Paragraf 8 / 2026
https://doi.org/10.18778/2956-3747.8.04

Justyna Krupa*

Sztuczna inteligencja pod lupą RODO

Streszczenie

Artykuł podejmuje intrygującą w obecnych czasach problematykę pogodzenia regulacji ochrony danych osobowych wynikających z RODO z nowymi ramami prawnymi przewidzianymi w AI Act. Analizie poddano zarówno wspólne punkty obu aktów, takie jak ocena ryzyka, jak i różnice w zakresie celów regulacyjnych i adresatów obowiązków. Refleksjom poddane zostały również praktyczne wyzwania, związane m.in. z przeprowadzaniem DPIA, oraz możliwe ścieżki integracji wymogów obu analizowanych reżimów prawnych. Artykuł porusza także kwestie rozwiązań prowadzących do ograniczenia dublowania procedur, wzmocnienia współpracy organów nadzorczych oraz rozwoju praktycznych standardów AI.

Słowa kluczowe: RODO, AI Act, sztuczna inteligencja, ochrona danych osobowych, dane wrażliwe, ocena ryzyka

Artificial intelligence under the scrutiny of the GDPR

Abstract

The article addresses the intriguing issue of reconciling the personal data protection regulations under the GDPR with the new legal framework provided for in the AI Act. The analysis encompasses both the common points of the two acts, such as risk assessment, and the differences in regulatory objectives and addresses of obligations. Moreover, it reflects on the practical challenges associated with conducting DPIA and possible paths for integrating the requirements of both legal regimes. The article also addresses solutions leading to the reduction of duplication of procedures, the strengthening of cooperation between supervisory authorities and the development of practical AI standards.

Keywords: GDPR, AI Act, artificial intelligence, personal data protection, sensitive data, risk assessment

* Magister, Uniwersytet Jagielloński w Krakowie, e-mail: justyna.krupa@student.uj.edu.pl, https://orcid.org/0009-0007-5154-0049

Received: 11.10.2025. Verified: 30.11.2025. Accepted: 31.03.2026.

Funding information: Not applicable. **Conflicts of interests:** None. **Ethical considerations:** The Authors assure of no violations of publication ethics and take full responsibility for the content of the publication.

1. Wprowadzenie

W ciągu kilku lat sztuczna inteligencja (*artificial intelligence*, AI) przeszła drogę od eksperymentów w laboratoriach badawczych do narzędzia kształtującego codzienne życie milionów ludzi. Jej rozwój wywołał emocje porównywalne np. do wcześniejszej rewolucji internetowej, budząc w społeczeństwie mieszankę silnych doznań, takich jak entuzjazm i lęk. Ludzie zaczęli mieć oczekiwania względem AI, widząc w niej nowe możliwości w postaci lepszej produktywności, kreatywnych narzędzi pracy odpowiadających za automatyzację, generowanie treści czy pomoc w nauce i działalności badawczej. Jednakże rozwój nowej technologii budził również obawy i niepewność o takie kwestie, jak miejsca pracy, dezinformacja oraz prywatność. Rewolucja internetowa umożliwiła połączenie i udostępnienie informacji, natomiast sztuczna inteligencja zaczęła imitować i wykonywać zadania, które do tej pory wydawały się *stricte* ludzkie. Internet zmienił sposób, w jaki dziś możemy się komunikować i zdobywać wiedzę, ale AI może zmienić sposób, w jaki pracujemy, uczymy się czy podejmujemy decyzje. To wszystko wywołuje debatę etyczną i prawno-społeczną oraz potrzebę regulacji.

Systemy oparte na uczeniu maszynowym – a szczególnie modele generatywne, takie jak ChatGPT[1], Claude[2] czy Gemini[3] – trafiły do codziennego użytku zarówno w biznesie, jak i w życiu prywatnym. Ich potencjał jest ogromny: od wsparcia procesów rekrutacyjnych i obsługi klienta po zastosowania w medycynie czy administracji publicznej.

W tym kontekście pytanie o zgodność AI z prawem ochrony danych osobowych staje się jednym z najważniejszych problemów współczesnej demokracji cyfrowej. Jak trafnie zauważa S. Wachter, „prawo do wyjaśnienia działania algorytmów – często postrzegane jako oczywisty element RODO[4] – w praktyce okazuje się znacznie bardziej złożone i niejednoznaczne”[5]. W odniesieniu do definicji przyjętej przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE), mówiącej o szerokiej interpretacji pojęcia danych osobowych, obejmującej wszelkie informacje umożliwiające identyfikację jednostki, nawet w sposób pośredni[6], daje to zdecydowanie duże pole do nadużyć w sferze prywatności. Należy jednak zauważyć, że przykłady działań z ostatnich lat pokazują aktywną postawę wielu instytucji w tym zakresie. Wystarczy wymienić tutaj Information Commissioner's Office[7] czy Commission Nationale de l'Informatique

1 ChatGPT to sztuczna inteligencja oparta na języku naturalnym, która korzysta z technologii GPT (Generative Pretrained Transformer), która pozwala mu na generowanie zrozumiałych i spójnych odpowiedzi na pytania lub komentarze użytkowników (zob. *ChatGPT – Co to jest i jak z tego korzystać?*, https://coderslab.pl/pl/blog/chatgpt-co-to-jest-i-jak-z-tego-korzystac, dostęp: 14.09.2025).

2 Claude AI to chatbot zaprojektowany do przetwarzania języka naturalnego, dzięki czemu lepiej rozumie, analizuje i generuje teksty w sposób zbliżony do języka ludzkiego. Model językowy Claude AI kładzie duży nacisk na etykę oraz bezpieczeństwo w użytkowaniu, co wyróżnia go na tle innych narzędzi sztucznej inteligencji (zob. *Co to jest Claude AI, co oznacza, jaka jest definicja pojęcia w słowniku*, https://www.sempire.pl/co-to-jest-claude-ai.html, dostęp: 14.09.2025).

3 Google Gemini to najnowszy i najbardziej zaawansowany model AI opracowany przez Google. Posiada funkcje multimodalne, co oznacza, że potrafi rozumieć i generować treści w różnych formatach, takich jak tekst, obrazy, dźwięk i wideo (zob. *Co to jest Google Gemini, co oznacza, jaka jest definicja pojęcia w słowniku*, https://www.sempire.pl/co-to-jest-google-gemini.html, dostęp: 14.09.2025).

4 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.Urz. UE L 119 z 4.05.2016, s. 1 ze zm.), dalej: RODO.

5 S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR*, „International Data Privacy Law” 2017, nr 7(2), s. 79–90.

6 Wyrok TSUE z 20 grudnia 2017 r. w sprawie Peter Nowak przeciwko Data Protection Commissioner, C-434/16 (ECLI:EU:C:2017:994).

7 ICO, *Guidance on AI and data protection*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ (dostęp: 14.09.2025).

et des Libertés[8], a także opinię dotyczącą relacji pomiędzy Artificial Intelligence Act[9] a RODO wydaną przez Europejską Radę Ochrony Danych[10]. Należy wyraźnie podkreślić, że AI Act, mimo że wprowadza komplementarne podejście oparte na ryzyku do regulacji systemów, nie zastępuje jednak RODO, lecz uzupełnia je, co oznacza, że organizacje wdrażające AI muszą równocześnie sprostać dwóm zestawom regulacji. Harmonizacja tych dwóch reżimów wymaga od administratorów wdrożenia zintegrowanego systemu zarządzania ryzykiem, który połączy wymogi bezpieczeństwa i jakości danych z wymogami ochrony praw podmiotów danych. Bez takiego spójnego modelu implementacyjnego AI będzie stwarzać chroniczne i trudne do zarządzania napięcie regulacyjne, uniemożliwiające jednoczesne spełnienie wymogów obu aktów prawnych.

Niniejszy artykuł ma na celu przedstawienie punktów styku oraz różnic między RODO a AI Act, omówienie najważniejszych wyzwań praktycznych dla administratorów danych oraz zaprezentowanie rekomendacji, które mogą pomóc w zgodnym z prawem wdrażaniu AI w organizacjach. Podjęta zostanie również próba odpowiedzenia na kluczowe pytanie: jak można pogodzić rewolucję technologiczną z obowiązującymi zasadami ochrony prywatności?

2. Relacja: RODO – AI Act. Konflikt czy komplementarność?

Zasadne w kontekście prowadzonych rozważań jest rozpocząć od przywołania ram prawnych obu omawianych aktów w celu uwidocznienia ich różnic oraz zbieżności. Wprowadzone w 2018 r. RODO stało się fundamentem europejskiego porządku prawnego w zakresie prywatności, ale dopiero przyjęcie w 2024 r. rozporządzenia w sprawie sztucznej inteligencji unaoczniło konieczność stworzenia nowych ram regulacyjnych, obejmujących zarówno kwestie techniczne, jak i etyczne. Co więcej, AI Act wprowadził zupełnie nową kategorię obowiązków dla twórców i użytkowników systemów AI w Unii Europejskiej. Warto zaznaczyć, że RODO, jako najważniejszy akt prawny regulujący zasady przetwarzania danych osobowych w Unii Europejskiej, opiera swoje normatywne podstawy, zgodnie z art. 5 ust. 1–2, na siedmiu fundamentalnych zasadach: (1) zgodności z prawem, rzetelności i przejrzystości, (2) ograniczenia celu, (3) minimalizacji danych, (4) prawidłowości, (5) ograniczenia przechowywania, (6) integralności i poufności oraz (7) rozliczalności. Zestawiając ten zbiór w kontekście sztucznej inteligencji, można zauważyć, że szczególnego znaczenia nabiera zasada rozliczalności z tego względu, że to na administratorze danych spoczywa obowiązek wykazania, iż zachodzące procesy przetwarzania, także te w systemach opartych na uczeniu maszynowym, są zgodne z prawem[11]. Jak podkreśla P. Fajgielski, ponieważ RODO jest aktem prawnym horyzontalnym, „cechuje się neutralnością technologiczną, co oznacza, że jego przepisy stosują się do każdej formy przetwarzania danych, niezależnie od używanej technologii”[12]. Kolejnym ważnym aspektem jest to, że na gruncie RODO problematyczne staje się profilowanie oraz zautomatyzowane podejmowanie decyzji. Problem ten wynika z art. 22 RODO, zgodnie z którym osoba fizyczna nie powinna podlegać decyzji wywołującej wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływającej, jeżeli decyzja ta oparta jest wyłącznie na zautomatyzowanym przetwarzaniu. Jak zauważa TSUE w wyroku z dnia 13 maja 2014 r., ograniczenie

8 CNIL, *Biométrie*, https://www.cnil.fr/fr/biometrie (dostęp: 14.09.2025).

9 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.Urz. UE L 2024/1689 z 12.07.2024), dalej: AI Act.

10 Opinion 28/2024 on the interplay between the AI Act and the GDPR, 2024, https://edpb.europa.eu (dostęp: 14.09.2025).

11 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 2020.

12 P. Fajgielski, *Komentarz do art. 5 ustawy o ochronie danych osobowych*, [w:] tegoż, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. 2, Warszawa 2022, art. 5.

to, w świetle bardzo dynamicznego rozwoju systemów scoringowych, rekrutacyjnych czy kredytowych, ma ogromne znaczenie praktyczne[13]. W tej dyskusji warto zwrócić uwagę na argumentację S. Wachtera i B. Mittelstadta, którzy uważają, że RODO nie tworzy wprost „prawa do wyjaśnienia", lecz jedynie obowiązek zapewnienia minimalnej przejrzystości procesu decyzyjnego[14].

Przechodząc do AI Act, należy zaznaczyć, że jest on pierwszym na świecie aktem prawnym o tak szerokim zakresie regulującym tę technologię. Trzeba też zwrócić uwagę, że w jego motywie 10 określono, iż celem rozporządzenia nie jest wpływanie na stosowanie obowiązującego prawa Unii Europejskiej regulującego przetwarzanie danych osobowych. Fundamentem AI Act jest koncepcja podejścia opartego na ryzyku, co oznacza, że regulacja ta nie traktuje wszystkich systemów AI jednakowo, ale uzależnia wymagania prawne i ograniczenia od tego, jakie ryzyko dla bezpieczeństwa, praw podstawowych i interesu publicznego może spowodować dany system. Dlatego właśnie w art. 5–7 AI Act ustawodawca unijny wyróżnił cztery kategorie ryzyka: systemy niedopuszczalne (zakazane), wysokiego ryzyka, ograniczonego ryzyka oraz minimalnego ryzyka[15]. Warto zaznaczyć, że minimalne ryzyko to większość codziennych systemów AI, które ze względu na niskie ryzyko dla praw podstawowych wiąże się z brakiem dodatkowych regulacji. Natomiast w przypadku wysokiego ryzyka są to systemy, które znacząco wpływają na bezpieczeństwo lub prawa podstawowe, i w stosunku do nich obowiązują ścisłe wymogi, do których zalicza się m.in. przejrzystość czy nadzór człowieka. Należy także podkreślić, że systemy niedopuszczalne są uznane za zbyt niebezpieczne dla praw podstawowych i bezpieczeństwa, a ich użycie jest zabronione (poza bardzo wąskimi wyjątkami przewidzianymi w akcie). Ciekawe jest również to, że AI Act w art. 52 zawiera przepisy dotyczące tzw. *foundation models*[16] i generatywnej AI[17], ponieważ po raz pierwszy wprowadzono regulacje nakazujące oznaczanie treści generowanych przez AI, np. *deepfake*, a także obowiązek udostępniania streszczeń dotyczących wykorzystywanych danych treningowych. Zdaniem M. Veale'a i F. Borgesiusa jest to przełom, który stawia Unię Europejską w roli pioniera w zakresie prawnej i etycznej kontroli nad AI[18].

Podejmując kwestię różnic i podobieństw AI Act oraz RODO, nie można zapominać, że są to akty prawne rangi rozporządzenia, które powinny być stosowane równolegle i są wobec siebie równorzędne. Zasadne jednak jest podkreślenie jednej z ważniejszych różnic obu omawianych aktów, jaką jest fakt, że RODO koncentruje się na ochronie danych osobowych na wszystkich etapach ich przetwarzania, począwszy już od ich zbierania. W AI Act natomiast nacisk położony jest na wynikach wykorzystania sztucznej inteligencji. Choć RODO i AI Act funkcjonują jako odrębne reżimy prawne, to w praktyce można dostrzec, że ich stosowanie będzie miało możliwość przenikania się. AI Act nakłada na dostawców i użytkowników systemów obowiązki związane z przejrzystością i zarządzaniem ryzykiem, które wprost korespondują z zasadami RODO, w tym szczególnie z zasadą rozliczalności i minimalizacji

13 Wyrok TSUE z 13 maja 2014 r., C-131/12, *Google Spain* (ECLI:EU:C:2014:317).

14 S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation*..., s. 76.

15 Tamże.

16 *Foundation models* to modele sztucznej inteligencji, które zostały przeszkolone na szerokim zbiorze danych i są zaprojektowane do wszechstronności w wykonywaniu szerokiej gamy zadań.

17 „W odniesieniu do samodzielnych systemów AI, a mianowicie systemów AI wysokiego ryzyka innych niż te, które są związanymi z bezpieczeństwem elementami produktów lub które same są produktami, należy je klasyfikować jako systemy wysokiego ryzyka, jeżeli w związku z ich przeznaczeniem stwarzają one wysokie ryzyko szkody dla zdrowia i bezpieczeństwa lub praw podstawowych osób, biorąc pod uwagę zarówno dotkliwość potencjalnych szkód, jak i prawdopodobieństwo ich wystąpienia, oraz jeżeli są one wykorzystywane w szeregu ściśle określonych z góry obszarów wskazanych w niniejszym rozporządzeniu. Identyfikacja tych systemów opiera się na tej samej metodyce i kryteriach przewidzianych również w odniesieniu do wszelkich przyszłych zmian w wykazie systemów AI wysokiego ryzyka, do przyjmowania których – w drodze aktów delegowanych – powinna być uprawniona Komisja, aby uwzględniać szybkie tempo rozwoju technologicznego, a także potencjalne zmiany w wykorzystaniu systemów AI" (AI Act, motyw 52).

18 M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, „Computer Law Review International" 2021, nr 22(4), s. 97–112.

danych. Jednocześnie jednak pojawiają się obszary potencjalnych napięć interpretacyjnych, czego przykładem może być obowiązek przejrzystości. AI Act w art. 13 bardzo wyraźnie wymaga, aby systemy wysokiego ryzyka były zaprojektowane w sposób umożliwiający użytkownikom zrozumienie ich działania. RODO natomiast w art. 13 i 14 przewiduje obowiązek informacyjny wobec osób, których dane są przetwarzane. W praktyce może to prowadzić do sytuacji, w której spełnienie wymagań AI Act (np. opisanie algorytmu) nie będzie wystarczające z punktu widzenia RODO, które wymaga jasnej, zrozumiałej i dostępnej dla laika informacji.

Odpowiadając na postawione w podtytule pytanie, należy zaznaczyć, że relacja między RODO a AI Act ma charakter komplementarny, ponieważ oba te akty prawne chronią prawa jednostki w erze cyfrowej, choć koncentrują się na dość różnych aspektach. Co ważne, RODO skupia się na ochronie danych osobowych i prywatności, natomiast AI Act identyfikuje szersze ryzyka związane ze sztuczną inteligencją, m.in. w zakresie niedyskryminacji, transparentności czy bezpieczeństwa systemów wysokiego ryzyka. W praktyce jednak istnieją obszary potencjalnego napięcia, które zostaną opisane w dalszej części tych rozważań.

3. Praktyczne wyzwania

Praktyczne wyzwania na styku RODO i AI Act nie sprowadzają się jedynie do teoretycznych rozważań prawnych, lecz mają bezpośrednie przełożenie na codzienną działalność przedsiębiorstw, instytucji publicznych czy twórców technologii. Dotyczą one zarówno kwestii zgodności formalnej, m.in. w zakresie dokumentacji, oceny ryzyka, jak i problemów technicznych, np. zapewnienia wyjaśnialności modeli czy ograniczenia uprzedzeń przy jednoczesnym respektowaniu kluczowej zasady RODO – minimalizacji danych. Z teoretycznego punktu widzenia AI mogłaby wspierać ochronę jednostki np. przez wykrywanie cyberzagrożeń i szybszą anonimizację. W realiach rynkowych i technologicznych dominują jednak mechanizmy, które tę ochronę podważają. Wskazuje to na problem leżący w celu i architekturze systemów AI, które są projektowane dla efektywności i zysku, a nie dla prywatności. Patrząc na główne wyzwania, należy wymienić: zarządzanie danymi wrażliwymi, ocenę ryzyka, niepewności interpretacyjne czy obciążenia dokumentacyjne.

Zaczynając od niezwykle istotnej kwestii, jaką jest zarządzanie danymi wrażliwymi, które w sposób szczególny dotykają prywatności każdego człowieka, przez co powinny być tym bardziej chronione, trzeba zwrócić uwagę, że AI Act dopuszcza w niektórych sytuacjach przetwarzanie danych należących do tej szczególnej kategorii, np. danych dotyczących zdrowia czy pochodzenia etnicznego. Kwestia ta jest regulowana przez art. 10 ust. 5 – w przypadku systemów wysokiego ryzyka dostawcy mogą przetwarzać dane wrażliwe, jeśli jest to ściśle konieczne do monitorowania, wykrywania i korygowania uprzedzeń, pod warunkiem wdrożenia odpowiednich zabezpieczeń. Dopuszczenie przez AI Act tego typu danych do przetwarzania ma na celu wykrywanie i ograniczanie algorytmicznej dyskryminacji. Natomiast RODO w przypadku dopuszczenia do przetwarzania tego typu danych wymaga wyjątkowych podstaw prawnych, np. zgody podmiotu czy ważnego interesu publicznego. Może to prowadzić do sytuacji, w której AI Act będzie wymagał, aby np. dane treningowe w systemach wysokiego ryzyka były kompletne i reprezentatywne, co może oznaczać konieczność zbierania również cech demograficznych lub innych wrażliwych danych w celu uniknięcia stronniczości. Należy jednak brać pod uwagę, że zbieranie takich danych może być zakazane albo wymagające szczególnej podstawy prawnej według RODO.

Dynamiczny rozwój technologii sprawił, że coraz częściej to systemy AI podejmują ważne decyzje mające wpływ na ludzi, takie jak wyniki rekrutacji czy dostęp do usług publicznych. Może się to wiązać z potencjalnymi dyskryminacjami poprzez projektowanie i użycie algorytmów w sposób nieuwzględniający ryzyk dyskryminacyjnych, a także przez dane historyczne skażone uprzedzeniami, np. wcześniejsze decyzje HR dyskryminujące kobiety lub mniejszości narodowe. Do wykrycia takich sytuacji niezbędne

jest jednak przetwarzanie przez organizacje danych wrażliwych, co zgodnie z art. 9 RODO[19] jest niedozwolone. Powstaje tutaj wyraźny konflikt pomiędzy dwiema kluczowymi wartościami, które są chronione przez Unię Europejską – ochroną danych osobowych i prywatności jednostki a zasadą równego traktowania i zakazem dyskryminacji. Problematykę tę podejmują M. Bekkum i F. Borgesius, którzy podkreślają, że systemy AI mogą prowadzić do dyskryminacji nawet wtedy, gdy formalnie nie wykorzystują danych wrażliwych, poprzez takie mechanizmy, jak dziedziczenie historycznych uprzedzeń oraz atrybuty proxy[20]. Autorzy wskazują, że algorytmy uczą się na danych historycznych, w których decyzje ludzi były stronnicze, tak jak w przypadku rekrutacji[21]. Warto w tym miejscu dodać, że system rekrutacyjny Amazona został porzucony właśnie z tego powodu[22]. W przypadku atrybutów proxy, Bekkum i Borgesius podkreślają jednoznacznie, że nawet w sytuacji, gdy algorytm nie ma dostępu do danych o etniczności czy religii, może korzystać z innych zmiennych silnie z nimi skorelowanych, takich jak kody pocztowe czy wybierana szkoła[23]. Jest to określane jako tzw. dyskryminacja przez przypadek, co może prowadzić do wysnucia refleksji odnoszącej się do paradoksu regulacyjnego, zgodnie z którym zakaz gromadzenia danych wrażliwych tak naprawdę nie eliminuje ryzyka dyskryminacji, ale raczej utrudnia jej wykrywanie i korektę. W tym przypadku warto rozważyć pojawiające się argumenty za i przeciw przetwarzaniu danych wrażliwych. Autorzy tacy jak Borgesius i Bekkum zwracają uwagę, że bez danych wrażliwych nie można rzetelnie sprawdzić, czy dany algorytm dopuszcza się dyskryminacji, oraz że analiza jedynie pośrednich danych daje niepełny obraz działania systemu sztucznej inteligencji[24]. Ponadto podnoszony jest argument, że dzięki wykorzystaniu danych wrażliwych do przetwarzania różne organy antydyskryminacyjne mogłyby zyskać skuteczne narzędzie do egzekwowania prawa w tym zakresie. Patrząc jednak z innej perspektywy, takie działania wiążą się z dużym ryzykiem inwigilacji, *debiasing* może bowiem stać się pretekstem do gromadzenia zbiorów danych wrażliwych, które później znajdą inne zastosowanie. Dodatkowo świadomość, że dany podmiot może przechowywać dane o orientacji seksualnej czy wyznawanej religii, może podważać zaufanie do tej instytucji, nawet jeśli te dane nie zostaną przez niego wykorzystane.

Kolejnym istotnym wyzwaniem w tej tematyce jest kwestia oceny ryzyka. RODO w art. 35[25] wprowadza obowiązek przeprowadzania oceny skutków dla ochrony danych (*Data Protection Impact Assessment*[26]), gdy przetwarzanie to może powodować wysokie ryzyko dla praw i wolności osób fizycznych. AI Act przewiduje natomiast odrębny obowiązek przeprowadzenia oceny ryzyka dla systemów AI wysokiego

19 Art. 9 RODO: „Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby".

20 To cechy, które same w sobie nie są chronionymi kategoriami (np. płeć, rasa, religia), ale są z nimi silnie skorelowane i mogą pośrednio ujawniać te informacje (zob. S. Yeom, A. Datta, M. Fredrikson, *Hunting for Discriminatory Proxies in Linear Regression Models*, [w:] *Advances in Neural Information Processing Systems*, red. S. Koyejo i in., 2018.

21 M. Van Bekkum, F. Zuiderveen Borgesius, *Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?*, „Computer Law & Security Review" 2022, nr 48, s. 1–12.

22 Więcej na ten temat: https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/?utm_source=chatgpt.com (dostęp: 17.09.2025).

23 M. Van Bekkum, F. Zuiderveen Borgesius, *Using Sensitive Data*..., s. 4–11.

24 Tamże.

25 Art. 35 RODO: „Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę".

26 Data Protection Impact Assessment, czyli ocena skutków dla ochrony danych osobowych, która jest wymagana, gdy przetwarzanie danych może stwarzać wysokie ryzyko dla praw i wolności osób, np. przy użyciu AI do profilowania ludzi (dalej: DPIA).

ryzyka, obejmujący m.in. analizę bezpieczeństwa, jakości danych, transparentności czy nadzoru ludzkiego[27]. W praktyce skutkuje to tym, że organizacje muszą łączyć dwa różne reżimy oceny, co zwiększa obciążenie administracyjne, a jednocześnie wymaga opracowania spójnej metodologii, aby uniknąć powtarzania i powielania procedur. Wiadomo, że ocena ryzyka stanowi kluczowy element zarówno AI Act, jak i RODO, mający na celu ochronę osób fizycznych przed potencjalnymi zagrożeniami związanymi z systemami AI. Jednakże różnice w zakresie stosowania, metodologii oraz w wymogach dokumentacyjnych obu regulacji mogą prowadzić do praktycznych trudności w ich równoczesnym stosowaniu. Przede wszystkim należy zwrócić uwagę, że systemy AI bardzo często działają na podstawie skomplikowanych modeli matematycznych, których działanie może być trudne do przewidzenia. W związku z tym ocena ryzyka związanego z takimi systemami wymaga zaawansowanej wiedzy technicznej oraz dostępu do danych wejściowych i procesów decyzyjnych systemu. Ponadto należy pamiętać, że ryzyka związane z AI mogą obejmować nie tylko bezpośrednie zagrożenia dla osób fizycznych, ale także pośrednie efekty społeczne, takie jak dyskryminacja czy utrata zaufania do instytucji. Jak zauważają m.in. Rintamäki i współpracownicy[28], FRIA w ramach AI Act koncentruje się na szerokim zakresie praw podstawowych, takich jak prawo do niedyskryminacji, prawo do prywatności czy prawo do sprawiedliwego procesu, podczas gdy DPIA w ramach RODO skupia się głównie na ochronie danych osobowych. Ponadto AI Act wprowadza bardziej szczegółowe wymagania dotyczące dokumentacji i audytowalności ocen ryzyka[29]. Wspomniani wcześniej autorzy zwracają również uwagę na wiele wyzwań związanych z równoczesnym stosowaniem DPIA i FRIA, w tym szczególnie na konieczność stosowania podwójnej dokumentacji, potencjalne powielanie działań oceny ryzyka oraz trudności w integracji różnych podejść metodologicznych. Dodatkowo przedstawiają oni praktyczne zalecenia w postaci sugestii opracowania narzędzi i procedur umożliwiających efektywne zarządzanie takimi obowiązkami. Pokazuje to, że problematyka oceny ryzyka w kontekście RODO oraz AI Act jest bardzo złożona i wielowymiarowa oraz że łączy w sobie zarówno aspekty prawne, jak i techniczne oraz społeczne. W praktycznym ujęciu wymaga ona strategicznego podejścia, zestawu zintegrowanych narzędzi, a także procesów oraz ścisłej współpracy zespołów zajmujących się kwestiami prawnymi i technicznymi.

Przechodząc do ostatniej już kwestii rozważanej w kontekście wyzwań praktycznych, należy zwrócić uwagę, że AI Act i RODO różnią się w zakresie definicji, celów i podejść do ochrony danych osobowych i praw podstawowych. Jak już wspomniano, RODO koncentruje się na ochronie danych osobowych, podczas gdy AI Act skupia się na zarządzaniu ryzykiem związanym z systemami sztucznej inteligencji. Te różnice mogą prowadzić do poważnych niejasności w kwestii stosowania obu tych regulacji w praktyce. Dodatkowo należy zwrócić uwagę, że brak spójności w terminologii i definicjach może znacząco utrudniać interpretację przepisów i ich zastosowanie w konkretnych przypadkach. Istotnym szczegółem jest również to, że AI Act nakłada na dostawców systemów AI obowiązek prowadzenia szczegółowej dokumentacji, która obejmuje m.in. ocenę ryzyka, procedury monitorowania oraz informacje dotyczące danych wejściowych i wyników systemu. Poza tym relewantne jest, że w przypadku systemów wysokiego ryzyka, takich jak te, które zajmują się przetwarzaniem danych wrażliwych, dokumentacja musi być wyjątkowo szczegółowa. Należy także uwzględnić, że wymogi dokumentacyjne określone w AI Act mogą prowadzić do znacznego obciążenia administracyjnego dla organizacji, zwłaszcza w kontekście przetwarzania właśnie danych wrażliwych.

Konieczność sporządzania i aktualizowania dokumentacji z pewnością pochłania znaczne zasoby zarówno ludzkie, jak i finansowe, co może utrudniać efektywne zarządzanie zgodnością z regulacjami.

27 Fundamental Rights Impact Assessment, czyli ocena wpływu na prawa podstawowe, która jest związana z AI Act i polega na analizie, czy stosowanie systemów AI może naruszać prawa człowieka lub podstawowe wolności (dalej: FRIA).

28 T. Rintamäki, D. Golpayegani, D. Lewis, E. Celeste, H.J. Pandit, *Impact Assessment Requirements in the GDPR vs the AI Act*, 2025, s. 11–28.

29 Tamże.

Według badania przeprowadzanego przez B. Paala przeciążenie dokumentacyjne wynika przede wszystkim z kumulacji wymogów regulacyjnych, które nakładają obowiązki szczegółowego raportowania i dokumentowania działań związanych z przetwarzaniem danych[30]. Interesujące jest również to, że zdaniem Paala dokumentacja nie powinna spełniać jedynie wymogów formalnych, ale realnie wspierać ocenę ryzyka, audyt oraz nadzór. Dodatkowo autor sugeruje bardzo intersującą kwestię, ponieważ uważa on, że w niektórych przypadkach dokumentacja staje się celem samym w sobie – „by mieć dokumentację" – ale niekoniecznie użyteczną. B. Paal wskazuje także, że ogólność RODO powoduje, iż organizacje często nie wiedzą, jak dalekie kroki powinny podejmować w kwestii tego, co należy dokumentować i jakie standardy techniczne zastosować[31]. Dlatego autor rozważa możliwość wprowadzenia nowych podstaw prawnych lub interpretacji, które lepiej uwzględniałyby AI, aby złagodzić obciążenie, ale jednocześnie zachować ochronę prywatności, sugerując konieczność ustanowienia odrębnej podstawy prawnej – jednej dla wszystkich operacji AI. Wskazuje, że jest to szczególnie ważne dla tych procesów, które wymagają dużej ilości danych albo które obejmują profilowanie, uczenie ciągłe i adaptację. Badacz wskazuje też kolejną istotną kwestię: regulacje powinny być interpretowane proporcjonalnie, a środki związane z dokumentacją, DPIA oraz obowiązki transparentności powinny być skalowane w zależności od ryzyka, dostępności środków, wielkości organizacji, typu AI w taki sposób, aby nie hamowały one innowacji. Jednocześnie ważne jest, aby środki te chroniły prawa osób, których dotyczą te dane. Tożsame refleksje ma M. Winau, która również uważa, że AI Act nie przewiduje wystarczająco jasno, jak rozstrzygać konflikty norm między nim a RODO, oraz że brakuje konkretnych przepisów proceduralnych, które umożliwiłyby taką koordynację[32].

Przeprowadzone rozważania ujawniają poważne wyzwania, jakimi bez wątpienia są niepewności interpretacyjne oraz przeciążenie dokumentacyjne. Paal podkreśla, że ogólność i nieostrość regulacji RODO, zwłaszcza w kontekście specyfiki uczenia maszynowego, prowadzą do istotnego braku pewności prawnej, co z kolei zmusza podmioty do gromadzenia nadmiernej dokumentacji, często o charakterze formalnym, lecz niekoniecznie realnie zwiększającej poziom ochrony danych. Trafne w tym kontekście jest stwierdzenie D. Lubasza, że RODO w tradycyjnym ujęciu, choć jest prawem celowym, jest metodologicznie niedostosowane do tempa i autonomii AI, gdyż skuteczność RODO nie może się opierać na kontroli *ex-post*, lecz musi być zapewniona poprzez integralność ochrony danych na etapie projektowania[33]. Winau wskazuje, że obowiązki wynikające z AI Act, takie jak wymóg zapewnienia kompletności i reprezentatywności zbiorów danych, mogą pozostawać w sprzeczności z zasadą minimalizacji danych przewidzianą w art. 5 ust. 1 lit. c RODO[34], co prowadzi do dodatkowych napięć i ryzyka dublowania wymogów dokumentacyjnych. W konsekwencji równoległe stosowanie obu regulacji może powodować zarówno wzrost kosztów zgodności, jak i wątpliwości co do priorytetów normatywnych. W tym przypadku ważna i konieczna jest koordynacja i harmonizacja instrumentów interpretacyjnych, tak aby uniknąć powielania lub wzajemnego wykluczania się obowiązków, a także dostosowanie wymogów dokumentacyjnych do zasady proporcjonalności przy jednoczesnym uwzględnieniu dostępnych zasobów danego podmiotu, ryzyka oraz skali działania.

30 B.P. Paal, *Artificial Intelligence as a Challenge for Data Protection Law – and vice versa*, [w:] *The Cambridge Handbook of Responsible Artificial Intelligence*, red. S. Voeneky, P. Kellmeyer, O. Mueller, W. Burgard, Cambridge 2022, s. 290–308.

31 Tamże, s. 292–306.

32 M. Winau, *Areas of Tension in the Application of AI and Data Protection Law: On the Lack of Substantive Balancing and Coordinated Legal Concretisation in the European Commission's Proposal for a Regulation on AI*, „European Data Protection Law Review" 2023, t. 9, nr 2, s. 123–135.

33 D. Lubasz, *RODO dla AI. Zgodność z zasadami godnej zaufania sztucznej inteligencji w modelu data protection by design*, Warszawa 2025, s. 110–120.

34 Dane muszą być: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

4. Propozycje rozwiązań

W obliczu praktycznych wyzwań wynikających z równoległego stosowania AI Act i RODO kluczowe, moim zdaniem, jest przyjęcie podejścia opartego na koordynacji, proporcjonalności i standaryzacji. Przede wszystkim konieczne jest wypracowanie zintegrowanych wytycznych interpretacyjnych ze strony organów nadzorczych, m.in. Komisji Europejskiej, które jednoznacznie ujednolicałyby rozumienie takich pojęć, jak „kompletność danych" czy „minimalizacja danych". Ponadto, na podstawie przywoływanych refleksji, można wysnuć wniosek, że ocena ryzyka powinna być zintegrowana i należy odejść od prowadzenia odrębnych procedur DPIA i analiz ryzyka wymaganego przez AI Act. Warto także rozważyć stworzenie jednolitego narzędzia oceny, które redukowałoby potencjalne obciążenia dokumentacyjne. W kwestii obowiązków dokumentacyjnych uważam, że należy uwzględnić przy ich projektowaniu zasadę proporcjonalności, bardziej szczegółowe wymogi powinny bowiem dotyczyć systemów wysokiego ryzyka i dużych podmiotów. Natomiast mniejsze organizacje powinny mieć dostęp do uproszczonych szablonów. Dodatkowo warto rozważyć, aby w perspektywie regulacyjnej doprecyzować podstawy prawne dla AI w ramach RODO lub stworzyć nowe wyjątki, które pozwoliłyby na zgodne i odpowiedzialne wykorzystywanie np. danych wrażliwych w procesie trenowania modeli. Takie podejście pozwoli uniknąć nadmiernego formalizmu, a jednocześnie zapewnić realną ochronę praw osób, których te dane dotyczą. Dzięki wprowadzeniu takich rozwiązań będzie możliwe ograniczenie wielu niepewności interpretacyjnych i ułatwienie podmiotom praktycznego wdrożenia zgodnych z prawem, a jednocześnie etycznych, rozwiązań opartych na sztucznej inteligencji.

5. Podsumowanie

Analiza relacji pomiędzy RODO a AI Act może prowadzić do wniosku, że obecnie nie mamy do czynienia z prostym konfliktem norm, ale z komplementarnością dwóch reżimów prawnych, które z różnych perspektyw próbują odpowiedzieć na wyzwania związane z nowymi technologiami. RODO koncentruje się przede wszystkim na ochronie danych osobowych jednostki, podczas gdy AI Act stawia w centrum zarządzanie ryzykiem technologicznym i społecznym, co razem tworzy podwójną warstwę zabezpieczeń. Jej głównym zadaniem jest nie tylko formalne zapewnienie zgodności z prawem, ale także budowanie zaufania społecznego do systemów AI. Jednakże jest wyraźnie widoczne, że pogodzenie obu tych aktów w praktyce rodzi liczne wyzwania. DPIA i ocena ryzyka przewidziana w AI Act mogą prowadzić do powielania procedur, o ile nie zostaną opracowane przemyślane mechanizmy ich integracji. Istotne zdanie na ten temat wyrażają Veale i Borgesius, którzy podkreślają, że AI Act może stać się narzędziem kształtowania kultury „odpowiedzialnej innowacji" w Europie, ale tylko wówczas, gdy będzie implementowany w ścisłej synergii z RODO[35].

W poszukiwaniu odpowiedzi na pytanie, jak pogodzić rewolucję technologiczną z obowiązującymi zasadami ochrony prywatności, należy raczej skupić się na procesie ciągłego dostosowywania zarówno prawa, jak i technologii oraz praktyki organizacyjnej. Dzięki temu będzie możliwe stworzenie spójnego systemu, w którym RODO będzie chronić jednostkę, a AI Act zabezpieczać społeczeństwo przed systemowymi ryzykami. W tym kontekście warto m.in. rozważyć podjęcie badań na temat tego, czy techniczne rozwiązania wyjaśnialności AI faktycznie spełniają prawny wymóg zrozumiałości i użyteczności dla jednostki. Wyniki takich badań umożliwiłyby tworzenie normatywnych wzorców projektowych interfejsów dla systemów AI, co bezpośrednio wpłynęłoby na ciągłe dostosowywanie praktyki inżynierskiej do realizacji prawnych celów RODO. Dzięki takim rozwiązaniom Europa miałaby szansę wyznaczyć nowy, globalny standard regulacyjny, który połączy innowacyjność z poszanowaniem praw

35 M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*..., s. 97–112.

człowieka. Skutki takich rozwiązań jeszcze wyraźnie podkreśliłyby różnice w podejściu Europy – tworzącej standardy rozwoju AI przy jednoczesnym poszanowaniu praw człowieka, w stosunku do Stanów Zjednoczonych, które postawiły rozwój AI ponad wszelkie prawa do ochrony prywatności jednostek.

Bibliografia

Bekkum M. Van, Zuiderveen Borgesius F., *Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?*, „Computer Law & Security Review" 2022, nr 48.

Fajgielski P., *Komentarz do art. 5 ustawy o ochronie danych osobowych*, [w:] tegoż, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. 2, Warszawa 2022.

Lubasz D., *RODO dla AI. Zgodność z zasadami godnej zaufania sztucznej inteligencji w modelu data protection by design*, Warszawa 2025.

Paal B.P., *Artificial Intelligence as a Challenge for Data Protection Law – and vice versa*, [w:] *The Cambridge Handbook of Responsible Artificial Intelligence*, red. S. Voeneky, P. Kellmeyer, O. Mueller, W. Burgard, Cambridge 2022.

Rintamäki T., Golpayegani D., Lewis D., Celeste E., Pandit H.J., *Impact Assessment Requirements in the GDPR vs the AI Act*, 2025.

Veale M., Zuiderveen Borgesius F., *Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, „Computer Law Review International" 2021, nr 22(4).

Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR*, „International Data Privacy Law" 2017, nr 7(2).

Winau M., *Areas of Tension in the Application of AI and Data Protection Law: On the Lack of Substantive Balancing and Coordinated Legal Concretisation in the European Commission's Proposal for a Regulation on AI*, „European Data Protection Law Review" 2023, t. 9, nr 2.

Yeom S., Datta A., Fredrikson M., *Hunting for Discriminatory Proxies in Linear Regression Models*, [w:] *Advances in Neural Information Processing Systems*, red. S. Koyejo i in., 2018.

Źródła internetowe

ChatGPT – Co to jest i jak z tego korzystać?, https://coderslab.pl/pl/blog/chatgpt-co-to-jest-i-jak-z-tego-korzystac (dostęp: 14.09.2025).

CNIL, *Biométrie*, https://www.cnil.fr/fr/biometrie (dostęp: 14.09.2025).

Co to jest Claude AI, co oznacza, jaka jest definicja pojęcia w słowniku, https://www.sempire.pl/co-to-jest-claude-ai.html (dostęp: 14.09.2025).

Co to jest Google Gemini, co oznacza, jaka jest definicja pojęcia w słowniku, https://www.sempire.pl/co-to-jest-google-gemini.html (dostęp: 14.09.2025).

EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (dostęp: 6.02.2026).

ICO, *Guidance on AI and data protection*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ (dostęp: 14.09.2025).

Opinion 28/2024 on the interplay between the AI Act and the GDPR, 2024, https://edpb.europa.eu (dostęp: 14.09.2025).

Akty prawne

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.Urz. UE L 119 z 4.05.2016, s. 1 ze zm.).

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.Urz. UE L 2024/1689 z 12.07.2024).

Orzecznictwo

Wyrok TSUE z 13 maja 2014 r., C-131/12, *Google Spain* (ECLI:EU:C:2014:317).

Wyrok TSUE z 20 grudnia 2017 r., C-434/16, *Peter Nowak przeciwko Data Protection Commissioner* (ECLI:EU:C:2017:994).