„Krytyka Prawa", tom 18, nr 1/2026, s. 98–114, ISSN 2080-1084, e-ISSN 2450-7938, © 2026 Author.

ELIZA ARENTOWSKA[1]

Prawo do bycia zapomnianym w erze AI: Czy pełne usunięcie danych z modelu sztucznej inteligencji jest możliwe?[2]

Wpłynął: 19.06.2025. Akceptacja: 11.02.2026

Streszczenie

Celem artykułu jest zbadanie ograniczeń zawartych w art. 17 RODO dotyczących prawa do bycia zapomnianym, a także możliwości technicznych usunięcia danych z algorytmów sztucznej inteligencji. Wybór tego tematu jest aktualny i trafny w związku z wprowadzeniem rozporządzenia Artificial Intelligence Act[3] (w skrócie AI Act), które jest rozszerzeniem obowiązujących przepisów Unii Europejskiej, skupiającym się na zagadnieniu sztucznej inteligencji oraz ochrony danych osobowych[4]. W artykule wskazano, że aktualne ograniczenia technologiczne uniemożliwiają pełną realizację obowiązku usunięcia danych treningowych z modeli sztucznej inteligencji.

Słowa kluczowe: sztuczna inteligencja, prawo do bycia zapomnianym, RODO, AI ACT, unlearning.

[1] Eliza Arentowska – Uniwersytet im. Adama Mickiewicza w Poznaniu (Polska), e-mail: eliza.arentowska@gmail.com

[2] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Artificial Intelligence Act) oraz zmieniające rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/30/UE, 2014/53/UE i 2014/90/UE.

[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).

„Krytyka Prawa", tom 18, nr 1/2026, s. 98–114, ISSN 2080-1084, e-ISSN 2450-7938, © 2026 Author.

ELIZA ARENTOWSKA

The right to be forgotten in the age of AI: Is it possible to completely remove data from an artificial intelligence model?[5]

Abstract

The aim of the article is to examine the limitations set out in Article 17 of the GDPR concerning the right to be forgotten, as well as the technical capabilities of data removal from artificial intelligence algorithms. The choice of this topic is current and relevant in light of the introduction of the Artificial Intelligence Act (AI Act), which is an extension of the existing European Union regulations, focusing on the issue of artificial intelligence and the protection of personal data.[6] The article concludes that, in light of existing technological limitations, the complete erasure of training data from AI models remains unattainable in practice.

Keywords: artificial intelligence, right to be forgotten, GDPR, AI ACT, unlearning.

5 The research in this article has not been supported financially by any institution.

6 *Ibidem*.

 DOI: 10.7206/kp.2080-1084.837

Wprowadzenie

Prawo do ochrony danych osobowych stanowi jedno z podstawowych praw człowieka, gwarantowane przez Unię Europejską na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., stosowanego od dnia 25 maja 2018 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz w sprawie swobodnego przepływu takich danych, uchylającego dyrektywę 95/46/WE[7]. Jednym z celów aktu jest zapewnienie jednostkom kontroli nad ich danymi osobowymi oraz sposobem ich przetwarzania[8], co ma kluczowe znaczenie w dobie cyfryzacji i szybkiego rozwoju technologii. W związku z tym w rozporządzeniu znalazła się regulacja zawarta w art. 17[9], wprowadzając prawo do usunięcia danych, zwane także „prawem do bycia zapomnianym". Na jego podstawie osoba, której dane dotyczą, ma prawo żądać od administratora ich usunięcia z bazy danych.

Zasadniczym celem niniejszego tekstu jest próba odpowiedzi na pytanie, czy systemy sztucznej inteligencji są w stanie spełnić wymogi wynikające z art. 17 RODO dotyczące prawa do bycia zapomnianym. Wątpliwości budzi bowiem fakt, iż wspomniany art. 17 nakłada na administratora danych obowiązek usunięcia całości danych osobowych na żądanie osoby, której dane dotyczą[10]. Jednakże w przypadku algorytmów sztucznej inteligencji jest to proces znacznie bardziej skomplikowany[11]. Dane wykorzystane do trenowania modeli AI mogą nie być przechowywane w swojej oryginalnej formie, lecz mimo to nadal mają możliwość

---

7 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO).

8 Por. motyw 7 i 10 preambuły RODO, w których podkreśla się potrzebę zapewnienia osobom fizycznym kontroli nad swoimi danymi osobowymi.

9 Zob. art. 17 RODO – prawo do usunięcia danych („prawo do bycia zapomnianym").

10 Zob. art. 17 ust. 1 RODO – m.in. obowiązek usunięcia danych, które „nie są już niezbędne do celów, w których zostały zebrane", lub na żądanie osoby, której dane dotyczą. Por. P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 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)*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022, art. 17. Pozyskano z: https://sip.lex.pl/#/commentary/587773161/670989/fajgielski-pawel-komentarz-do-rozporzadzenia-nr-2016-679-w-sprawie-ochrony-osob-fizycznych-w...?cm=URELATIONS (dostęp: 07.04.2025).

11 Por. E. Fosch-Villaronga, P. Kieseberg, T. Li, *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, "Computer Law & Security Review" 2018, 34(2), s. 304–313.

wpływania na strukturę algorytmu[12]. Zaistniały stan rzeczy budzi wątpliwości co do skuteczności mechanizmów całkowitego usunięcia danych oraz o skutecznego egzekwowania prawa do bycia zapomnianym.

Pierwsza część artykułu zawiera analizę art. 17 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., z uwzględnieniem obowiązków nałożonych na administratorów danych, którzy są zobowiązani do podejmowania określonych działań w zakresie realizacji prawa do bycia zapomnianym. Natomiast druga część dotyczy zagadnień związanych ze sztuczną inteligencją oraz zawiera konfrontację z wymogami znajdującymi się w art. 17 RODO.

W przygotowaniu artykułu zastosowano metodologię prawno-dogmatyczną, popartą literaturą interdyscyplinarną.

Charakterystyka obowiązków administratora danych w świetle art. 17 RODO

RODO, czyli ogólne rozporządzenie o ochronie danych osobowych, jest stosowane od dnia 25 maja 2018 r., stanowiąc fundamentalny akt prawny regulujący ochronę danych osobowych w Unii Europejskiej. Rozporządzenie to wprowadziło jednolite zasady ochrony danych we wszystkich państwach członkowskich UE, wzmacniając prawa obywateli do kontroli nad swoimi danymi osobowymi. RODO przyznało jednostkom szereg praw, w tym prawo dostępu do danych, prawo do ich sprostowania, prawo do ograniczenia ich przetwarzania oraz prawo do bycia zapomnianym. Wprowadzenie RODO miało istotny wpływ na przedsiębiorstwa i instytucje, które są zobowiązane do zapewnienia zgodności z jego przepisami poprzez wdrożenie odpowiednich mechanizmów ochrony danych. RODO nakłada również surowe sankcje finansowe za naruszenia, co motywuje podmioty do starannego przestrzegania przepisów dotyczących ochrony danych, jednakże zawsze istnieje ryzyko, że niektóre naruszenia przepisów nie zostaną skutecznie powstrzymane[13].

Zgodnie z przepisami RODO dane osobowe mogą być zbierane i przetwarzane jedynie w sytuacjach, gdy jest to zgodne z określonymi i legalnymi celami, które mają uzasadnienie prawne. Podmioty zajmujące się przetwarzaniem danych muszą przestrzegać zasad ochrony prywatności, dzięki temu zapewniając użytkowników, iż dane osobowe nie będą wykorzystywane w sposób sprzeczny z prawem. Dane

---

12 Por. E. Kosta, O.J. Gstrein, *The Ethical and Legal Implications of AI Development and Data Processing*, "Journal of Data Protection & Privacy" 2020, 4(2), s. 130–133.

13 Zob. A. Pązik, *Prawo sztucznej inteligencji i nowych technologii, Roszczenie(?) z art.79 RODO jako środek ochrony przed bezprawnym przetwarzanie danych osobowych z wykorzystaniem nowych technologii*, Warszawa 2021, s. 447.

 DOI: 10.7206/kp.2080-1084.837

osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[14]. Zgodnie z art. 4 pkt 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO), osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności poprzez odniesienie do takiego identyfikatora jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub do jednego bądź kilku szczególnych czynników określających tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tej osoby[15].

Prawo do bycia zapomnianym wywodzi się z potrzeby ochrony prywatności jednostki w erze cyfrowej, gdzie dane osobowe są przetwarzane na niespotykaną dotąd skalę[16]. Geneza tego prawa sięga orzeczenia Trybunału Sprawiedliwości Unii Europejskiej z 2014 r. w sprawie Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) oraz Mario Costeja González, gdzie Trybunał uznał, że jednostki mają prawo do usunięcia informacji o sobie z wyników wyszukiwania, jeśli są one nieaktualne, nieistotne lub nadmierne w kontekście celu przetwarzania danych osobowych[17].

Formalizacja prawa do bycia zapomnianym nastąpiła wraz z wejściem w życie RODO, które w art. 17 ustanowiło prawo do usunięcia danych. Zgodnie z tym przepisem osoba fizyczna[18] może żądać od administratora usunięcia danych , m.in. wtedy, gdy dane nie są już niezbędne do celów, dla których zostały zebrane, gdy osoba wyrazi chęć wycofania zgody na ich przetwarzanie, gdy dane były przetwarzane niezgodnie z prawem, lub gdy wystąpiły inne uzasadnione przyczyny przewidziane przez RODO. W ujęciu prawnym art. 17 RODO stanowi narzędzie równoważące ochronę prywatności z innymi prawami, takimi jak wolność wypowiedzi i dostęp do informacji[19]. Pomimo swoich zalet realizacja tego prawa wiąże się z wieloma wyzwaniami, zwłaszcza w zakresie określenia jego granic oraz wyjątków w przypadku, gdy dane są niezbędne do realizacji prawa do informacji lub wypełnienia obowiązku prawnego. Zagwarantowanie prawa do bycia

---

14 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), art. 4 ust. 1.

15 *Ibidem*.

16 European Data Protection Supervisor. (2021). *EDPS Report on the State of Data Protection in the EU*. Pozyskano z: https://edps.europa.eu, https://www.edps.europa.eu/annual-reports_en.

17 Zob. Wyrok TSUE z 13 V 2014 r. w sprawie C 131/12 Google Spain i Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) i Mario Costeja Gonzalez. Pozyskano z: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:62012CJ0131.

18 Zob. Motyw 14 RODO; por. M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym*, Wrocław 2021.

19 M. Czerniawski, *Komentarz do art. 17 RODO*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018. Pozyskano z: https://sip.lex.pl/komentarze-i-publikacje/komentarze/rodo-ogolne-rozporzadzenie-o-ochronie-danych-komentarz-587747142; por. motyw 65 RODO, który wskazuje na konieczność uwzględnienia prawa do bycia zapomnianym w kontekście innych praw podstawowych, takich jak wolność wypowiedzi i informacji.

zapomnianym nakłada na administratorów danych stosowanie odpowiednich procedur i mechanizmów technicznych, które umożliwią skuteczną realizację żądania usunięcia danych[20].

Administratorzy danych odgrywają kluczową rolę w realizacji prawa do bycia zapomnianym, odpowiadając za wdrożenie skutecznych procedur dążących do identyfikacji oraz usunięcia danych zgodnie z żądaniami osób fizycznych. Administratorami danych są „osoby fizyczne lub prawne, organy publiczne, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych"[21]. Przetwarzanie danych musi odbywać się z poszanowaniem zasad ochrony prywatności, a dane nie mogą być wykorzystywane w sposób sprzeczny z prawem. Prawo do usunięcia danych osobowych znajduje zastosowanie w sytuacjach, w których dalsze przetwarzanie danych traci swoją podstawę prawną lub faktyczną. Dotyczy to w szczególności przypadków, gdy dane osobowe przestają być niezbędne dla realizacji celu, w jakim zostały zgromadzone, osoba, której dane dotyczą, skutecznie cofa udzieloną zgodę, przetwarzanie odbywa się z naruszeniem przepisów o ochronie danych osobowych lub gdy na administratorze ciąży obowiązek prawny wymagający usunięcia danych.[22].

Problem stanowi również kontynuowanie lub ponowne przetwarzanie danych osobowych mimo wyczerpania przesłanek uzasadniających ich pierwotne gromadzenie. Dalsze przetwarzanie danych może być uznane za zgodne z pierwotnym celem ich zbierania, jeśli odbywa się w ramach badań naukowych, historycznych lub statystycznych. Niemniej nie ma precyzyjnej definicji tego, co stanowi badania naukowe, a to stwarza ryzyko, że rozwój systemów sztucznej inteligencji w sytuacjach nieuzasadnionych mógłby zostać zakwalifikowany jako działalność badawcza. Warto jednak zaznaczyć, że gdy model AI jest już statyczny i wdrożony, dalsze gromadzenie danych w tym kontekście nie powinno być traktowane jako badania[23].

Prawo do bycia zapomnianym, choć istotne dla ochrony danych osobowych, nie jest absolutne[24] i podlega pewnym ograniczeniom, które wynikają z konieczności ochrony innych wartości prawnych i społecznych. Przetwarzanie danych jest niezbędne ze względu na korzystanie z prawa do wolności wypowiedzi,

---

20 Por. A. Popowicz-Pazdej, *Why the Generative AI Models Do Not Like the Right to Be Forgotten: A Study of Proportionality of Identified Limitations*, „Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza" 2023, t. 15, s. 223–227.

21 Art. 4 pkt 7 RODO. Zob. na ten temat M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO*, Wrocław, 2019 r., s. 9 i n.

22 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).

23 E. Kosta, O.J. Gstrein, *The Ethical and Legal Implications…*, s. 130–133.

24 Zob. A. Popowicz-Pazdej, *Why the Generative AI Models Do Not Like the Right to Be Forgotten: A Study of Proportionality of Identified Limitations*, „Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza" 2023, t. 15, s. 218.

 DOI: 10.7206/kp.2080-1084.837

interes publiczny, obowiązki prawne, badania naukowe, historyczne i statystyczne, dochodzenie lub obronę roszczeń prawnych, zadania realizowane w ramach sprawowania władzy publicznej. Administratorzy muszą wykazywać się nie tylko wrażliwością na prawa jednostki, ale także umiejętnością równoważenia interesów różnych stron, co często wymaga indywidualnego podejścia do każdego przypadku.

Prawo do bycia zapomnianym wymaga, aby osoba fizyczna złożyła wniosek o usunięcie danych do administratora, który musi zapewnić łatwo dostępne środki do składania takich wniosków. Brak wskazania przez ustawodawcę konkretnej formy oraz obligatoryjnych elementów wniosku wprowadza dobrowolność wniesienia żądania, należy jednak zwrócić uwagę, aby wniesiony wniosek dawał możliwość weryfikacji tożsamości osoby składającej żądanie[25]. Administrator po otrzymaniu wniosku ocenia jego zasadność, uwzględniając podstawy prawne oraz możliwe wyjątki. Jeśli wniosek jest zasadny, dane powinny zostać usunięte „bez zbędnej zwłoki"[26] zarówno z aktywnych baz, jak i kopii zapasowych, a osoba wnioskująca powinna zostać w sposób zrozumiały poinformowana o czynnościach[27]. Zwrot „bez zbędnej zwłoki" zawarty w art. 17 w praktyce oznacza czas około miesiąca do dwóch miesięcy w przypadku zawiłych spraw, co określa art. 12 ust. 3 RODO.

Sztuczna inteligencja a przetwarzanie danych osobowych

Dynamiczny rozwój sztucznej inteligencji (AI) w coraz większym stopniu wpływa na różne aspekty życia codziennego. Rosnąca potrzeba automatyzacji i usprawnienia rutynowych czynności wiąże się jednak z ryzykiem niekontrolowanego udostępniania danych osobowych, które we współczesnym świecie uzyskały status cennego zasobu[28]. Obawy dotyczące ochrony prywatności są w pełni uzasadnione i stanowią istotne wyzwanie dla administratorów danych osobowych. Dotychczasowe działania w dziedzinie AI koncentrowały się głównie na poprawie efektywności algorytmów, w tym zwiększeniu szybkości reakcji oraz rozwijania umiejętności samodzielnego uczenia. Tradycyjny paradygmat opiera się na uczeniu maszynowym, które zakłada, że algorytmy AI uczą się rozpoznawać wzorce

25 Zob. M. Jabłoński, J. Węgrzyn, *Prawo do bycia* zapomnianym, Wrocław 2021; por. https://sylwiaczub.pl/wniosek-o-usuniecie-danych-osobowych-wedlug-rodo/ (dostęp: 10.09.2021).

26 Art. 17 RODO, również art. 12 ust. 3 RODO.

27 Por. art. 19 RODO.

28 J. Lubacha, B. Mäihäniemi, R. Wisła (red.), *The European Digital Economy: Drivers of Digital Transition and Economic Recovery*, London 2023, s. 34.

oraz zależności z dostępnych zbiorów danych. Dzięki temu możliwe staje się formułowanie trafnych prognoz lub podejmowanie decyzji w nowych, nieznanych sytuacjach, na podstawie wcześniej zgromadzonych danych[29]. Warto również zwrócić uwagę na pojęcia związane ze zgodą oraz informowaniem o przetwarzaniu danych osobowych użytkownika[30]. W kontekście sztucznej inteligencji kwestie te nie są do końca klarowne ze względu na ciągłe zmiany zachodzące w algorytmach adaptacyjnych[31].

Proces trenowania modeli sztucznej inteligencji (AI) polega na dostarczeniu algorytmom odpowiednich danych, które umożliwiają im uczenie się, formułowanie **wniosków, co skutkuje doskonaleniem osiągniętych wyników**. W przypadku algorytmów uczenia maszynowego (*machine learning*) dane te są kluczowym elementem procesu, który decyduje o zdolności modelu do precyzyjnej analizy i trafnych prognoz. Dane osobowe, jeśli są wykorzystywane, odgrywają istotną rolę w trenowaniu modeli AI, przede wszystkim w usługach spersonalizowanych, systemów rekomendacyjnych, rozpoznawania obrazów czy przetwarzania języka naturalnego. Podczas trenowania modeli AI dane osobowe są wykorzystywane jako materiał wejściowy, na podstawie którego algorytmy uczą się wzorców i zależności w danych. Na przykład w systemach rekomendacyjnych, które personalizują oferty w e-commerce, dane osobowe użytkowników, takie jak preferencje zakupowe, historia przeglądania czy dane demograficzne, mogą być kluczowe dla modelu, aby skutecznie prognozować, jakie produkty lub usługi mogą zainteresować daną osobę[32]. Im bardziej dokładne i zróżnicowane są dane, tym lepsze wyniki może osiągnąć model.

Dane osobowe, takie jak wiek, płeć, lokalizacja, preferencje użytkownika czy **powtarzalne wzorce** korzystania z urządzeń, pozwalają modelom AI na bardziej precyzyjne i trafne prognozy. Proces ten polega na analizie **wielomilionowego zbioru** przykładów, dzięki czemu algorytm może nauczyć się wyodrębniać kluczowe cechy, które determinują określone zachowania lub preferencje użytkowników. Modele uczące się na takich danych mogą dostarczać personalizowane wyniki, które odpowiadają indywidualnym potrzebom użytkownika. Z raportu

---

29 I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning,* Cambridge, MA 2016, s. 2–3.

30 Por. Ł. Nasiadka, *Prawo do bycia zapomnianym w perspektywie przetwarzania danych osobowych*, „Studia Prawa Publicznego" 2023, 2(42), s. 77–80, gdzie wskazuje się na trudności w określeniu zakresu zgody na przetwarzanie danych w kontekście nowych technologii.

31 K. Chałubińska-Jentkiewicz, *Prawo do prywatności w czasach nadzoru i sztucznej inteligencji*, „Themis Polska Nova" 2024, 1(15); zob. Ł. Nasiadka, *Prawo do bycia zapomnianym…*

32 R. Shokri, M. Stronati, C. Song, V. Shmatikov, *Membership Inference Attacks Against Machine Learning Models*, IEEE Symposium on Security and Privacy (SP), 2017, s. 1.

 DOI: 10.7206/kp.2080-1084.837

opracowanego przez firmę Surfshark[33] wynika, iż ilość danych oraz ich różnorodność są znaczące w kontekście możliwej utraty prywatności użytkowników chatbotów. Dla przykładu chatbot firmy Google „Gemini" pobiera do 22 różnych typów danych od użytkowników, w tym m.in. dostęp do listy kontaktów. Prowadzi to do powstania niepokojących możliwości dalszego przetwarzania danych dotyczących nie tylko osoby korzystającej z systemu, lecz również jej otoczenia. Tego rodzaju praktyki niosą ze sobą istotne wątpliwości z perspektywy realizacji prawa do bycia zapomnianym, zwłaszcza w sytuacji, w której dane te mogą zostać wykorzystane w procesach uczenia systemów sztucznej inteligencji[34].

Zgodnie z art. 17 ust. 3 RODO prawo do usunięcia danych osobowych nie ma jednak charakteru bezwzględnego i podlega licznym ograniczeniom, w szczególności w przypadkach, gdy dalsze przetwarzanie jest niezbędne do realizacji zadań wykonywanych w interesie publicznym, ochrony zdrowia publicznego, prowadzenia badań naukowych lub statystycznych albo ustalenia, dochodzenia lub obrony roszczeń[35]. W tym kontekście ograniczeniem stosowania prawa do bycia zapomnianym pozostaje również przetwarzanie danych służące realizacji interesu publicznego, które w określonych sytuacjach może uzasadniać dalsze wykorzystywanie danych osobowych pomimo zgłoszonego żądania ich usunięcia. W rozumieniu RODO interesem publicznym jest przetwarzanie danych ze względu na ochronę w dziedzinie zdrowia publicznego[36]. W tym kontekście szczególnego znaczenia nabiera wykorzystanie algorytmów sztucznej inteligencji, które dają szansę na zwiększenie efektywności działań w obszarze opieki zdrowotnej[37]. W konsekwencji prawo do bycia zapomnianym nie znajduje zastosowania w przypadku przetwarzania danych osobowych pacjentów, w tym informacji dotyczących stosowanych metod leczenia, jeżeli przetwarzanie to odbywa się przez lekarzy

---

33 Surfshark to firma technologiczna specjalizującą się w dostarczaniu narzędzi z zakresu ochrony prywatności w internecie, takich jak usługi VPN, monitorowanie wycieków danych osobowych oraz usuwanie danych z baz brokerów danych.

34 Ranked: *Which AI Chatbots Collect the Most Data About You*?, Visual Capitalist. Pozyskano z: https://www.visualcapitalist.com/ranked-which-ai-chatbots-collect-the-most-data-about-you/ (dostęp: 29.03.2025).

35 Art. 17 ust. 3 lit. a–e rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).

36 Zgodnie z motywem 54 RODO „zdrowie publiczne należy interpretować zgodnie z definicją z rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1338/2008, czyli jako wszelkie elementy związane ze zdrowiem, mianowicie stan zdrowia, w tym zachorowalność i niepełnosprawność, czynniki warunkujące stan zdrowia, potrzeby w zakresie opieki zdrowotnej, zasoby opieki zdrowotnej, oferowane usługi opieki zdrowotnej i powszechny dostęp do nich, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów". Zob. również art. 9 ust. 2 lit. h) oraz i), art. 9 ust. 3 RODO, art. 17 ust. 3 lit. c), RODO.

37 S. Wachter, B. Mittelstadt, L. Floridi, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, "International Data Privacy Law" 2017, 7(2), s. 76–99.

w celach naukowych na podstawie przepisów prawa i pozostaje związane z obowiązkiem przechowywania dokumentacji medycznej[38].

Problemy techniczne oraz prawne

Usunięcie danych osobowych z systemów sztucznej inteligencji (AI) wiąże się z licznymi trudnościami technicznymi i operacyjnymi, zwłaszcza w kontekście modeli uczących się. Zastosowanie algorytmów wykorzystujących uczenie maszynowe, w tym głębokie uczenie, prowadzi do sytuacji, w której dane osobowe użyte w procesie trenowania modeli nie muszą być bezpośrednio przechowywane w ich pierwotnej formie, lecz wpływają na strukturę samego modelu[39]. Skutkuje to tym, że choć same dane mogą zostać wycofane z bazy danych, mają nadal wpływ na parametry modelu, co stwarza trudności w pełnym usunięciu ich śladu z systemu[40].

W przypadku mniejszej zawiłości technologicznej, gdy przechowywane dane są tzw. surowymi danymi, usunięcie ich z algorytmu jest stosunkowo proste. Surowe dane wraz z ich usunięciem przestają być wykorzystywane przez system AI. Problem ze skasowaniem danych osobowych użytkownika pojawia się w sytuacji, gdy zostały one rozpowszechnione do osób trzecich bądź użyte do głębokiego uczenia, co spowodowało przyspieszenie badań na temat możliwości oduczenia algorytmu[41]. Zdarza się, że osoba wnioskująca do administratora o usunięcie danych z algorytmu robi to ze względu na informacje, które zostały już przez model ujawnione[42]. Systemy sztucznej inteligencji, po przetworzeniu danych, nie przechowują ich w postaci bezpośredniej, ale wykorzystują te dane do optymalizacji swoich parametrów. W związku z tym usunięcie wpływu tych danych na model wymagałoby ponownego trenowania systemu, co jest zarówno czasochłonne, kosztowne oraz ma wpływ na jego skuteczność[43]. W niektórych przypadkach może okazać się skrajnie trudne, aby całkowicie usunąć dane osobowe, które były wykorzystywane w procesie uczenia maszynowego, bez znacznych zmian w samym

---

38 Urząd Ochrony Danych Osobowych (UODO), *Kodeks postępowania dla sektora ochrony zdrowia*, Warszawa, 11 grudnia 2023. Pozyskano z: https://uodo.gov.pl/pl/file/4525 (dostęp: 04.06.2025).

39 R. Chourasia, N. Shah, *Forget Unlearning: Towards True Data Deletion in Machine Learning*, w: Proceedings of the 40th International Conference on Machine Learning (ICML 2023), PMLR 202, Honolulu, Hawaii, USA 2023, s. 2.

40 Zob. E. Fosch-Villaronga, P. Kieseberg, T. Li, *Humans Forget…*, s. 309.

41 Więcej na ten temat piszą: T.T. Nguyen, T.T. Huynh, Z. Ren, P. Nguyen, A. Wee-Chung Liew, H. Yin, Q. Viet Hung Nguyen, *A survey of machine unlearning,* 2022 r., arXiv preprint arXiv:2209.02299.

42 R. Chourasia, N. Shah, *Forget Unlearning*, s. 2.

43 *Ibidem*, s. 1.

 DOI: 10.7206/kp.2080-1084.837

modelu[44]. W procesie całkowitego usuwania danych osobowych z modelu wyzwaniem są również ukryte warstwy przetwarzania danych, które nie są w pełni zrozumiałe nawet dla samych twórców modeli[45].

Powyższe ograniczenia o charakterze technicznym znajdują bezpośrednie odzwierciedlenie w sferze prawnej. RODO przyznaje bowiem osobom, których dane dotyczą, uprawnienie do żądania ich usunięcia, jednak regulacja ta była tworzona przede wszystkim z myślą o tradycyjnych sposobach przetwarzania danych, a nie o systemach wykorzystujących modele sztucznej inteligencji. W rezultacie dochodzi do powstania konfliktu pomiędzy wynikającym z regulacji zakresem prawa do bycia zapomnianym a faktycznymi możliwościami jego wykonania w środowisku technologicznym opartym na rozwiązaniach AI.

AI ACT

AI ACT ustanawia zharmonizowane zasady dotyczące sztucznej inteligencji podkreśla słuszność implementacji zasad ochrony prywatności już na etapie projektowania oraz we wszystkich fazach cyklu życia systemów sztucznej inteligencji[46]. Zgodnie z art. 25 rozporządzenia zasady ochrony danych osobowych powinny być uwzględniane już na etapie projektowania i domyślnych ustawień systemów, co prowadzi do ograniczenia zbierania, przechowywania oraz przetwarzania danych osobowych już na samym początku korzystania ze sztucznej inteligencji. Minimalizacja, wskazywana jako jeden z proponowanych środków zwiększających poziom ochrony danych osobowych, oznacza, że dane osobowe powinny być stosowne, adekwatne oraz ograniczone do zakresu niezbędnego dla celu ich przetwarzania, w związku z czym wszelkie formy nadmiernego gromadzenia informacji powinny zostać wyraźnie ograniczone[47].

Wprowadzenie w życie zasad dotyczących przetwarzania danych osobowych przez systemy sztucznej inteligencji jest istotne w celu redukcji ryzyka nadużyć

---

44 Zob. V. Gupta, Ch. Jung, S. Neel, A. Roth, S. Sharifi-Malvajerdi, Ch. Waites, *Adaptive Machine Unlearning*, 35th Conference on Neural Information Processing Systems (NeurIPS), 2021, s. 1. Pozyskano z: https://arxiv.org/abs/2106.04378.

45 Zob. B. Goodman, and Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a Right to Explanation*, presented at ICML Workshop on Human Inter pretability in Machine Learning (WHI 2016). New York, NY, June 2016.

46 European Commission, European Union Artificial Intelligence Act – Guide, April 2025, s. 16.

47 Por. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa ochronie danych osobowych. Komentarz*, Warszawa 2022, s. 149–152 oraz P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 159–160.

danych oraz zapobiegnięciu nieautoryzowanego dostępu do informacji osobistych. Twórcy systemów AI powinni projektować[48] oraz stosować technologie, które uwzględniają możliwie najwyższy poziom ochrony prywatności użytkowników. Wspomniana ochrona powinna zostać zaimplementowana na każdym etapie funkcjonowania systemu[49], ze względu na szczególne znaczenie w kontekście zarówno przetwarzania danych osobowych, jak i zagrożeń związanych z ich niewłaściwym użyciem.

Minimalizacja danych wiąże się także z koniecznością wdrażania środków technicznych i organizacyjnych, które wspierają ten proces. Jest to m.in. pseudonimizacja lub anonimizacja danych[50]. Kluczowym znaczeniem dla bezpieczeństwa danych osobowych jest świadomość oraz odpowiednia procedura zapewniająca projektowane systemów AI w taki sposób, by ograniczyć do minimum zakres gromadzonych danych osobowych, a także zadbanie o ich szybkie usunięcie po zakończeniu celu przetwarzania.

Zarówno RODO, jak i AI Act posiadają regulacje dotyczące obowiązków informacyjnych, które w określonych przypadkach mogą dawać możliwość osobie fizycznej uzyskania informacji na temat mechanizmu działania systemów zautomatyzowanego podejmowania decyzji. W odniesieniu do systemów wysokiego ryzyka zdefiniowanych w AI Act ustawodawca przyznaje prawo do uzyskania wyjaśnienia, jeśli decyzje te mogą mieć istotny wpływ na podstawowe prawa jednostki. Natomiast zgodnie z art. 22 RODO osoby fizyczne mają prawo nie podlegać decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywołują wobec nich skutki prawne lub w podobny sposób istotnie na nie wpływają. Wspomniane powyżej rozporządzenie Unii Europejskiej promuje przejrzystość oraz odpowiedzialność, umożliwiając osobom fizycznym zrozumienie oraz kwestionowanie decyzji podejmowanych przez systemy AI, co może dodatkowo wspierać „prawo do bycia zapomnianym" poprzez zapewnienie jednostkom kontroli nad tym, w jaki sposób ich dane są wykorzystywane i analizowane przez automatyczne systemy.

Przejrzystość w przetwarzaniu danych staje się szczególnie ważna w kontekście decyzji, które mogą mieć daleko idące konsekwencje dla jednostki. Systemy sztucznej inteligencji są coraz częściej stosowane w kontekstach finansowym, medycznym, prawnym oraz edukacyjnym, co wymaga zapewnienia pełnej jawności procesów

---

48 Zob. European Commission, European Union Artificial Intelligence Act Guide, 2025, s. 13.

49 D. Zhang, P. Finckenberg-Broman, T. Hoang, S. Pan, Z. Xing, M. Staples, X. Xu, *Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions*, 2024, s. 14. Pozyskano z: https://arxiv.org/abs/2307.03941.

50 Zob. art. 4 pkt 5 oraz motyw 26 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), również w: A. Kaszuba, *Wyjaśnialność sztucznej inteligencji w trakcie projektowania*, Materiały pokonferencyjne autorstwa uczestników webinaru: Projektowanie systemów SI zgodnych z RODO, Urząd Ochrony Danych Osobowych, Warszawa 2023, s. 41.

 DOI: 10.7206/kp.2080-1084.837

decyzyjnych. Wdrożenie transparentnych zasad przetwarzania, takich jak możliwość uzyskania informacji na temat źródeł danych oraz logiki, na podstawie której podejmowane są decyzje, stanowi podstawę zaufania do systemów AI i minimalizuje ryzyko nieetycznych działań.

Prawo do wyjaśnienia odgrywa kluczową rolę w zapewnieniu, że systemy AI działają w sposób sprawiedliwy i transparentny. Obywatele powinni mieć możliwość otrzymania informacji, jakie czynniki przyczyniły się do podjęcia konkretnej decyzji, jakie dane były przetwarzane oraz jakie algorytmy zostały zastosowane. Taka przejrzystość pozwala jednostkom lepiej chronić swoje prawa i w razie konieczności domagać się korekty bądź usunięcia decyzji, które zostały podjęte automatycznie.

Przyszłe kierunki rozwoju

Społeczeństwo potrzebuje prawa, które będzie odpowiedzią na rosnące społeczne oczekiwania co do utrzymania prywatności w świecie rozwijających się technologii[51]. Zastosowanie nowych technologii w działaniu sztucznej inteligencji, takich jak *machine unlearning* (oduczanie), może stanowić rozwiązanie problemu związanego z ochroną danych osobowych w kontekście zaawansowanych systemów sztucznej inteligencji. Polega ono na modyfikacji modeli sztucznej inteligencji w taki sposób, aby nie uwzględniały one danych, które zostały wcześniej wykorzystane w procesie ich treningu[52]. W praktyce *machine unlearning* oznacza efektywne usunięcie wpływu określonych danych, które przestają mieć wpływ na model, gdy dalsze przetwarzane nie znajduje już uzasadnienia, w szczególności ze względu na wycofanie zgody podmiotu lub zmian w obowiązujących regulacjach prawnych. Istotne jest to, że technologie tego rodzaju wciąż pozostają na wczesnym etapie rozwoju i ich implementacja nie jest jeszcze powszechna. Skuteczna realizacja *machine unlearning* wymaga nie tylko znaczących nakładów pracy badawczej, lecz także innowacji w zakresie algorytmów umożliwiających eliminację danych z modelu bez pogorszenia jego efektywności operacyjnej.

Prawo do bycia zapomnianym, określone w artykule 17 RODO, stanowi szczególne wyzwanie dla twórców systemów sztucznej inteligencji. Modele uczenia maszynowego przetwarzają znaczne ilości danych, których całkowite usunięcie bywa szczególnie trudne ze względu na ich głębokie wkomponowanie w strukturę

[51] A. Popowicz-Pazdej, *Why the generative AI models…*, s. 223.

[52] Por. V. Gupta, Ch. Jung, S. Neel, A. Roth, S. Sharifi-Malvajerdi, Ch. Waites, *op. cit.*, s. 1.

modelu[53]. Niemniej jednak skuteczna anonimizacja danych osobowych, polegająca na uniemożliwieniu ich przypisania do konkretnej osoby fizycznej, jest uznawana za spełnienie wymogu realizacji prawa do bycia zapomnianym. Zanonimizowane dane nie są już uważane za dane osobowe, a zatem nie podlegają rygorom wynikającym z przepisów o ochronie danych, takich jak RODO, ponieważ nie istnieje możliwość ponownej identyfikacji osób. Proces anonimizacji musi jednak zostać przeprowadzony z niezwykłą starannością, aby zagwarantować, że dane rzeczywiście nie będą mogły zostać powiązane z konkretnymi osobami, nawet w wyniku zaawansowanej analizy[54].

Powyższe rozważania znajdują potwierdzenie w analizach dotyczących praktycznego wykorzystania systemów sztucznej inteligencji w zawodach zaufania publicznego. Na podstawie raportu *The Future is Now: Artificial Intelligence and the Legal Professioni*, przygotowanego przez Międzynarodowe Stowarzyszenie Prawników (International Bar Association, IBA), wskazano, że zarządzanie danymi, bezpieczeństwo i ochrona prywatności nabierają szczególnego znaczenia przy wykorzystaniu AI w kancelariach prawniczych[55]. W raporcie podkreślono również, że dla spełnienia wymagań wynikających z prawa do usunięcia danych kluczowe znaczenie ma zapewnienie, aby dane osobowe wykorzystywane w systemach sztucznej inteligencji mogły być w sposób odpowiedni zarządzane, usuwane lub modyfikowane zgodnie z prawami przysługującymi użytkownikom.

W praktyce osoby, których dane dotyczą często nie przypisują informacjom osobowym należnej wagi, czego przejawem jest między innymi akceptowanie warunków korzystania z usług bez uprzedniego zapoznania się z treścią regulaminów oraz zasad przetwarzania danych. Tymczasem informacje pozwalające na identyfikację osoby fizycznej mają ogromną wartość. Firmy inwestują miliony w ich zbieranie, przetwarzanie oraz zabezpieczenie swoich uprawnień do tych danych. Jednocześnie ochrona praw przysługująca podmiotom bywa odbierana jako zbyt czasochłonna i obciążająca. Konieczne jest wprowadzenie zmian w tym obszarze, polegających na zwiększeniu przejrzystości warunków umownych, w szczególności w odniesieniu do postanowień formułowanych drobnym drukiem, które w praktyce mogą prowadzić jedynie do pozornej kontroli nad zakresem przetwarzania danych osobowych[56].

---

53 Por. S.F. Ahmed, M.S.B .Alam, M. Hassan i in., *Deep learning modelling techniques: current progress, applications, advantages, and challenges*, "Artificial Intelligence Review" 2023, 56.

54 Por. European Commission, *European Union Artificial Intelligence Act – Guide*, April 2025, p. 24.

55 Zob. International Bar Association, *The Future is Now: Artificial Intelligence and the Legal Profession*, 2024, s. 11. Pozyskano z: https://www.fasken.com/-/media/b313030dbd324877bb741e5b6d56e9b9.pdf.

56 Zob. J. Powell, A. Kleiner, *Dylematy sztucznej inteligencji*, Gliwice 2024, s. 76.

 DOI: 10.7206/kp.2080-1084.837

Zakończenie

Przedmiotem analizy niniejszego artykułu było zagadnienie prawa do bycia zapomnianym w świetle rozwoju technologii w obszarze sztucznej inteligencji, z naciskiem na algorytmy działające w oparciu o głębokie uczenie, które ze względu na swoją architekturę i sposób przyswajania danych stwarzają szczególne wyzwanie dla skutecznego usuwania informacji osobowych. Całkowite usunięcie danych osobowych użytkowników z algorytmów, które używają uczenia głębokiego nie jest w stu procentach skuteczne. Metody oduczania algorytmów znajdują się nadal w fazie rozwoju, dlatego nie są jeszcze stosowane na skalę globalną. Artykuł 17 RODO nie jest zatem respektowany przez administratorów ze względu na ograniczone możliwości techniczne. Dynamiczny rozwój technologii oraz coraz większa złożoność jej działania przyczynia się do powstawania luk w prawie oraz wątpliwości dotyczących prywatności człowieka.

Bibliografia

Ahmed S. F., Alam M.S.B., Hassan M. i in., *Deep learning modelling techniques: current progress, applications, advantages, and challenges*, "Artificial Intelligence Review" 2023, 56. https://doi.org/10.1007/s10462-023-10466-8.

Chałubińska-Jentkiewicz K., *Prawo do prywatności w czasach nadzoru i sztucznej inteligencji*, „Themis Polska Nova" 2024, 1(15).

Chourasia R., Shah N., *Forget unlearning: Towards true data deletion in machine learning*, Proceedings of the 40th International Conference on Machine Learning, PMLR, Honolulu 2023.

Czerniawski M., *Komentarz do art. 17 RODO*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

European Data Protection Supervisor, EDPS Report on the State of Data Protection in the EU, 2021. Pozyskano z: https://www.edps.europa.eu.

Fajgielski P., *Komentarz do art. 17*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022.

Fosch-Villaronga E., Kieseberg P., Li T., *Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten*, "Computer Law & Security Review" 2018, 34(2), 2018. https://doi.org/10.1016/j.clsr.2017.08.007

Goodfellow I., Bengio Y., Courville A., *Deep Learning*, Cambridge (MA) 2016.

Goodman B., Flaxman S., *European Union Regulations on Algorithmic Decision-Making and a Right to Explanation, ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)*, New York 2016.

Gupta V., Jung C., Neel S., Roth A., Sharifi-Malvajerdi S., Waites C., *Adaptive Machine Unlearning*, Proceedings of the 35th Conference on Neural Information Processing Systems (NeurIPS), 2021. Pozyskano z: https://arxiv.org/abs/2106.04378.

International Bar Association, *The Future is Now: Artificial Intelligence and the Legal Profession*, 2024. Pozyskano z: https://www.fasken.com/-/media/b313030dbd324877bb741e5b6d56e9b9.pdf.

Jabłoński M., Węgrzyn J., *Prawo do bycia zapomnianym*, Wrocław 2021. https://doi.org/10.34616/142660.

Jabłoński M., Wygoda K., *Praktyczne znaczenie podstawowych pojęć RODO*, Wrocław 2019.

Kaszuba A., *Wyjaśnialność sztucznej inteligencji w trakcie projektowania*, [w:] *Projektowanie systemów SI zgodnych z RODO, materiały pokonferencyjne*, Urząd Ochrony Danych Osobowych, Warszawa 2023.

Kosta E., Gstrein O.J., *The Ethical and Legal Implications of AI Development and Data Processing*, "Journal of Data Protection & Privacy" 2020, 4(2). Pozyskano z: https://www.researchgate.net/publication/377569605_The_Ethical_and_Legal_Implications_of_Using_Big_Data_and_Artificial_Intelligence_for_Public_Relations_Campaigns_in_the_United_States.

Litwiński P. (red.), Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa 2018.

Lubacha J., Mäihäniemi B., Wisła R. (red.), *The European Digital Economy: Drivers of Digital Transition and Economic Recovery*, London 2023. https://doi.org/10.4324/978100345016.

Nasiadka Ł., *Prawo do bycia zapomnianym w perspektywie przetwarzania danych osobowych*, „Studia Prawa Publicznego" 2023, 2(42), s. 77–80

Nguyen T.T., Huynh T.T., Ren Z., Nguyen P., Liew A. W.-C., Yin H., Nguyen Q.V.H., *A survey of machine unlearning*, arXiv preprint arXiv:2209.02299, 2022.

Pązik A., *Prawo sztucznej inteligencji i nowych technologii. Roszczenie z art. 79 RODO jako środek ochrony przed bezprawnym przetwarzaniem danych osobowych z wykorzystaniem nowych technologii*, Warszawa 2021.

Popowicz-Pazdej A., *Why the Generative AI Models Do Not Like the Right to Be Forgotten: A Study of Proportionality of Identified Limitations*, "Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza" 2023, t. 15. https://doi.org/10.14746/ppuam.2023.15.10

Powell J., Kleiner A., *Dylematy sztucznej inteligencji*, Gliwice 2024.

Ranked: Which AI Chatbots Collect the Most Data About You?, Visual Capitalist. Pozyskano z: https://www.visualcapitalist.com (dostęp: 29.03.2025).

Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks Against Machine Learning Models*, IEEE Symposium on Security and Privacy, 2017. https://doi.org/10.1109/SP.2017.41

Wachter S., Mittelstadt B., Floridi L., *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, "International Data Privacy Law" 2017, 7(2). https://doi.org/10.1093/idpl/ipx005

Zhang D., Finckenberg-Broman P., Hoang T., Pan S., Xing Z., Staples M., Xu X., *Right to be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions*, 2024. https://doi.org/10.1007/s43681-024-00573-9

Akty normatywne i orzecznictwo

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO).

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie harmonijnych przepisów dotyczących sztucznej inteligencji (AI Act), COM(2021) 206 final, 21 kwietnia 2021 r.. Pozyskano z: https://eur-lex.europa.eu.

Wyrok Trybunału Sprawiedliwości UE z 13 maja 2014 r., C-131/12, Google Spain SL i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González. Pozyskano z: https://eur-lex.europa.eu.