Paragraf 7 / 2025
https://doi.org/10.18778/2956-3747.7.03

Mateusz Brzózka*

Ochrona danych biometrycznych jako danych szczególnie wrażliwych w świetle współczesnych wyzwań technicznych i cyfrowych

Streszczenie

Celem przedstawionego artykułu jest omówienie złożoności problematyki danych biometrycznych w dobie postępującej cyfryzacji. Unikalność danych biometrycznych czyni je wyjątkowymi, pozwalającymi na precyzyjną identyfikację każdej osoby, ale jednocześnie dane biometryczne stają się szczególnym punktem zainteresowania hakerów. Biometria to nie tylko zbiór jakichkolwiek danych, lecz kategoria szczególnie chroniona przez przepisy RODO, co wiąże się z obowiązkiem traktowania ich z najwyższą ostrożnością. W artykule wskazano, jakie zagrożenia niesie za sobą przetwarzanie na masową skalę danych biometrycznych. Omówiono również podstawowe regulacje prawne i wskazano na konkretne przypadki, w których doszło do naruszeń w kontekście przetwarzania tego rodzaju danych. Bezpieczna przyszłość danych biometrycznych zależy nie tylko od przyjęcia kolejnych regulacji prawnych, lecz także od zapewnienia społecznej odpowiedzialności za tożsamość cyfrową.

Słowa kluczowe: dane biometryczne, dane osobowe, cyfrowa tożsamość, bezpieczne przetwarzanie danych, prywatność

The Protection of Biometric Data as a Special Category of Sensitive Data in Light of Contemporary Technological and Digital Challenges

Abstract

The purpose of the presented article is to discuss the complexities surrounding biometric data in the era of advancing digitalization. The uniqueness of biometric data renders it exceptional, enabling precise identification of individuals; however, at the same time, such data increasingly becomes a focal point of interest for hackers. Biometrics do not constitute merely an ordinary set of data, but rather represent a category afforded special protection under the provisions of the GDPR, thereby necessitating their

* Student IV roku prawa, Akademia Leona Koźmińskiego, Kolegium Prawa, e-mail: 47647@kozminski.edu.pl, https://orcid.org/0009-0001-4783-5596

Received: 20.04.2025. Verified: 4.06.2025. Accepted: 10.10.2025.

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.

treatment with the utmost caution. The article outlines the risks inherent in the large-scale processing of biometric data. It also examines the fundamental legal regulations and highlights specific instances in which breaches occurred in the context of the processing of such data. The secure future of biometric data depends not only on the adoption of further legal frameworks but also on the assurance of societal responsibility for digital identity.

Keywords: biometric data, personal data, digital identity, secure data processing, privacy

1. Wstęp

W epoce coraz szybszego postępu technologicznego dane biometryczne stały się niezaprzeczalnie istotnymi instrumentami przy elektronicznej identyfikacji osób fizycznych. Pomimo niewątpliwych korzyści, jakie niesie za sobą ich zastosowanie, przetwarzanie tych danych wiąże się z istotnymi zagrożeniami dla praw i wolności jednostki, w szczególności zaś dla prawa do prywatności i autonomii informacyjnej[1]. Zarówno sektor publiczny, jak i globalne korporacje są na coraz większym celowniku zaawansowanych cyberataków, co skutkuje wyciekiem danych osobowych na niewyobrażalną skalę. Istotnym potwierdzeniem rzeczywistego i wielowymiarowego zagrożenia dla integralności danych biometrycznych jest cyberatak na amerykański Office of Personnel Management, w wyniku którego doszło do ujawnienia odcisków palców ponad czterech milionów osób, a nawet na szwank zostały narażone poufne dane ponad 21 milionów osób[2]. Do podobnego wycieku danych biometrycznych doszło także w wyniku ataku na narzędzie zabezpieczające w Biostar 2, w ramach którego ujawniono w przestrzeni cyfrowej ponad milion odcisków palców i innych poufnych danych[3]. Przytoczone przykłady unaoczniają skalę oraz intensyfikację zagrożeń związanych z nieadekwatnymi mechanizmami ochrony prawnej. Należy przy tym wskazać, iż wyciek danych biometrycznych nie zawsze jest tylko rezultatem wadliwych regulacji prawnych, lecz także braku skutecznego ich wdrażania.

W literaturze wskazuje się na problem bardzo istotny z punktu widzenia regulacji prawnych. Mianowicie, koniecznym jest przedefiniowanie podejścia do zarządzania ryzykiem w stosunku do ochrony danych osobowych[4]. W mojej ocenie, jak słusznie wskazano, ryzyko związane z naruszeniem danych biometrycznych ma charakter strukturalny, a nie jedynie incydentalny. Jednostkowy wyciek może prowadzić do daleko idących skutków, takich jak trwałe naruszenie prywatności. O ile bowiem hasło może zostać zmienione, o tyle odcisk palca czy unikalny wzorzec siatkówki oka pozostają niezmienne przez całe życie. Utrata kontroli nad takimi danymi skutkuje trwałym naruszeniem naszego prawa do ochrony danych osobowych, co w dalszej konsekwencji prowadzić może do ingerencji w konstytucyjnie chronione prawo do prywatności. Dodatkowo pojawia się problem łączenia danych z różnych źródeł, które może prowadzić do nieautoryzowanego profilowania osób, co nie jest wystarczająco uregulowane w obowiązujących aktach prawnych. Z tego względu pozostaje uzasadnione pytanie co do efektywności obowiązujących mechanizmów ochrony prawnej w dobie dynamicznie postępującej cyfryzacji oraz wzrastającej zależności wielu sfer życia społecznego od technologii biometrycznych.

1 A. Michałowicz, *Przetwarzanie danych biometrycznych a ochrona jednostek – analiza wybranych zagadnień na tle ogólnego rozporządzenia o ochronie danych i projektu aktu w sprawie sztucznej inteligencji*, czerwiec 2021, s. 83 i nast.

2 K. Finklea i in., *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, „Congressional Research Service", lipiec 2015, https://sgp.fas.org/crs/natsec/R44111.pdf (dostęp: 1.08.2025).

3 Ch. Baraniuk, *Biostar Security Software 'leaked a Million Fingerprints'*, „BBC" 2019, https://www.bbc.com/news/technology-49343774 (dostęp: 30.07.2025).

4 R. Gellert, *Understanding the Notion of Risk in the General Data Protection Regulation*, „Computer Law and Security Review" 2018.

2. Analiza statusu prawnego danych biometrycznych

Do roku 2016 pojęcie danych biometrycznych zarówno w unijnych aktach prawnych, jak i w polskim prawodawstwie nie było uregulowane. Do porządku prawnego Unii Europejskiej definicja legalna danych biometrycznych została wprowadzona dopiero w rozporządzeniu Parlamentu Europejskiego i Rady 2016/679[5]. To właśnie w art. 4 pkt 14 tego aktu wskazano, czym tak naprawdę są dane biometryczne. Zakreślony zakres znaczeniowy danych biometrycznych, wynikający z tego przepisu obejmuje przede wszystkim informacje dotyczące cech fizycznych, fizjologicznych oraz behawioralnych osób fizycznych[6]. Unijny prawodawca, tworząc treść art. 4 RODO, przyjął kluczowe elementy definicyjne wypracowane zarówno w orzecznictwie, jak i w poglądach doktryny. W głównej mierze posłużyło temu stanowisko Grupy Roboczej art. 29 ds. Danych Osobowych, która jeszcze przed wejściem w życie rozporządzenia RODO na gruncie dyrektywy 95/46/WE[7] wypracowała wytyczne. Wskazane jest, iż dane biometryczne w większości przypadków powinny być traktowane jako dane osobowe, jednakże koniecznym jest możliwość ich powiązania z konkretną osobą fizyczną. Jak wskazała ta grupa robocza „typowymi przykładami danych biometrycznych są odciski palców, wzorzec siatkówki, struktura twarzy, głos, ale także geometria dłoni, układ żył lub nawet pewne głęboko zakorzenione umiejętności lub inne cechy zachowania (takie jak własnoręczny podpis, uderzenie w klawisz, szczególny chód lub sposób mówienia)”[8]. Z uwagi na zakwalifikowanie danych biometrycznych jako szczególnej kategorii danych osobowych ich przetwarzanie objęte jest zaostrzonym reżimem ochronnym, polegającym na ustanowieniu generalnego zakazu ich przetwarzania. By można było mówić o danych biometrycznych, powinny zostać spełnione kumulatywnie wszystkie przesłanki wynikające z art. 4 pkt 14 RODO. Odpowiednio są to:

1. Dane biometryczne muszą dotyczyć cech fizycznych, fizjologicznych lub behawioralnych osób fizycznych. Oznacza to bezpośredniość związania tych cech z indywidualnymi właściwościami danej konkretnej osoby[9].
2. Dane te ze względu na swoją unikalność pozwalają na jednoznaczne zidentyfikowanie osoby fizycznej, a co za tym idzie nie powtarzają się w stosunku do innych podmiotów[10].
3. Ich proces przetwarzania technicznego ma mieć charakter czynności specjalnej. Kluczowy w tym postępowaniu jest cel, któremu ma to służyć.

Ciekawa z tego punktu widzenia jest możliwość podzielenia danych biometrycznych na dwie kategorie[11]:

— Biometria biologiczna – obejmuje techniki bazujące na mierzeniu cech fizycznych i fizjologicznych osób (*physical and physiological-based*). Wykorzystuje niezmienne cechy, które posiada każdy z nas. W szczególności obejmują one: weryfikację odcisków palców, analizę obrazu palca, rozpoznawanie tęczówki, analizę siatkówki, rozpoznawanie twarzy, zarys wzorów dłoni,

5 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.U.UE.L.2016.119.1).

6 W. Chomiczewski i in., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Wolters Kluwer Polska, 2018.

7 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.1995.281.31).

8 Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r.

9 Grupa Robocza ds. ochrony danych powołana na mocy Art. 29, *Opinia 4/2007 w sprawie pojęcia danych osobowych*, s. 13 (01248/07/PL WP 136).

10 W. Chomiczewski i in., *RODO. Ogólne rozporządzenie*...

11 Grupa Robocza ds. ochrony danych powołana na mocy art. 29, *Opinion 3/2012 on developments in biometric technologies*, przyjęta 27.04.2012 r., s. 4 i nast. (00720/12/EN WP193).

rozpoznawanie kształtu uszu, wykrywanie zapachu ciała, rozpoznawanie głosu, analizę wzorów DNA i analizę porów potowych.

— Biometria behawioralna – opiera się na mierzeniu zachowań osób i obejmuje weryfikację podpisu odręcznego, analizę uderzeń klawiszy, analizę chodu, sposób chodzenia lub poruszania się, jak również wzorce odzwierciedlające podświadome procesy myślowe. Skupia się na wzorcach zachowań osoby podczas interakcji z jakimś urządzeniem[12].

Każda z powyższych kategorii danych biometrycznych posiada swoje unikalne zalety. Biometria biologiczna posiada wysoką jakość i stanowi niesłychaną trudność przy chęci oszukania systemu[13]. Tymczasem jedną z głównych zalet biometrii behawioralnej jest możliwość ciągłego monitorowania użytkownika korzystającego z danego systemu informatycznego. Jej właściwości służą chociażby do wykrywania nieupoważnionych logowań w bankowości elektronicznej[14]. Dychotomiczny podział pomiędzy biometrię biologiczną a behawioralną implikuje konieczność szczególnej ochrony systemów informatycznych, gdzie dane te są przetwarzane.

Ich przetwarzanie w zgodzie z prawem występuje w przypadkach wskazanych w art. 9 ust. 2 RODO[15]. Przesłanki legalizujące przetwarzanie obejmują chociażby: wyraźną zgodę osoby, której dane dotyczą (lit. a), wykonywanie obowiązków w dziedzinie prawa pracy (lit. b), ochronę żywotnych interesów osoby (lit. c), a także ważny interes publiczny wynikający z prawa Unii lub prawa państwa członkowskiego (lit. g) czy cele związane z profilaktyką zdrowotną lub medycyną pracy (lit. h). Uwzględnienie katalogu czynności w definicji legalnej przetwarzania danych osobowych istotnie ogranicza wątpliwości interpretacyjne w zakresie kwalifikacji prawnej konkretnych działań, zastrzegając jednak, że uznanie ich za przetwarzanie wymaga każdorazowego spełnienia ogólnych przesłanek, zawartych w pierwszej części tej definicji[16].

Oprócz ogólnego rozporządzenia o ochronie danych osobowych dane biometryczne zostały objęte także zakresem regulacyjnym innych aktów prawa wtórnego Unii Europejskiej. Przede wszystkim należałoby wskazać na tak zwaną dyrektywę NIS 2[17], a także na potocznie nazywane rozporządzenie eIDAS[18]. Mimo braku bezpośredniego odwołania do danych biometrycznych w swoich postanowieniach istotnie wpływają na ich status prawny oraz wskazują na konieczną ochronę wrażliwych danych w obszarze cyfrowym. Wpisując tym samym dane biometryczne w aspekt obowiązków związanych z cyberbezpieczeństwem oraz uwierzytelnianiem elektronicznym, należy wziąć po uwagę ich wrażliwy charakter, wymagając tym samym wzmocnionej ochrony. Aby poznać w sposób prawidłowy charakterystykę danych biometrycznych w kontekście prawodawstwa unijnego, konieczne jest przedstawienie charakteru prawnego i faktycznego wyżej wskazanych aktów prawnych. Głównym celem rozporządzenia eIDAS jest ujednolicenie ram prawnych dla funkcjonowania jednolitego rynku cyfrowego poprzez ustanowienie wspólnych standardów dla identyfikacji elektronicznej. Regulacja ta ma na celu zwiększenie bezpieczeństwa prawnego oraz zaufania do transakcji elektronicznych w obrocie transgranicznym[19]. Nie można nie zauważyć, iż rozporządzenie to nadal odgrywa szczególną rolę

12 *Biometria behawioralna – czym jest i jakie ma znaczenie w zapobieganiu nadużyciom?*, „Algolytics", sierpień 2023, https://algolytics.com/pl/biometria-behawioralna-czym-jest-i-jakie-ma-znaczenie-w-zapobieganiu-naduzyciom/ (dostęp: 30.07.2025).

13 M. Sołtysiak, *Dane biometryczne w kontekście ochrony danych osobowych*, Lex digital, 2023.

14 J. Mlaskawa, *Biometria w bankowości – szanse i zagrożenia Banku przyszłości*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2015, nr 3, s. 110–120.

15 D. Dörre-Kolasa, *Ochrona danych osobowych w zatrudnieniu*, Warszawa 2020.

16 A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.

17 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (Dz.U.UE.L.2022.333.80).

18 Rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U.UE.L.2014.257.73).

19 M. Marucha-Jaworska, *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Wolters Kluwer Polska, 2017.

w kontekście przetwarzania danych biometrycznych, gdyż środki identyfikacji elektronicznej coraz częściej opierają się na wykorzystaniu tych właśnie danych. Natomiast jeśli chodzi o przyjęcie dyrektywy NIS 2, jej głównym zamierzeniem było wprowadzenie minimalnych standardów w zakresie zarządzania ryzykiem cybernetycznym, ustanawiając bardziej spójne i kompleksowe wymogi dla szerokiego kręgu podmiotów operujących w kluczowych sektorach. Głównym filarem tej regulacji jest ustanowienie jednolitego reżimu obowiązków sprawozdawczych oraz zasad reagowania na incydenty, co ma przeciwdziałać rozbieżnościom stosowania prawa w państwach członkowskich UE[20]. Dlatego też dane biometryczne jako coraz powszechniej wykorzystywany element systemów uwierzytelniania i kontroli dostępu nabierają charakteru aktywów wymagających szczególnej ochrony w świetle obowiązków wynikających z dyrektywy NIS 2. Instytucje Unii Europejskiej, kontynuując politykę, której głównym zamierzeniem jest stworzenie bezpiecznego i odpowiedzialnego porządku prawnego w obszarze sztucznej inteligencji, przyjęły rozporządzenie AI Act (AIA)[21]. Szczególną uwagę należy zwrócić na wprowadzony zakaz niecelowego pozyskiwania danych biometrycznych z przestrzeni publicznej oraz ograniczenia w zakresie ich analizy. Kluczowym w tym aspekcie staje się art. 5 tego aktu, który przewiduje zakaz stosowania najbardziej inwazyjnych i możliwie szkodliwych praktyk wykorzystywania sztucznej inteligencji w zakresie nieuprawnionego przetwarzania danych biometrycznych. Zakazane praktyki obejmują wszelkie zastosowania systemów AI, które poprzez stosowania technik podprogowych, manipulacyjnych prowadzą do istotnego zniekształcenia ich zachowań oraz narażenia na poważną szkodę. Ustanowiony został także zakaz niecelowego pozyskiwania danych biometrycznych z przestrzeni publicznej czy predykcyjnego profilowania w obszarze kryminalnym oraz inferencji emocji w środowisku pracy i edukacji[22]. Bez wątpienia regulacje te mają na celu ochronę prywatności jednostki oraz służą przeciwdziałaniu nieuczciwym formom ingerencji sztucznej inteligencji w tak wrażliwą przestrzeń, jaką stanowi przetwarzanie danych biometrycznych.

Postępująca cyfryzacja, głównie w obszarze identyfikacji oraz uwierzytelniania danych osób fizycznych, przyczyniła się do wzrostu znaczenia danych biometrycznych, a idzie za tym konieczność wprowadzenia szczególnych regulacji prawnych. Dane te nie stanowią jedynie dość specyficznej kategorii danych osobowych w rozumieniu prawa unijnego, lecz pozostają także przedmiotem ochrony naszego krajowego porządku prawnego. RODO przyznaje państwom członkowskim możliwość wprowadzenia modyfikacji w ramach krajowego ustawodawstwa pod warunkiem, że nie naruszają one celów oraz podstawowych założeń regulacji unijnej, a także nie prowadzą do osłabienia poziomu ochrony danych osobowych zagwarantowanego w rozporządzeniu[23]. W polskim porządku konstytucyjnym ze względu na specyficzny charakter danych biometrycznych mieszczą się one w obrębie ochrony udzielanej przez szereg przepisów Konstytucji Rzeczypospolitej Polskiej. W odniesieniu do postanowień Konstytucji RP szczególnego znaczenia nabiera konieczność wyważenia dwóch konstytucyjnych wartości: prawa dostępu do informacji publicznej oraz prawa do ochrony prywatności i prawa ochrony danych osobowych[24]. Jak wskazuje orzecznictwo Trybunału Konstytucyjnego, prawo dostępu do informacji publicznej nie ma charakteru absolutnego i jego wykonywanie musi odbywać się z poszanowaniem innych praw konstytucyjnych, w szczególności prawa do ochrony życia prywatnego[25]. Ochrona ta musi obejmować także

20 R. Bujalski, *Nowe środki w zakresie cyberbezpieczeństwa (dyrektywa NIS 2)*, System Informacji Prawnej LEX 2023.

21 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U.UE.L.2024).

22 D. Flisak, *Akt w sprawie sztucznej inteligencji*, LEX/el. 2024.

23 D. Echaust-Przybytniak, *Przetwarzanie danych biometrycznych w polskim porządku prawnym*, „Krytyka Prawa" 2019, t. 11, nr 2.

24 Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U., nr 78, poz. 483).

25 Wyrok TK z 20.03.2006 r., K 17/05, OTK-A 2006/3/3.

prawo jednostki do decydowania o udostępnianiu danych osobowych, zwłaszcza wrażliwych, takich jak dane biometryczne. Konieczność zapewnienia autonomii informacyjnej wymaga nie tylko uwzględnienia standardów prawnych wynikających z RODO, lecz także respektowania granic wymierzonych przez postanowienia Konstytucji RP.

Przy uwzględnieniu mocy prawnej, jaką temu rozporządzeniu nadaje art. 288 TFUE[26], uzasadnione jest postawienie tezy, iż polski ustawodawca powinien wprowadzić odrębne przepisy regulujące przetwarzanie danych biometrycznych (w aktach szczególnych dotyczących poszczególnych sektorów), tworząc w ten sposób podstawę prawną dla przetwarzania danych biometrycznych do konkretnych celów (np. identyfikacji) w sposób zapewniający zgodność z RODO oraz realizację konstytucyjnych standardów ochrony praw jednostki. Nasz krajowy prawodawca stara się w pewnym stopniu wychodzić naprzeciw potrzebie zapewnienia adekwatnego poziomu ochrony danych osobowych. W efekcie czego postanowił znowelizować Kodeks pracy poprzez wprowadzenie art. 22^{1b}[27], gdzie wskazano, iż wszelkie dane wrażliwe w rozumieniu art. 9 RODO mogą być przetwarzane wyłącznie z inicjatywy pracownika[28]. Wyjątek stanowi przetwarzanie danych biometrycznych pracowników wyłącznie za ich zgodą i jedynie, gdy jest to niezbędne do kontroli dostępu do pomieszczeń lub urządzeń wymagających szczególnej ochrony. Należy jednak podkreślić, że przetwarzanie takich danych musi odbywać się przy zachowaniu zasad celowości, minimalizacji oraz z zastosowaniem odpowiednich środków organizacyjnych i technicznych, zabezpieczających ich poufność[29]. Ustawodawca winien nadal konsekwentnie wprowadzać regulacje prawne w zakresie takim, jakim dopuszcza na to RODO, uwzględniając specyfikę danych biometrycznych, ich trwały, niezmienny charakter oraz wysoki potencjał ingerencji w sferę prywatności osób znajdujących się pod polską jurysdykcją.

3. Konieczność zapewnienia skutecznej ochrony danych osobowych w procesie ich przetwarzania

W dzisiejszym świecie biometria działa jak złożony mechanizm. Kluczowe znaczenie mają w tym kontekście przepisy RODO, a w szczególności art. 32 i art. 35, które formułują obowiązki w zakresie bezpieczeństwa przetwarzania oraz ochrony danych osobowych. Współczesne systemy biometryczne funkcjonują najczęściej w modelu zdecentralizowanym, w którym dostawcy technologii i podmioty przetwarzające dane osobowe pełnią odrębne, choć powiązane funkcjonalnie role.

Zgodnie z art. 32 RODO administrator oraz podmiot przetwarzający są zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewnią stopień bezpieczeństwa odpowiadający ryzyku. Zgodnie z zasadą integralności i poufności dane osobowe powinny być przetwarzane w sposób gwarantujący ich odpowiedni poziom bezpieczeństwa, obejmujący ochronę przed niedozwolonym lub niezgodnym z prawem procesem przetwarzania[30]. W odniesieniu do danych szczególnie wrażliwych, jakimi są dane biometryczne, obowiązek ten przyjmuje formę wzmocnioną. W praktyce wymaga to zastosowania m.in. szyfrowania, pseudonimizacji, segmentacji dostępu czy monitorowania nieautoryzowanych działań w czasie rzeczywistym.

Natomiast jeśli chodzi o wcześniej wspomniany przeze mnie art. 35 RODO, norma wynikająca z tego przepisu wskazuje na obowiązek przeprowadzenia oceny skutków dla ochrony danych, jeśli dany rodzaj przetwarzania (ze względu na swoją naturę, zakres, kontekst i cele) może powodować wysokie

26 Traktat o Funkcjonowaniu Unii Europejskiej (Dz.U. C 202 z 7.6.2016).

27 Ustawa z 26.06.1974 r. Kodeks pracy (Dz..U. z 1998 r., nr 21, poz. 94 ze zm.).

28 M. Gersdorf, M. Raczkowski, [w:] W. Ostaszewski i in., *Kodeks pracy. Komentarz*, wyd. IV, Warszawa 2024, art. 22(1(b)).

29 M. Kuba, [w:] *Kodeks pracy. Komentarz. Tom I. Art. 1–93, wyd. VII*, red. K.W. Baran, Warszawa 2025, art. 22(1(b)).

30 W. Chomiczewski i in., *RODO. Ogólne rozporządzenie…*

ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli taka przesłanka zachodzi, ocena skutków staje się obligatoryjna. System regulacyjny przewidziany w art. 35 RODO zakłada zatem konieczność dokonania uprzedniej wstępnej analizy każdego rodzaju przetwarzania, umożliwiającej kwalifikację stopnia ryzyka. RODO nie ustanawia formalnej procedury przeprowadzania oceny skutków, wskazuje jednak elementy obligatoryjne, jakie taka analiza powinna zawierać. Przy braku szczegółowej regulacji administratorzy mogą posiłkować się wytycznymi organów nadzorczych i ramami Privacy Impact Assessment, dostosowując je do konkretnego kontekstu przetwarzania danych[31]. Jak słusznie zostało zauważone w wytycznych dotyczących oceny skutków dla ochrony danych (DPIA), przetwarzanie danych biometrycznych niemal zawsze wymaga sprawdzenia, jakie ryzyko może spowodować akurat dane konkretne przetwarzanie[32]. Dostawcy rozwiązań biometrycznych, oferując swoje usługi, muszą to robić przy uwzględnieniu przede wszystkim zgodności tych czynności z zasadami *privacy by design* i *privacy by default*.

4. *Privacy by design* i *privacy by default* a ochrona danych wrażliwych

Samo znaczenie zasady *privacy by design* zostało zaproponowane przez Komisarz ds. Informacji i Prywatności kanadyjskiej prowincji Ontario – Ann Cavoukian. Natomiast terminem prawnie zdefiniowanym w art. 25 ust. 1 RODO jest *Data Protection by Design*. Różnica pomiędzy tą terminologią ma charakter normatywny, lecz często w praktyce stosowana zamiennie prowadzi do nieporozumień. Zasada ta sama w sobie zakładała maksymalny poziom ochrony prywatności jako integralnie wbudowany w architekturę systemów informatycznych i procesów globalnego biznesu. Prywatność użytkownika powinna być chroniona automatycznie, bez potrzeby podejmowania przez niego jakichkolwiek dodatkowych działań[33]. Ochrona danych stanowi element domyślny, a nie opcjonalny, musi reagować automatycznie i natychmiast. Już na etapie projektowania procesów przetwarzania danych na administratorze spoczywa obowiązek wdrożenia odpowiednich środków technicznych, które zapewnią pełną zgodność tych procesów z postanowieniami RODO[34]. Każdy wyciek, błędne przetworzenie czy nieuprawniony dostęp do takich danych mogą skutkować nie tylko trwałym naruszeniem prywatności jednostki, ale również zagrożeniem jej bezpieczeństwa fizycznego lub społecznego. Jedną z zasad *privacy by design*, a w mojej ocenie jedną z kluczowych jest konieczność integralnego wpisania ochrony prywatności w strukturę każdego systemu informatycznego. Ochrona danych osobowych, a w szczególności danych biometrycznych powinna stanowić jedną z podstawowych i nieodzownych funkcjonalności danego rozwiązania technologicznego. Nie może być ona traktowana jako element wtórny, implementowany *post factum* w drodze modyfikacji istniejących systemów, lecz musi być zaprojektowana jako ich konstytutywny komponent[35]. Prywatność zyskuje tym samym status nieodzownej cechy systemu, a nie jedynie dodatku o charakterze proceduralnym czy technicznym.

---

31 Tamże.

32 Grupa Robocza ds. ochrony danych powołana na mocy art. 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, przyjęta 4.04.2017 r. (17/EN WP 248 rev.01).

33 A. Cavoukian, *Privacy by Design. The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices*, *Information & Privacy Commissioner*, Ontario 2011.

34 *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). Komentarz*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021.

35 W. Wiewiórowski, *Privacy by design jako paradygmat ochrony prywatności*, Warszawa 2012, s. 17.

Przechodząc natomiast do zasady *privacy by default*, interpretacja wymogów określonych przez art. 25 ust. 2 RODO w pewnym stopniu została wyjaśniona przez Europejską Radę Ochrony Danych. Jak wskazuje rada, wdrożenie zasady ochrony danych w fazie projektowania (*privacy by design*) musi nastąpić już na etapie definiowania środków przetwarzania, czyli w momencie podejmowania decyzji co do wyboru architektury systemu. Ocena ta musi uwzględniać chociażby aktualny stan wiedzy technicznej, koszt wdrożenia, charakter i kontekst przetwarzania, jego zakres oraz cele, a także skalę i prawdopodobieństwo wystąpienia ryzyka. Wszak administratorzy powinni być również w stanie wykazać, że proces ten został przeprowadzony w odniesieniu do każdego środka przetwarzania wchodzącego w skład całego procesu[36]. W tym ujęciu przetwarzanie danych biometrycznych w celach wtórnych, np. marketingowych, bez uprzedniej zgody stanowiłoby naruszenie zasady minimalizacji danych, a w konsekwencji naruszałoby postanowienia RODO[37]. Jedną z głośniejszych spraw, która w sposób praktyczny ukazuje istnienie tego problemu, był wyciek danych biometrycznych z platformy Biostar 2. Akurat w tym przypadku dane szczególnie wrażliwe (jak np. odciski palców, dane rozpoznawania twarzy) były przechowywane bez żadnej formy szyfrowania. Konsekwencją braku zabezpieczenia mogłoby być swobodne edytowanie konta istniejącego użytkownika i dodać swój własny odcisk palca, a następnie uzyskać dostęp do dowolnego budynku, do którego użytkownik jest upoważniony[38]. Incydent ten jasno potwierdził, że systemy nieposiadające żadnych ograniczeń w zakresie dostępu czy zakresu gromadzonych informacji znajdują się w kolizji z zasadą *privacy by default*, wskazaną w art. 25 ust 2 RODO.

Wdrożenie zarówno zasady *privacy by design*, jak i *privacy by default* jest w sposób spójny powiązany z koniecznością dokonywania oceny skutków dla ochrony danych (inaczej zwaną DPIA). Ma to w szczególności zastosowanie przy wdrażaniu nowych technologii, opartych na biometrycznych metodach identyfikacji. Stanowisko Europejskiej Rady Ochrony Danych nakazuje, aby każdy system oparty na danych biometrycznych, działający w sposób zautomatyzowany i ukierunkowany na identyfikację osoby fizycznej, powinien zostać uprzednio poddany szczegółowej analizie ryzyka oraz ocenie zgodności z zasadami wynikającymi z art. 5 i art. 25 RODO[39].

5. Techniczne i prawne środki zabezpieczenia danych biometrycznych

Szyfrowanie danych biometrycznych pełni ważną rolę w systemach ochrony danych osobowych. Jest to jeden z kluczowych sposobów na zagwarantowanie bezpieczeństwa technicznego, które zostało zapewnione przez ogólne przepisy RODO. W art. 32 ust. 1 tegoż aktu jasno zostało zawarte, że administrator lub inny podmiot przetwarzający dane muszą stosować odpowiednie środki techniczne oraz organizacyjne, jak szyfrowanie, aby zapewnić bezpieczny poziom odpowiadający ryzyku.

Dane biometryczne, z powodu ich niepowtarzalności oraz unikalności, są typem informacji osobowych o bardzo dużym potencjale identyfikacyjnym[40]. O ile w przypadku danych takich jak hasła czy tokeny uwierzytelniające da się je szybko zmienić po wystąpieniu incydentu bezpieczeństwa, o tyle dane biometryczne (takie jak obraz siatkówki, odcisk palca, wzorzec głosu) są stałe i trwale powiązane z konkretną osobą. Skupiając się *sensu stricto* na technicznym punkcie widzenia, szyfrowanie danych

36 Europejska Rada Ochrony Danych, *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*, październik 2020.

37 Rozporządzenie Parlamentu Europejskiego i Rady(UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U.UE.L.2014.257.73).

38 J. Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, „The Guardian", 14 sierpnia 2019.

39 Europejska Rada Ochrony Danych, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, maj 2023.

40 K. Langer, *Biometria w miejscu pracy – kiedy i jak pracodawca może ją stosować zgodnie z prawem?*, „ODO 24" 2024, https://odo24.pl/blog-post.biometria-w-miejscu-pracy-kiedy-i-jak-pracodawca-moze-ja-stosowac-zgodnie-z-prawem (dostęp: 1.08.2025).

biometrycznych powinno opierać się na algorytmach kryptograficznych zapewniających odporność na ataki ze strony podmiotów trzecich. Zapewnienie bezpieczeństwa danym biometrycznym wiąże się coraz bardziej także z niewykorzystaniem technologii rozproszonego rejestru, potocznie znanym jako blockchain. Dane osobowe, a w szczególności dane wrażliwe w zgodzie z RODO należy przetwarzać poza łańcuchem blocków. Daje to możliwość uniknięcia wystąpienia naruszeń rozporządzenia w związku z przeniesieniem danych do rejestrów rozproszonych[41]. Administratorzy są wręcz zobowiązani do skutecznego uniemożliwienia zdobycia danych szczególnie wrażliwych przez podmioty nieposiadające takich uprawnień.

6. Przetwarzanie danych biometrycznych – studium przypadku polskiej szkoły

Bez wątpienia chęć przetwarzania danych biometrycznych przez placówki oświatowe budzi pewne wątpliwości, a nawet zakłopotanie. Tutaj pojawia się pytanie, czemu tak naprawdę miałoby to służyć. By poznać to zagadnienie, warto przyjrzeć się temu, co wydarzyło się w jednej z polskich szkół podstawowych. Mianowicie, od roku 2015 w placówce tej był wykorzystywany czytnik biometryczny, a co ciekawsze, został on umieszczony przy wejściu do stołówki szkolnej. Dzieci, by odebrać przynależny im posiłek, musiały zeskanować swoje linie papilarne. Szkoła, tłumacząc swoje postępowanie, powoływała się na chęć ułatwienia automatycznego pobierania opłat oraz przyspieszenia wydawania posiłków. Jeden z rodziców dowiedziawszy się o tym fakcie, złożył skargę do Prezesa Urzędu Ochrony Danych Osobowych.

Prezes UODO, działając na podstawie przepisów powszechnie obowiązującego prawa, wszczął postępowanie administracyjne[42], a następnie nałożył karę finansową na tę placówkę[43] w związku z naruszeniem szeregu postanowień RODO. W tym konkretnym przypadku głównie chodziło o naruszenie zasady legalności (art. 5 ust. 1 lit. a RODO) oraz warunków przetwarzania szczególnych kategorii danych osobowych (art. 9 ust. 1). Organ nadzorczy wskazywał na brak możliwości wyrażenia zgody na przetwarzanie danych biometrycznych w sposób dobrowolny oraz przetwarzanie tych danych, zdaniem Prezesa UODO, nie było warunkiem koniecznym do otrzymania obiadu przez dziecko[44], co powodowałoby *ex lege* nieskuteczność tej czynności.

Decyzja ta natomiast nie spotkała się z akceptacją ze strony Wojewódzkiego Sądu Administracyjnego w Warszawie, który tym samym uchylił decyzję Prezesa UODO. W wyroku tym sąd wskazuje na zbyt rygorystyczne działanie ze strony organu nadzorczego oraz pominięcie celowości pozyskiwania danych biometrycznych przez szkołę[45]. Stanowisko sądu I instancji zostało potwierdzone w postępowaniu kasacyjnym przed Naczelnym Sądem Administracyjnym. Sąd rozpoznający skargę kasacyjną podniósł fakt, że pomimo istnienia alternatywnych sposobów przetwarzania danych zgoda wyrażona w sposób zgodny z RODO nie może być w sposób swobodny i arbitralny podważana przez organ sprawujący nadzór[46]. Przy czym zarówno z wyroku Wojewódzkiego, jak i Naczelnego Sądu Administracyjnego płynie sentencja systemowa, która wskazuje, jakie przymioty powinna posiadać zgoda, by można było w sposób prawidłowy przetwarzać dane biometryczne. Są to odpowiednio: dobrowolność, jednoznaczność, konkretność, świadomość. Choć Sąd słusznie zaakcentował konieczność spełnienia określonych warunków

41 Grupa robocza ds. rejestrów rozproszonych i blockchain, *RODO a technologia blockchain*, Ministerstwo Cyfryzacji, 7.11.2019 r.

42 Ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 1960 r., nr 30, poz. 168).

43 Ustawa z 10.05.2018 r. O ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781).

44 Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 18.02.2020 r. (ZSZS, 440.768.2018), https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018

45 Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 7.08.2020 r., II SA/Wa 809/20, LEX nr 3127372.

46 Wyrok Naczelnego Sądu Administracyjnego z 10.10.2024 r., III OSK 4804/21, LEX nr 3774636.

zgody, lecz pominął fakt, że przetwarzanie danych biometrycznych wymaga szczególnej ostrożności. Co więcej, motywy RODO akcentują potrzebę zwiększonej troski przy przetwarzaniu danych dzieci jako podmiotów szczególnie narażonych oraz precyzyjnego wskazania przez administratora danych celu i właściwej podstawy prawnej[47]. Ponadto nie rozważono realnych alternatyw dla biometrycznej identyfikacji ani nie oceniono ryzyka nierównowagi stron w relacji szkoła – rodzic. Tak przyjęta wykładnia w sposób znaczny ogranicza prewencyjną funkcję RODO, która chronić ma podmioty danych przed nadmierną ingerencją. Stanowisko NSA pomija szerszy kontekst aksjologiczny RODO, nie podąża w kierunku zapewnienia pełnej formy bezpieczeństwa przetwarzania danych biometrycznych.

7. Podsumowanie

W obliczu postępu technologicznego wzrasta realne zagrożenie bezpieczeństwa i prywatności jednostki w kontekście wykorzystywania danych biometrycznych. Jak pokazują przytoczone przeze mnie przykłady ataków hakerskich na Biostar 2 czy Office of Personnel Management, współczesne systemy informatyczne nie są przygotowane na tak daleko idącą ingerencję z zewnątrz. Na kanwie tych przykładów możemy zaobserwować poważniejsze skutki, będące efektem wycieku danych biometrycznych niż te w przypadku wycieku zwykłych danych osobowych. Podyktowane jest to charakterem biometrii, która cechuje się niezmiennością, unikalnością, niepowtarzalnością. Istniejący problem wskazuje na konieczność podjęcia systemowych rozwiązań, zmieniających chociażby podejście do pojęcia zarządzania ryzykiem. Nieodzowne staje się również wzmocnienie obowiązujących regulacji prawnych, a w szczególności postanowień RODO, rozporządzenia eIDAS oraz dyrektywy NIS 2. Ochrona danych biometrycznych stanowi prawdziwe wyzwanie. Wymaga wprowadzenia skomplikowanych i wielowarstwowych technik, jak szyfrowanie czy pseudonimizacja. Kluczowe jest także stosowanie zasad *privacy by design* i *privacy by default*, które wymuszają myślenie o prywatności już na etapie projektowania systemów informatycznych. Znaczenie tych regulacji unaocznia historia jednej z polskich szkół podstawowych, która wprowadziła biometryczny system wymagający od uczniów skanowania linii papilarnych przy odbieraniu posiłku. Interwencja Prezesa Urzędu Ochrony Danych Osobowych wywołała szeroką dysputę prawną. Wszczęto postępowanie administracyjne, nałożono karę finansową. Natomiast sądy uznały, że wszystko odbywało się zgodnie z RODO. Zgoda, jeśli jest dobrowolna i świadoma, nie może być z góry kwestionowana przez organ nadzorczy bez przedstawienia wiarygodnych faktów i dowodów. Zobowiązanie to jest skierowane do wszystkich instytucji publicznych, które zdecydują się na przetwarzanie tej kategorii danych osobowych. Dane biometryczne jako niezmienne i posiadające wysoki potencjał identyfikacyjny wymagają zaawansowanej ochrony technicznej i solidnych gwarancji prawnych. W erze cyfryzacji i rosnącej popularności technologii biometrycznych potrzebujemy spójnych regulacji prawnych. Muszą one być zgodne z unijnym porządkiem prawnym, ale także realnie chronić jednostkę przed nadużyciami i utratą kontroli nad danymi, które stanowią część jej tożsamości. Pamiętajmy, że my sami również musimy dbać o naszą prywatność i cyfrowe bezpieczeństwo.

47 Motywy 38 i 40 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.U.UE.L.2016.119.1).

Bibliografia

Baraniuk Ch., *Biostar Security Software 'leaked a Million Fingerprints'*, „BBC" 2019, https://www.bbc.com/news/technology-49343774 (dostęp: 30.07.2025).

Biometria behawioralna – czym jest i jakie ma znaczenie w zapobieganiu nadużyciom?, „Algolytics" 2023, https://algolytics.pl/biometria-behawioralna-czym-jest-i-jakie-ma-znaczenie-w-zapobieganiu-naduzyciom/ (dostęp: 30.07.2025).

Bujalski R., *Nowe środki w zakresie cyberbezpieczeństwa (dyrektywa NIS 2)*, „System Informacji Prawnej, LEX 2023.

Cavoukian A., *Privacy by Design. The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices, Information & Privacy Commissioner*, Ontario 2011.

Chomiczewski W., Czerniawski M., Drobek P., Góral U., Kuba M., Łuczak J., Makowski P., Witkowska-Nowakowska K., Zawadzka N., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Wolters Kluwer Polska, 2018.

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 18.02.2020 r. (ZSZS,440.768.2018). https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018

Dörre-Kolasa D., *Ochrona danych osobowych w zatrudnieniu*, Warszawa 2020.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.1995.281.31).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (Dz.U.UE.L.2022.333.80).

Echaust-Przybytniak D., *Przetwarzanie danych biometrycznych w polskim porządku prawnym*, „Krytyka Prawa" 2019, t. 11, nr 2. https://doi.org/10.7206/kp.2080-1084.306

Europejska Rada Ochrony Danych, *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*, październik 2020.

Europejska Rada Ochrony Danych, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, maj 2023.

Finklea K., Christensen M.D., Fischer E.A., Lawrence S.V., Theohary C.A., *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, „Congressional Research Service", lipiec 2015, https://sgp.fas.org/crs/natsec/R44111.pdf (dostęp: 1.08.2025).

Flisak D., *Akt w sprawie sztucznej inteligencji*, LEX/el. 2024.

Gellert R., *Understanding the Notion of Risk in the General Data Protection Regulation*, „Computer Law and Security Review" 2018. https://doi.org/10.1016/j.clsr.2017.12.003

Gersdorf M., Raczkowski M., [w:] W. Ostaszewski, K. Rączka, A. Zwolińska, M. Gersdorf, M. Raczkowski, *Kodeks pracy. Komentarz, wyd. IV*, Warszawa 2024, art. 22(1(b)).

Grupa Robocza ds. ochrony danych powołana na mocy art. 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, przyjęta 4.04.2017 r. (17/EN WP 248 rev.01).

Grupa Robocza ds. ochrony danych powołana na mocy art. 29, *Opinia 4/2007 w sprawie pojęcia danych osobowych* (01248/07/PL WP 136).

Grupa Robocza ds. ochrony danych powołana na mocy art. 29, *Opinion 3/2012 on developments in biometric technologies*, przyjęta 27.04.2012 r. (00720/12/EN WP193).

Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r.

Grupa robocza ds. rejestrów rozproszonych i blockchain, *RODO a technologia blockchain*, Ministerstwo Cyfryzacji, 7.11.2019 r.

Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U., nr 78, poz. 483).

Krasuski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.
Kuba M., [w:] *Kodeks pracy. Komentarz. Tom I. Art. 1–93, wyd. VII*, red. K.W. Baran, Warszawa 2025, art. 22(1(b)).
Langer K., *Biometria w miejscu pracy – kiedy i jak pracodawca może ją stosować zgodnie z prawem?*, „ODO 24" 2024, https://odo24.pl/blog-post.biometria-w-miejscu-pracy-kiedy-i-jak-pracodawca-moze-ja-stosowac-zgodnie-z-prawem (dostęp: 1.08.2025).
Marucha-Jaworska M., *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Wolters Kluwer Polska, 2017.
Michałowicz A., *Przetwarzanie danych biometrycznych a ochrona jednostek – analiza wybranych zagadnień na tle ogólnego rozporządzenia o ochronie danych i projektu aktu w sprawie sztucznej inteligencji*, czerwiec 2021.
Mlaskawa J., *Biometria w bankowości – szanse i zagrożenia Banku przyszłości*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2015, nr 3, s. 110–120.
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). Komentarz, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.U.UE.L.2024).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U.UE.L.2014.257.73).
Sołtysiak M., *Dane biometryczne w kontekście ochrony danych osobowych*, Lex digital, 2023.
Taylor J., *Major Breach Found in Biometrics System Used by Banks, UK police and defence firms*, „The Guardian", 14 sierpnia 2019.
Traktat o Funkcjonowaniu Unii Europejskiej (Dz.U.UE C 202 z 7.6.2016).
Ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 1960 r., nr 30, poz. 168).
Ustawa z 26.06.1974 r. Kodeks pracy (Dz.U. z 1998 r., nr 21, poz. 94 ze zm.).
Ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781).
Wiewiórowski W., *Privacy by design jako paradygmat ochrony prywatności*, Warszawa 2012.
Wyrok Naczelnego Sądu Administracyjnego z 10.10.2024 r., III OSK 4804/21, LEX nr 3774636.
Wyrok Trybunału Konstytucyjnego z 20.03.2006 r., K 17/05, OTK-A 2006/3/3.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 7.08.2020 r., II SA/Wa 809/20, LEX nr 3127372.