształtowana paleta przesłanek zmusza organy Unii Europejskiej do korzystania z rozwiązań przewidzianych przez akty prawa Unii (w myśl art. 5 ust. 2 tego rozporządzenia) albo ze zgody osoby, której dane dotyczą – a tej konstrukcja jest tożsama z podejściem przyjętym w RODO, a co za tym idzie – będą jej dotyczyć te same problemy.

Przetwarzanie danych osobowych nierozerwalnie związane jest z bezpieczeństwem systemów, których podmioty używają do realizacji ich procesów. Nie sposób jednak nie zauważyć, że szerokie wykorzystanie rozwiązań opartych na sztucznej inteligencji będzie wiązało się również z obsługą systemów technologicznych, w tym tych będących składnikami infrastruktury krytycznej czy kluczowych sektorów gospodarki. W zabezpieczeniu tych podmiotów na priorytetową pozycję wysuwa się cyberbezpieczeństwo, które w ramach funkcjonowania Unii reguluje dyrektywa NIS2[21]. Choć rozporządzenie jest datowane na 2022 r., to o systemach opartych na sztucznej inteligencji lub uczeniu maszynowym wspomina jedynie lakonicznie w motywach 51 i 89, gdzie ustawodawca europejski zachęca do wykorzystywaniu tych systemów w celu lepszego identyfikowania i wykrywania cyberzagrożeń. W ramach określania wymagań stawianych kolejnym rodzajom podmiotów nie sposób jednak odnaleźć norm regulujących konkretnie warunki korzystania i zabezpieczenia takich systemów. Tworzy to lukę prawną, która może utrudniać podmiotom właściwe zabezpieczenie systemów, gdyż brak precyzyjnych wytycznych może prowadzić do niepewności co do stosowanych środków bezpieczeństwa i narażać na ryzyko zarówno podmioty przetwarzające dane osobowe, jak i osoby, których dane te dotyczą. Jednak ustawodawca europejski podjął już próbę uszczelnienie systemu regulacji poprzez będący jeszcze w fazie procedowania AI Act[22], który pozwoli na klasyfi-

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG).

[21] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2) (Tekst mający znaczenie dla EOG).

[22] Projekt rozporządzenia Parlamentu Europejskiego i Rady (UE) COM/2021/206 *final*.

kację rozwiązań opartych na sztucznej inteligencji poprzez cel, do jakiego będą wykorzystywane, a w konsekwencji zastosowanie do nich jednolitych systemów mierzenia bezpieczeństwa i zabezpieczeń dopasowanych do przyznanej kategorii.

Podsumowanie

Rozpowszechnienie systemów przetwarzania danych za pomocą funkcjonalności opartych na sztucznej inteligencji jest efektem dynamicznie postępującego rozwoju technologicznego i informatyzacji społeczeństwa. Przed legislatorami oraz administratorami czuwającymi nad procesami przetwarzania danych osobowych stoi wyzwanie, aby nadążyć ze stworzeniem mechanizmów pozwalających zapewnić odpowiedni poziom bezpieczeństwa podmiotów danych. Dynamicznie zmieniające się sposoby na wykorzystywanie informacji w dobie zmian mogą stanowić rzetelny papierek lakmusowy aktualnej dojrzałości systemu ochrony danych osobowych w Europie oraz prowadzić do sprawdzenia, ile wyzwań pozostało jeszcze do przezwyciężenia przez uczestników biorących udział w procesach przetwarzania. Przywołane zagadnienia stanowią jedynie zarys najpotrzebniejszych mechanizmów pozwalających na prawidłowe funkcjonowanie rozwiązań AI w przestrzeni prawnej i nie obejmują one norm postępowania skierowanych do pozostałych uczestników procesu. Przykładem takiego scenariusza mogłoby być działanie prawodawcze w postaci utworzenia rejestru podmiotów, które nie chcą, aby ich dane były przetwarzane w ten konkretny sposób realizowany przez narzędzia sztucznej inteligencji. Scentralizowanie bazy oświadczeń woli podmiotów o niepodleganie tak szeroko zakrojonemu zautomatyzowanemu przetwarzaniu pozwoliłoby na stworzenie mechanizmów, które wstrzymywałyby realizację zapytania dotyczącego danych osobowych aż do momentu uzyskania informacji na temat figurowania lub niefigurowania konkretnego zestawu danych osobowych we wspomnianym rejestrze. Pozwoliłoby to na jeszcze dynamiczniejsze zarządzanie wykorzystaniem swoich danych osobowych przez ich właścicieli.

Aktualnym problemem pozostaje także sytuacja już istniejących administratorów danych, którzy odpowiadają za publikację treści. W związku z ich decyzyjnością o celach i sposobach przetwarzania są oni w stanie za pomocą mechanizmów ich stron internetowych umożliwić lub zabronić przeglądanie zawartości ich witryn przez rozwiązania zautomatyzowane. Klasyfikując udostępnienie danych jako formę ich przetwarzania (w myśl definicji znajdującej się w art. 4 RODO), administratorzy zobligowani są co najmniej do aktualizacji swojego podejścia do procesu przetwarzania lub też zmiany sposobu jego działania dla ochrony praw i wolności osób (zgodnie z normą art. 25 RODO). Wymaganym działaniem z ich strony jest dostosowanie informacji, jakie są przekazywane w ramach realizacji obowiązków informacyjnych, oraz ponowne dokonanie oce-

ny ryzyka dla przetwarzanych w ten sposób danych osobowych, a także na tej podstawie zrealizowanie dodatkowych działań w celu zapewnienia bezpieczeństwa całego rozwiązania. W skrajnych przypadkach może to prowadzić również do zaktualizowania się obowiązku przeprowadzenia oceny skutków dla przetwarzania danych osobowych lub modyfikacji oferowanych publicznie treści (zob. sprawa Google i Google Spain – C-131/12).

Bibliografia

Artificial Intelligence and Data Mining Approaches in Security Frameworks, red. N. Bhargava, R. Bhargava, P.S. Rathore, R. Agrawal, John Wiley & Sons Incorporated 2021.

Artificial Intelligence Model Aces US Medical Licensing Exam, https://www.tasnimnews.com/en/news/2023/02/11/2851984/artificial-intelligence-model-aces-us-medical-licensing-exam (13.12.2023).

Ciechomska M., *E-usługi a RODO*, Warszawa 2021.

Fischer B., Pązik A., Świerczyński M., *Prawo sztucznej inteligencji i nowych technologii 2*, Warszawa 2022.

Humerick M., *Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, „Santa Clara High Technology Law Journal" 2018, vol. 32 issue 4, art. 3.

Hutson M., *Self-taught artificial intelligence beats doctors at predicting heart attacks*, https://www.science.org/content/article/self-taught-artificial-intelligence-beats-doctors-pre dicting-heart-attacks (13.12.2023).

Kung T.H., Cheatham M., Medenilla A., Sillos C., De Leon L., Elepaño C., Madriaga M., Aggabao R., Diaz-Candido G., Maningo J., Tseng V., *Performance of ChatGPT on USMLE: Potential for AI-assisted medical education using large language models*.

Mitrou L., *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, SSNR 2019, czerwiec.

Ogólne rozporządzenie o ochronie danych osobowych: Komentarz, red. M. Sakowska-Baryła, Warszawa 2018.

Vall du P., Dziedzic K., Fajgielski P., *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2021.

Streszczenie

Celem artykułu jest zbadanie problemów i wyzwań związanych z zapewnieniem zgodności rozwiązań opartych na sztucznej inteligencji (AI) z podstawowymi mechanizmami systemu ochrony danych osobowych w ramach Unii Europejskiej. W opracowaniu omawiane zostały różne aspekty przetwarzania danych osobowych przez systemy AI, takie jak podstawy prawne, obowiązki informacyjne, prawa podmiotów danych czy też ryzyko naruszenia praw podstawowych. W artykule wskazywano potrzebę wprowadzenia odpowiednich regulacji prawnych oraz mechanizmów technicznych i organizacyjnych, które pozwolą na skuteczną realizację zasad i celów RODO w kontekście stosowania AI.

Słowa kluczowe: sztuczna inteligencja, uczenie maszynowe, ochrona danych osobowych, RODO, prawa podmiotów danych

ARTIFICIAL INTELLIGENCE (AI) VS. PERSONAL DATA PROTECTION (RODO) – HOW TO ENSURE THAT AI SOLUTIONS COMPLY WITH THE BASIC MECHANISMS OF THE EU DATA PROTECTION REGIME?

Summary

The purpose of this article is to explore the problems and challenges of ensuring the compatibility of artificial intelligence (AI) based solutions with the basic mechanisms of the personal data protection regime within the European Union. The article discusses various aspects of the processing of personal data by AI systems, such as the legal basis, information obligations, rights of data subjects, and the risk of violation of fundamental rights. The article points out the need for appropriate legal regulations as well as technical and organizational mechanisms to effectively implement the principles and objectives of the RODO in the context of the application of AI.

Keywords: artificial intelligence, machine learning, personal data protection, GDPR, data subject rights