

*Marek Porzeżyński*¹

Politechnika Warszawska, Polska

e-mail: marek.porzezynski@pw.edu.pl

ORCID: 0000-0002-4709-2788

PRAWNE I ETYCZNE OGRANICZENIA WYKORZYSTANIA DANYCH BIOMETRYCZNYCH W UNII EUROPEJSKIEJ I W POLSCE

LEGAL AND ETHICAL RESTRICTIONS ON THE USE OF BIOMETRIC DATA IN THE EUROPEAN UNION AND POLAND

Abstract

Technological development has never been so rapid as today. Due to the emerging technologies, their users gain considerable advantages in their everyday life. At the same time, such facilitation has an effect on our privacy and entails a risk of a wide range of information becoming easily available to unauthorised entities or persons. However, the risk is even greater when the scope of data required to get access to a particular solution becomes broader. In some cases, the amount of data requested from the user seems largely redundant. In this context, it is worth mentioning, for example, biometric data increasingly used for authentication of the user wishing to access applications by means of fingerprint scanning or facial recognition. The question is whether this is really necessary in all situations, or possibly in some circumstances the use of biometrics may

¹ Kwerenda biblioteczna przeprowadzona na potrzeby przygotowania niniejszego artykułu została sfinansowana ze środków Narodowego Centrum Nauki w programie MINIATURA.

pose a greater threat to privacy than to the information protected this way. The author presents the current restrictions on the use of biometric data, along with their assessment.

KEYWORDS

data, personal data, biometric data, information, new technologies

SŁOWA KLUCZOWE

dane, dane osobowe, dane biometryczne, informacje, nowe technologie

1. WSTĘP

Jak mantrę powtarza się stwierdzenie, że rozwój technologiczny nigdy nie był jeszcze tak szybki jak obecnie. Nie sposób się z tym jednak nie zgodzić. Technologia rozwiązuje bowiem wiele problemów, o których istnieniu jeszcze niedawno nie wiedzieliśmy. Wiele z nowinek technologicznych została opracowana chociażby w celu ułatwienia życia, jak np. aplikacje służące do zamawiania przewozu lub zakupów w jednym miejscu czy zdalny dostęp do naszego konta w banku. Coraz większy zakres takich usług przekłada się na ilość² danych możliwych do zebrania przez podmioty je dostarczające. W związku z tym również gromadzenie danych na szeroką skalę nigdy nie było tak proste jak obecnie. Zasadniczo każda usługa udostępniana za pomocą internetu czy w ramach urządzeń połączonych z internetem rzeczy³ uzyskuje dostęp i możliwość wykorzystania danych przekazanych przez użytkowników lub wygenerowanych (wytworzonych) w ramach korzystania. Użytkownicy częstokroć wyrażają również dodatkowe zgody dotyczące przetwarzania danych osobowych w celu skorzystania z usług towarzyszących. Taką usługą może być bowiem inny sposób potwierdzenia tożsamości danej osoby, np. w celu uzyskania dostępu do telefonu, co daje szeroką możliwość dla zebrania dodatkowych informacji niezbędnych do wykonania operacji potwierdzenia.

² Jak również jakość.

³ Ang. Internet of Things (IoT).

Biometria jako metoda weryfikacji⁴ nie jest przy tym nową technologią. Definiuje się ją jako technikę pomiarów istot żywych⁵, co umożliwia późniejszą weryfikację tożsamości konkretnej osoby fizycznej. Pierwszych udokumentowanych zastosowań biometrii należy się bowiem doszukiwać już w Babilonii, gdzie odcisk palca na tabliczce stanowił potwierdzenie zawarcia kontraktu⁶, choć nawet wcześniej dokonywano identyfikacji konkretnych osób za pomocą np. naocznego rozpoznania rysów ich twarzy. Dopiero, jak się wydaje, pod koniec XIX w. doszło do przełomu w postaci usystematyzowania metodologii porównania odpowiednich cech, co zdecydowanie bardziej przybliżyło ludzkość do dzisiejszych metod biometrycznych⁷. Ostatnie dekady przyniosły natomiast możliwość szerszego i zdecydowanie dokładniejszego zastosowania zasad biometrii, w szczególności za pośrednictwem zautomatyzowanego przetwarzania danych wykorzystywanych w tym celu, co miało miejsce w następstwie wydarzeń z 11 września 2001 r. w celu zapewnienia wyższego poziomu bezpieczeństwa. USA miały odegrać znaczącą rolę w lobbingu za zastosowaniem tej metody identyfikacji⁸ na nieznaną wcześniej skalę.

Powyższe przyczyniło się do rozwoju technologii pozwalającej na identyfikację osób fizycznych w czasie rzeczywistym, jak również umożliwiło jej wykorzystanie. Technologia ta wykorzystywana początkowo jedynie dla zapewnienia szczególnego poziomu bezpieczeństwa przeobraża się powoli w technologię użytkową, z którą mamy do czynienia każdego dnia, jak w przypadku wspomnianej metody potwierdzania tożsamości za pomocą rysów w telefonach komórkowych. Jednocześnie w ten sposób wiele podmiotów może uzyskiwać dostęp do nowego, szerokiego zakresu danych, które umożliwiają większą monetyzację usług lub dostęp do nowych rynków zbytu⁹. Oswajanie społeczeństwa z biometrią nie powoduje jednak, że dane biometryczne są lepiej zabezpieczane. Z tego powodu niezbędna

⁴ Zaznaczenia wymaga różnica pomiędzy pojęciem identyfikacji i weryfikacji, w których to procesach wykorzystywana jest biometria. Pierwszy z nich zakłada ustalenie tożsamości osoby fizycznej, a drugi jej potwierdzenie. W ramach przeprowadzonych badań różnica ta nie miała jednak znaczenia, gdyż w obu przypadkach rodzaj danych i ograniczenia ich wykorzystania są tożsame. Więcej informacji: A. Zajkowska, W. Zimnoch, *Technologie biometryczne – istota i możliwości wykorzystania w MSP*, (w:) S. Lachiewicz, M. Matejun (red.), *Problemy współczesnej praktyki zarządzania*, t. 2, Łódź 2007, s. 205.

⁵ Za *Słownikiem języka polskiego PWN*, <https://sjp.pwn.pl/sjp/biometria;2444846.html> (dostęp: 3.03.2022 r.).

⁶ K. Krassowski, I. Sołtyszewski, *Biometria – zarys problematyki*, „Problemy Kryminalistyki” 2006, nr 252, s. 39.

⁷ Metoda Bertillona opracowana przez Alhonsa de Bertillon ok. 1890 r., zgodnie z którą należało dokonać pomiaru różnych części ciała i je odpowiednio skatalogować.

⁸ *Ibidem*; tak również: Ł. Stasiak, A. Czajka, P. Strzelczyk, M. Chochowski, A. Pacut, *Od biometrii do bezpiecznej biometrii*, SECURE 2006, Bezpieczeństwo – czas na przełom, Warszawa, 17–18 października 2006 r.

⁹ Więcej na ten temat: M. Porzeżyński, *Własność danych w dobie internetu rzeczy*, „Państwo i Prawo” 2021, z. 2; lub M. Porzeżyński, *Wycena danych – złota XXI wieku*, (w:) M. Jankowska,

jest weryfikacja możliwości zbierania i korzystania z danych biometrycznych w świetle przepisów prawa, jak również w zgodzie z normami etycznymi.

2. DANE BIOMETRYCZNE¹⁰

Pojęciem centralnym dla badań i prowadzonej w ich ramach analizy są dane biometryczne. Bez rozpoznania znaczenia biometrii niemożliwe było w szczególności przejście do kolejnego etapu badań, w którym danym biometrycznym nadaje się odpowiednią kwalifikację prawną, co ma zasadnicze znaczenie dla wskazania prawnych ograniczeń w ich wykorzystaniu.

Dane biometryczne stanowią kategorię rozpoznaną i zdefiniowaną w aktach prawnych¹¹ oraz dokumentach związanych ze stosowaniem prawa. Przykładowo, w normie ISO/IEC 2382:2015¹² pojęcie to zostało zdefiniowane jako użycie specyficznych atrybutów odzwierciedlających unikalne cechy osoby, takie jak: odcisk linii papilarnych palca, struktura układu żył krwionośnych (palca, nadgarstka), cechy charakterystyczne głosu, w celu potwierdzenia tożsamości osoby. Podobnie do wskazanej powyżej definicji wiele z przyjętych interpretacji koncentruje się na aspekcie wykorzystania mierników związanych z konkretną osobą fizyczną w celu identyfikacji lub weryfikacji jej tożsamości. Każda z przywołanych cech może być zastosowana w celu identyfikacji lub weryfikacji, jak również każda z nich będzie odznaczała się innym poziomem użyteczności i bezpieczeństwa¹³. Dokonanie wyboru wykorzystania konkretnej cechy na potrzeby danej analizy biometrycznej jest zależne od wielu czynników, do których należy w szczególności wygoda pobrania próbki, szybkość weryfikacji, rozmiar pamięci do przechowywania wzorca czy wymagany poziom bezpieczeństwa¹⁴. Niezmienne jednak wszystkie należą do danych biometrycznych i choć mogą mieć wpływ

M. Pawełczyk, S. Augustyn, M. Panfil (red.), *Znaczenie wyceny własności intelektualnej. Proving the worth. Putting a value on intellectual property*, Warszawa 2019.

¹⁰ Autor niezależnie przeprowadził badania, których celem było odczytanie zakresu definicyjnego pojęcia danych biometrycznych. Prezentacja wyników tych badań jest obecnie w trakcie postępowania publikacyjnego.

¹¹ Np. RODO, o czym będzie mowa w kolejnym rozdziale.

¹² Norma ISO/IEC 2382:2015 – Information Technology – vocabulary, będąca obecnie w procesie planowej rewizji.

¹³ I. J. Józwiak, M. Szczepanik, *Wydajność i niezawodność wielomodułowych systemów biometrycznych*, „Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie” 2013, z. 64, s. 100.

¹⁴ R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, *Biometria*, Warszawa 2016.

na etykę ich wykorzystania, to nie mają zasadniczego znaczenia dla ich kwalifikacji prawnej¹⁵.

Należy również zauważyć, że obecnie dysponujemy również definicją legalną danych biometrycznych, co ma zasadnicze znaczenie dla atrybutu pewności prawa związanej z określoną kwalifikacją konkretnych informacji. Definicja legalna danych biometrycznych została uwzględniona w treści rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r.¹⁶. Zgodnie z art. 4 pkt 14 RODO dane biometryczne to „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby (...)”. W dalszej części przywołanej powyżej definicji wymieniono przykładowe dane wchodzące w zakres danych biometrycznych – „wizerunek twarzy lub dane daktyloskopijne”. Warto zwrócić uwagę, że definicja ta jest odmienna od wykorzystywanych w ramach innych dziedzin nauki. Zgodnie z nią nie wszystkie informacje lub dane, które są możliwe do wykorzystania w ramach metod biometrii, będą automatycznie zakwalifikowane jako dane biometryczne w rozumieniu RODO, lecz jedynie te, które spełniają wskazane w jej ramach wymagania, tj.: 1) wynikają ze specjalnego przetwarzania technicznego; 2) dotyczą cech osoby fizycznej, takich jak: a) fizyczne lub b) fizjologiczne, lub c) behawioralne; 3) a zarazem w odniesieniu do identyfikacji osoby fizycznej, jednoznacznie ją: a) umożliwiają lub b) potwierdzają. Wyjaśnienia takiego ukształtowania omawianej definicji można się dopatrywać w motywie 51 RODO, zgodnie z którym „przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją »danych biometrycznych« tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości”. Choć powyższe może zostać uznane za zgodne ze zdrowym rozsądkiem, to bez wątpienia pozostawia ona poza obrębem tejże definicji przypadki, które mogą nosić informacje uznawane za dane biometryczne w powszechnym rozumieniu tego terminu, a jednocześnie niemieszczące się w zakresie wskazanej definicji.

¹⁵ Takie znaczenie może wystąpić w sytuacjach skrajnych, w których np. użyteczność jest na tak niskim poziomie, że nie pozwala zakwalifikować konkretnych informacji jako danych biometrycznych lub – szerzej – danych osobowych.

¹⁶ 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 nr 119 z 2016 r., s. 1); dalej: RODO.

3. DANE BIOMETRYCZNE JAKO SZCZEGÓLNA KATEGORIA DANYCH OSOBOWYCH

Oprócz rozważenia kwalifikacji danych biometrycznych jako części szerszej kategorii danych osobowych należy zauważyć również, że w ramach przywołanego rozporządzenia RODO wyróżnia się zasadniczo ich dwa rodzaje. Są to dane osobowe określane bezprzymiotnikowo i dane osobowe szczególnej kategorii, które nazywane są również danymi wrażliwymi lub sensytywnymi. Kwalifikacja jako danych osobowych szczególnej kategorii jest doniosła prawnie, ponieważ niesie ze sobą obowiązek spełnienia dodatkowych wymagań. Dane biometryczne są zaś wprost wskazane jako dane osobowe szczególnej kategorii w ramach art. 9 RODO, zgodnie z którym „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”. Dane biometryczne zostały zatem ujęte w jednej kategorii z danymi dotyczącymi zdrowia czy danymi genetycznymi, co może pokazywać podejście do danych tego rodzaju. Jednocześnie wydaje się ono być podyktowane faktem wcześniejszego zawężenia samych danych biometrycznych w ramach definicji wskazanej w art. 4 pkt 14 RODO. Należy również zaznaczyć, że dane biometryczne mogą częstokroć być nośnikiem informacji dotyczących zdrowia, co uzasadnia traktowanie tych kategorii w ten sam sposób.

Prawodawca unijny zwraca uwagę, że przyporządkowanie danych tego rodzaju do szczególnej ich kategorii jest podyktowane faktem, że kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności osoby fizycznej¹⁷. Zauważyć jednocześnie należy, że są to te same elementy, które podlegają analizie z etycznego punktu widzenia. W odniesieniu do danych przetwarzanych w celach zdrowotnych wprost przewiduje się kontekst, w jakim mogą one być wykorzystywane bez uszczerbku dla wskazanych zasad nadrzędnych¹⁸. W odniesieniu do danych biometrycznych brak jest takich wytycznych.

Kraje członkowskie mają jednak możliwość zaproponowania wyższego poziomu zabezpieczenia poprzez wprowadzenie dalej idących ograniczeń do prawa krajowego. Nie mogą one jednakże wpływać na ograniczenie lub nawet utrudnienie transgranicznego przetwarzania danych, co może zakłócać ich przepływ pomiędzy krajami należącymi do Unii Europejskiej. Powyższe może mieć znaczenie chociażby w odniesieniu do danych biometrycznych w związku z rozpowszechnieniem się dokumentów zawierających elementy biometryczne, w tym

¹⁷ Motyw 51 RODO.

¹⁸ Np. w ramach motywu 53 RODO.

tw. paszportów biometrycznych¹⁹. W tym zakresie istnieją jednak przepisy szczególnie w postaci rozporządzenia w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie²⁰.

4. OGRANICZENIA W KORZYSTANIU Z DANYCH BIOMETRYCZNYCH

Dane biometryczne należą do informacji, których posiadanie²¹ przez różnego rodzaju podmioty funkcjonujące na rynku może łączyć się ze szczególną uciążliwością dla osób, których dotyczą. Bardzo często są to bowiem informacje (i dane), które dotyczą sfery intymnej lub które są otaczane przez znaczną część osób szczególną pieczę. Z całą pewnością wiele osób chroni je w zdecydowanie większym zakresie niż np. swoje imię i nazwisko czy adres. W kontekście prawnym bez wątpienia należą do danych osobowych szczególnej kategorii, z którą to kwalifikacją łączy się generalny zakaz przetwarzania. Stąd należy przyjąć wniosek, że w odniesieniu do możliwości ich wykorzystania należy w pierwszej kolejności poddać analizie normy prawne, które przewidują wyjątki od wskazanego zakazu.

W następnej kolejności przeprowadzono badania w zakresie zasad etycznych, które mogą mieć dodatkowe (pozanormatywne) znaczenie dla możliwości szerszego wykorzystania rozwiązań opartych na danych. Normy i wytyczne natury etycznej mogą bowiem oprócz bycia drogowskazem moralnym, stanowić również podbudowę argumentacji faktycznej dla uzasadnienia (lub braku zasadności) zastosowania jednego z wyjątków umożliwiających przetwarzanie tych danych od strony prawnej. Niezależnie od powyższego, ostatnie wydarzenia związane z wojną w Ukrainie i bojkotami marek, które nie wycofały się w jej rezultacie z rynku rosyjskiego, pokazują, że wymiar moralny może bezpośrednio przekładać się na otaczającą rzeczywistość, w tym aktywność biznesową czy nowe regulacje prawne.

¹⁹ Zob. np. rozwiązania jednego z dostawców paszportów biometrycznych: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/passport> (dostęp: 9.03.2022 r.).

²⁰ Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie (Dz.Urz. UE L nr 385 z 2004 r., s. 1).

²¹ A zatem również przetwarzanie w rozumieniu RODO.

4.1. OGRANICZENIA PRAWNE DOTYCZĄCE PRZETWARZANIA DANYCH BIOMETRYCZNYCH

Na wstępie należy zauważyć, że już sama konstrukcja art. 9 ust. 1 RODO wskazuje na wyższy poziom ochrony określonych w nim danych poprzez zastosowanie generalnego zakazu ich przetwarzania, w przeciwieństwie do zezwolenia na przetwarzanie²² pozostałych danych osobowych. Zakaz ten nie jest jednak bezwzględny i ustawodawca dopuszcza możliwość ich przetwarzania na podstawie wprost przewidzianych wyjątków, których lista jest zamknięta. Zaznaczenia wymaga jednak, że nawet w przypadku spełnienia jednego z wymogów zezwalającego na przetwarzanie danych szczególnej kategorii zdarza się, że organy władzy publicznej mogą kwestionować zasadność przyjętego rozwiązania²³ w świetle ogólnych zasad dotyczących ochrony danych osobowych, np. zasady minimalizmu²⁴. Wyjątki te nie powinny być zatem postrzegane jako klucze otwierające bramy do nieskrępowanej możliwości przetwarzania danych szczególnej kategorii, ale raczej jako mapę, która wskazuje, w jaki sposób osiągnąć zakładany cel, jednakże nie gwarantuje jego osiągnięcia we wszystkich przypadkach.

Wyjątki od zakazu wskazanego we wstępie niniejszego rozdziału zostały wymienione enumeratywnie przez prawodawcę unijnego w art. 9 ust. 2 RODO. W rzeczonym artykule przewidziano łącznie dziesięć sytuacji, w których zakaz przetwarzania danych biometrycznych zasadniczo nie ma zastosowania. Choć może się wydawać, że to stosunkowo szeroka lista wyjątków, to zaznaczenia wymaga, że istotnie różnią się one od siebie i wiele z nich jest zarezerwowanych dla konkretnych podmiotów lub do rodzaju wykorzystania w precyzyjnie określonym i uzasadnionym celu. W tym kontekście stanowią one zatem podstawę dla możliwości działania w ściśle uzasadnionych przypadkach, które zostały przewidziane przez prawodawcę. Stąd tylko niektóre z wyjątków znajdują zastosowanie do możliwości przetwarzania danych biometrycznych.

Zaznaczenia również wymaga, że w odniesieniu do połowy z wyjątków określonych w analizowanym akcie prawnym, niezbędne jest zapewnienie przez prawo Unii Europejskiej lub prawo państwa członkowskiego dodatkowych zabezpieczeń²⁵, co również wpływa zasadniczo na możliwość ich zastosowania dla otwartego rynku. W doktrynie wskazuje się również, że każda z tych przesłanek ma charakter autonomiczny i niezależny²⁶. Jednocześnie należy zaznaczyć,

²² Przy spełnieniu odpowiednich wymagań.

²³ Zob. np. decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 18 lutego 2020 r., nr ZSZS.440.768.2018.

²⁴ Zgodnie z art. 5 ust. 1 lit. c RODO dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

²⁵ E. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Dordrecht, Leuven 2013, s. 745.

²⁶ Tak również: P. Litwiński (red.), *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwa-*

że niektóre z organów nadzoru podkreślają, iż przetwarzanie danych tego rodzaju wymaga oprócz wykazania spełniania jednej z omawianych poniżej przesłanek, również przedstawienia podstawy przetwarzania z art. 6 RODO²⁷. Z uwagi na zakres niniejszego artykułu i ograniczenia objętościowe niemożliwe jest szczegółowe przeanalizowanie wszystkich wyjątków przewidzianych w art. 9 RODO²⁸, dlatego uzasadnione jest odwołanie się jedynie do tych, które mają lub mogą mieć najszerze znaczenie dla możliwości wykorzystania danych biometrycznych.

Zgoda osoby, której dane dotyczą, jest podstawową przesłanką przetwarzania danych osobowych²⁹. Zarazem jest ona wyjątkiem najszerzej umożliwiającym prywatne wykorzystanie danych biometrycznych w obrocie. Należy jednak podkreślić, że w ramach art. 9 ust. 2 pkt a RODO, w którym wymienia się tę podstawę, zaznaczono, iż ma być to zgoda wyraźna³⁰. W ramach omawianego rozporządzenia próżno szukać objaśnienia, czym ma się różnić zgoda wyraźna od zgody „zwykłej”, która może być podstawą przetwarzania innych rodzajów danych niż dane szczególnej kategorii³¹, do której należą dane biometryczne. Jednocześnie ograniczono ogólnie możliwość skorzystania z tego wyjątku w przypadku, w którym prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania tych danych.

Warto w tym kontekście wskazać również, że wymóg wyraźnej zgody dla przetwarzania danych osobowych szczególnej kategorii został zaczerpnięty bezpośrednio z dyrektywy 95/46/WE³², która została uchylona (i zastąpiona) przez RODO. Stąd można odwoływać się do poglądów i opinii wyrażonych w poprzednim stanie prawnym. W pierwszej kolejności należy zaznaczyć, co wynika z samej konstrukcji językowej, że zgoda wyraźna powinna stanowić wyższy poziom potwierdzenia w stosunku do (zwykłej) zgody, która jest chociażby przewidziana w ramach art. 6 ust. 1 lit. a RODO. Stąd musi ona w opinii autora spełniać wszelkie wymagania dla (zwykłej) zgody³³, jak również zapewniać szerszy

rzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (w:) P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, komentarz do art. 9.

²⁷ Zob. I. Małobęcka-Szwast, K. Syska, *Podwójne podstawy prawne przetwarzania danych wrażliwych*, „ABI Expert” 2019, nr 4, s. 57.

²⁸ A tym bardziej omówienie łącznie przesłanek przewidzianych w art. 9 i 6 RODO.

²⁹ W odróżnieniu od podstaw z art. 6 RODO, w tym przypadku przewidziano wymóg „wyraźnej” zgody.

³⁰ Ten rodzaj zgody pojawia się w RODO również w art. 49 ust. 1 lit. a w odniesieniu do transferu danych osobowych do państwa trzeciego.

³¹ Zgodnie z art. 6 ust. 1 lit. a RODO.

³² Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L nr 281 z 1995 r., s. 31).

³³ Zgodnie z motywem 32 RODO zgoda „powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świad-

zakres informacji dla osoby, która ją wyraża. W doktrynie wskazuje się, że nie powinna ona budzić wątpliwości co do faktu jej udzielenia³⁴. Wydaje się zatem, że nacisk położony jest w tym przypadku na świadomość osoby udzielającej zgody, a nie na jej formę. Potwierdzać to może również stanowisko Europejskiej Rady Ochrony Danych³⁵.

Zwraca się również często uwagę na aspekt dobrowolności udzielenia tego rodzaju zgody. W szczególności ma to miejsce w przypadku stosunków w środowisku pracy, gdzie usytuowanie w hierarchii może mieć znaczenie dla udzielanych zgód. W szczególności powyższe będzie widoczne w sytuacji, w której pracodawca będzie próbował wprowadzać rozwiązania, które z braku innych możliwości będą się opierały na przetwarzaniu danych osobowych na podstawie zgody. Należy jednocześnie zauważyć, że powyższe zostało należycie zaadresowane w ramach polskiego ustawodawstwa, albowiem w ramach art. 22^{1b} § 1 Kodeksu pracy³⁶ przewidziano, że dane szczególnej kategorii mogą być przetwarzane jedynie, gdy są przekazane z inicjatywy podmiotu danych. Trudno w takich okolicznościach wyobrazić sobie za skuteczne twierdzenie, że pracownik z własnej inicjatywy udzielił pracodawcy zgody na przetwarzanie jego danych biometrycznych w celu kontroli wejścia do budynku z wykorzystaniem tej technologii w większości przypadków. Zupełnie inaczej przedstawiać się może taka sytuacja, gdy konkretny pracownik miałby dostęp do istotnych dokumentów danego pracodawcy, przy spełnieniu podstawowych zasad ich zabezpieczenia.

Następnie wskazano na wyjątek, zgodnie z którym przetwarzanie danych biometrycznych jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą. Wyjątek ten odnosi się jednak do szczególnych praw w zakresie: prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii Europejskiej lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. Wyjątek ten nie ma już zatem potencjalnie nieograniczonego zakresu, jak ma to miejsce w przypadku standardowej zgody. W tym przypadku odwołano się bezpośrednio

dome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia”.

³⁴ P. Litwiński (red.), *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)*, (w:) P. Litwiński (red.), *Ogólne rozporządzenie...*, komentarz do art. 9.

³⁵ Guidelines 05/2020 on consent under Regulation 2016/679, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, s. 20 (dostęp: 15.03.2022 r.).

³⁶ Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (tekst jedn. Dz.U. z 2022 r., poz. 1510, z późn. zm.); dalej k.p.

do regulacji dotyczących szeroko pojętego prawa pracy, co oznacza, że nie zawężono ich jedynie do regulacji Kodeksu pracy.

Kolejnym wyjątkiem jest przetwarzanie, które może być niezbędne w celu ochrony żywotnych interesów podmiotu danych lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody. W przypadku tej przesłanki odniesiono się zatem do pojęcia występującego już w RODO w charakterze podstawy dla przetwarzania danych innych niż dane osobowe szczególnej kategorii, a jednocześnie dodano element stanu faktycznego, zgodnie z którym osoba, której dane dotyczą, nie może mieć możliwości samodzielnego wyrażenia takiej zgody. Co ważne, możliwość taka może być wyłączona zarówno przez okoliczności, np. zdrowotne, jak również przez okoliczności prawne związane z taką osobą. Nie wydaje się jednak, aby miała ona szerokie zastosowanie w odniesieniu do danych biometrycznych.

Natomiast w ramach art. 9 ust. 2 lit. e wskazuje się, że można przetwarzać dane szczególnej kategorii, które zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą. W ramach rzeczowej przesłanki należy zatem zwrócić uwagę na dwa elementy konstrukcyjne: 1) upublicznienie danych osobowych; 2) przez osobę, której dane te dotyczą. Oba te elementy muszą być przy tym spełnione łącznie. Omawiana przesłanka nie znajdzie zatem zastosowania w przypadku, gdy dane osobowe wrażliwe zostaną upublicznione przez jakąkolwiek inną osobę, niż osoba której dotyczą³⁷, jak również w przypadku, gdy dojdzie do ich ujawnienia, ale nie będzie ono mieściło się w granicach upublicznienia, tj. dojdzie do tego w ramach wymiany prywatnych informacji. Przesłanka ta jest szczególnie ciekawa do analizy w odniesieniu do danych biometrycznych. Dane te bowiem mogą być ujawniane przez osoby, których dotyczą, np. w wyniku standardowej działalności takich osób, w przypadku rejestracji ich postury, zdjęcia twarzy lub innych części ciała, które mogą być nośnikiem danych biometrycznych, czy szeroko rozumianego zachowania. W każdym z tych przypadków bez wątplenia dojdzie do ujawnienia przez osobę, której dane dotyczą, i najczęściej będzie takie ujawnienie nosiło znamiona publicznego. Wydaje się, że prawodawca unijny nie przewidział takiej sytuacji, jednakże bezpośrednio wykluczyła możliwość zastosowania analizowanej przesłanki w przypadku monitoringu wizyjnego Europejska Rada Ochrony Danych³⁸. Na tej samej podstawie niemożliwe będzie wykorzystanie w ten sposób danych biometrycznych zaczerpniętych ze zdjęć udostępnionych przez daną osobę fizyczną. W obu przypadkach zachodzi bowiem ten sam problem – dane, jeśli już, zostały upublicznione w zupełnie innym celu niż ten, do którego w następstwie ich upublicznienia można by je wykorzystać.

³⁷ Nawet w przypadku działania za zgodą osoby, której dane te dotyczą.

³⁸ Zob. Wytyczne European Data Protection Board 3/2019 z dnia 29 stycznia 2020 r. w sprawie przetwarzania danych osobowych przez urządzenia wideo, s. 19, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf (dostęp: 10.03.2022 r.).

Dodatkowo przetwarzać dane biometryczne można, jeśli jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy. W tym zakresie w szczególności może mieć to znaczenie dla danych daktyloskopijnych lub np. DNA. W tym przypadku nie ulega jednak wątpliwości, że celem jest umożliwienie sądom dostępu do danych, które są im niezbędne dla sprawowania wymiaru sprawiedliwości. Podobnego rodzaju przesłanką jest niezbędność ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego³⁹.

W praktyce najczęściej wykorzystywanymi przesłankami przetwarzania danych biometrycznych jest zgoda podmiotu danych oraz wypełnienie obowiązków i wykonywanie szczególnych praw przez administratora lub podmiot danych we wskazanych dziedzinach⁴⁰. W pierwszym przypadku najczęściej stosuje się wyjątek w odniesieniu do różnego rodzaju metod uwierzytelniania, a w drugim, w szczególności w uzasadnionych przypadkach w ramach kontroli dostępu w zakładach pracy⁴¹. Zarazem są to również te przypadki, w których najczęstsze zastosowanie mają usługi i produkty oparte na przetwarzaniu danych biometrycznych. W przypadku danych szczególnej kategorii należy jednak zdecydowanie ostrożniej podejść do weryfikacji potencjalnego naruszenia ogólnych zasad ochrony danych osobowych czy okoliczności, które towarzyszą spełnianiu tych przesłanek, w szczególności wyrażaniu zgody, co było już nadmienione.

4.2. DODATKOWE WYMAGANIA ZWIĄZANE Z PRZETWARZANIEM DANYCH BIOMETRYCZNYCH

Sama weryfikacja możliwości zastosowania jednego z wyjątków omówionych w poprzednim podrozdziale nie będzie wystarczająca dla zapewnienia zgodności z obowiązującymi przepisami. RODO przewiduje bowiem wiele dodatkowych wymagań, które trzeba wypełnić⁴². W szczególności należy wymienić obowiązek przewidziany w art. 35 RODO, zgodnie z którym jeżeli dany rodzaj przetwarzania⁴³ z dużym prawdopodobieństwem może powodować wysokie ryzyko naru-

³⁹ Państwa te mają zapewnić, że odnośne przepisy są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

⁴⁰ To jest wyjątki określone w art. 9 ust. 2 lit. a i b.

⁴¹ Chodzi o kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony zgodnie z art. 22^{lb} § 2 k.p.

⁴² Autor nie odwołuje się w tym przypadku do ogólnych zasad przetwarzania danych wskazanych w RODO, które mają zastosowanie do wszelkiego rodzaju danych osobowych, ale skupia się jedynie na wymaganiach związanych z danymi szczególnej kategorii.

⁴³ Ze względu na swój charakter, zakres, kontekst i cele.

szenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem ich przetwarzania musi przeprowadzić ocenę skutków takiego przetwarzania dla ochrony danych osobowych⁴⁴. Powyższe zostało przewidziane w szczególności dla przetwarzania przy wykorzystaniu nowych technologii, a więc w przypadku danych biometrycznych, które z zasady wymagają „specjalnego przetwarzania technicznego”. Dodatkowo wprowadzono również katalog przykładowych sytuacji, dla których wymagane jest przeprowadzenie DPIA, w których między innymi wymieniono przetwarzanie na dużą skalę szczególnych kategorii danych osobowych, czy systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie⁴⁵. Obie powyższe sytuacje mogą mieć szczególne znaczenie dla technologii biometrycznych i możliwości wykorzystania technologii opartych na przetwarzaniu tego rodzaju danych, a zatem uprawnione jest uogólnienie, że w odniesieniu do przetwarzania danych tego rodzaju niezbędne będzie przeprowadzenie DPIA.

Zwraca się jednocześnie uwagę, że organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania wskazanej oceny skutków dla ochrony danych. Obecnie obowiązujący Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony⁴⁶ przewiduje obowiązek wykonania DPIA dla operacji przetwarzania w postaci systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie wykorzystujących elementy rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni.

Dodatkowo wprowadzono jednak ograniczenie, zgodnie z którym „do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa”. Stąd należy uznać, że rzeczony obowiązek nie obejmuje tradycyjnego monitoringu, który nie wykorzystuje jakichkolwiek dodatkowych możliwości rozpoznawania lub identyfikacji osób lub konkretnych atrybutów, a zarazem wykorzystywany jest jedynie w sytuacji analizy zarejestrowanych sytuacji naruszeń prawa. Jednakże w przypadku stosowania rozwiązań tego rodzaju, np. dla kontroli dostępu wykorzystującej funkcjonalność rozpoznawania twarzy, niezbędne będzie przeprowadzenie DPIA, jak również weryfikacja, czy odpowiednio spełniane są inne zasady wskazane w RODO, w tym zasada minimalizacji danych w celu ograniczenia ryzyka ponoszonego przez osoby, których te dane dotyczą⁴⁷. Powyższe jest przedmiotem analizy w ramach decyzji

⁴⁴ Ang. Data Protection Impact Assessment – DPIA.

⁴⁵ Zgodnie z art. 35 ust. 3 lit. b i c RODO.

⁴⁶ „Monitor Polski” 2019 r., poz. 666.

⁴⁷ Tak również: Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, październik 2018 r., s. 36.

organów nadzoru, które zwracają uwagę m.in. że należy ocenić, czy identyfikacja za pomocą danych biometrycznych jest konieczna i proporcjonalna do celów uwierzytelniania lub bezpieczeństwa, ponieważ – zdaniem organu nadzoru – o ile biometria może być wykorzystywana do kontroli wstępu do pomieszczeń z uwagi na istotną potrzebę bezpieczeństwa, to nie może być wymagana w stosunku do wszelkiego rodzaju pomieszczeń. Podobny wydźwięk ma wiele decyzji odnoszących się do możliwości wykorzystania danych biometrycznych⁴⁸.

4.3. OGRANICZENIA NATURY ETYCZNEJ DOTYCZĄCE WYKORZYSTANIA DANYCH BIOMETRYCZNYCH

Poruszana tematyka jest ważna nie tylko z prawnego punktu widzenia, ale również, a może przede wszystkim, z etycznego. Coraz szersze wykorzystanie nowinek technologicznych nie pozostaje bowiem bez wpływu na człowieka, którego wolności są stale ograniczane. Zauważa się przy tym, że biometria musi być postrzegana odrębnie od innych przypadków nowych technologii, jak np. sztucznej inteligencji, analityki danych⁴⁹, robotyki, nanotechnologii i innych⁵⁰. Podkreślenia wymaga bowiem, co zostało już przywołane w ramach rozważań dotyczących danych szczególnej kategorii, że dane biometryczne mogą nieść ze sobą wiele dodatkowych informacji, których wykorzystanie może być uznawane za znaczącą ingerencję w prywatność danej osoby. Stąd też wskazuje się, że przekazanie lub zbieranie danych biometrycznych może być określane jako oddawanie części siebie⁵¹. Stwierdzenie to może być uważane za hiperbolę, ale jego autorzy nie pozostawili go bez dostatecznej argumentacji. Wywiedziono je bowiem z analogii przekazania danych biometrycznych do pobrania próbki żywego organizmu, z uwzględnieniem odrębności obu sytuacji. W obu przypadkach można uzyskać wiele dodatkowych informacji, w tym również odnoszących się do zdrowia podmiotu danych, które pierwotnie nie były celem ich przekazania. Niewątpliwie już wskazane środki prawne zapewniające ograniczenie możliwości przetwarzania danych biometrycznych wywierają skutek w postaci zapewnienia odpowiedniego

⁴⁸ Komunikat Urzędu Ochrony Danych Osobowych, *Dane biometryczne mogą być wykorzystywane tylko w wyjątkowych sytuacjach*, 3.03.2021 r., <https://uodo.gov.pl/pl/138/1943> (dostęp: 8.03.2022 r.).

⁴⁹ Należy jednak zwrócić uwagę, że sztuczna inteligencja i analityka danych mogą wykorzystywać metody biometryczne w pewnym zakresie i w ten sposób stać się częścią rozwiązania dotyczącego danych biometrycznych.

⁵⁰ B.-A. Schuelke-Leech, *A model for understanding the orders of magnitude of disruptive technologies*, "Technological Forecasting and Social Change" 2018, Vol. 129, s. 270 i n.

⁵¹ A. Alterman, *A piece of yourself: Ethical issues in biometric identification*, "Ethics and Information Technology" 2003, Vol. 5(3), s. 139. Podobnie: A. Sprokkereef, P. de Hert, *Biometrics, privacy and agency. In Second generation biometrics: The ethical, legal and social context*, New York 2012, s. 82 i n., czy A. K. Jain, A. Kumar, *Biometric recognition: an overview. In Second generation biometrics: The ethical, legal and social context*, New York 2012, s. 51.

poziomu etyki stosowania mechanizmów opartych na przetwarzaniu danych tego rodzaju. W szczególności należy podkreślić, że w przypadku szerokiego zakresu decyzji dotyczących tej problematyki podkreśla się obowiązek zapewnienia prywatności⁵² osób fizycznych i ich niedyskryminacji⁵³. W doktrynie można się jednak spotkać z poglądem, że pomimo faktu odnoszenia się w ramach przepisów również do wielu zagadnień etycznych związanych z wykorzystaniem danych biometrycznych, nie są one wystarczające⁵⁴.

Istotnie wątpliwe etycznie wydaje się wykorzystanie systemów rozpoznawania twarzy na szeroką skalę⁵⁵. W szczególności na podkreślenie w odniesieniu do omawianej technologii zasługuje stwierdzenie, że systemy rozpoznawania twarzy są najbardziej niebezpiecznym mechanizmem inwigilacji kiedykolwiek wymyślonym⁵⁶, z którym autor się całkowicie zgadza. Systemy tego rodzaju są stosowane obecnie powszechnie jedynie w celu zapewnienia wyższego poziomu bezpieczeństwa, gdyż w odniesieniu do innych użyć budzą społeczny opór. W tym kontekście należy wskazać, że wiele z informacji, które technologia ta umożliwia zbierać, może prowadzić do dyskryminacji osoby, np. ze względu na pochodzenie rasowe lub etniczne. Systemy rozpoznawania twarzy również nie są idealne i podlegają wielu błędom, które same w sobie mogą być uznawane za dyskryminujące. W szczególności należy w tym kontekście przywołać badanie przeprowadzone przez NIST⁵⁷, który to instytut szczegółowo przeanalizował wiele systemów rozpoznawania twarzy dostarczonych przez ich wytwórców. Najlepsze z przebadanych systemów zapewniały ponad 99% dokładność wyników, a ich dostawcy odpowiadają za większą część rynku tej technologii. Należy jednak zauważyć, że znacząca większość⁵⁸ dostawców podobnych rozwiązań notowało zdecydowanie niższe wyniki, w szczególności w ramach rozróżnień pomiędzy płciami i rasami, obnażając największą ilość błędów w odniesieniu do czarnoskórych kobiet⁵⁹. Sama technologia może zatem w tym przypadku umożliwiać lub nawet powodować szerszą dyskryminację.

⁵² Tak np. A. Alterman, *A piece of yourself*..., s. 140.

⁵³ Może mieć to w szczególności wyraz w decyzji Prezesa Urzędu Ochrony Danych Osobowych z dnia 18 lutego 2020 r., nr ZSZZS.440.768.2018., której przedmiotem było przetwarzanie danych biometrycznych dzieci w celu weryfikacji dostępu do stołówki.

⁵⁴ A. North-Samardzic, *Biometric Technology and Ethics: Beyond Security Applications*, "Journal of Business Ethics" 2020, Vol. 167, s. 433 i n.

⁵⁵ Zob. Biometrics Institute, *State of Biometrics 2020*, s. 8.

⁵⁶ W. Hartzog, E. Selinger, *Just a Face in the Crowd? Not Anymore*, "The New York Times", April 18, 2018.

⁵⁷ Ang. National Institute of Standards and Technology.

⁵⁸ W ujęciu ilościowym.

⁵⁹ P. Grother, M. Ngan, K. Hanaoka, *Facial Recognition Vendor Test, Part 3: Demographic Effects*, National Institute of Standards and Technology, U.S. Department of Commerce, 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> (dostęp: 11.03.2022 r.).

Kolejnym etycznym wyzwaniem, które jest wskazywane stosunkowo często, jest tzw. *function creep*, co rozumie się jako możliwe nadużycie danych biometrycznych w ramach eksploatacji ich poza pierwotnym celem, do którego zostały one przeznaczone lub na który wyrażono zgodę albo też zbieranie nadmiarowych danych. Najczęściej przywoływanym przykładem tego zjawiska jest numer ubezpieczenia społecznego⁶⁰ w USA, który początkowo nie mógł być wykorzystywany do identyfikacji jednostki⁶¹, a następnie upowszechnił się jako jeden z podstawowych dokumentów używanych na potrzeby identyfikacji⁶². Jest to oczywiście sytuacja, która może mieć miejsce w odniesieniu do wszelkich innych rodzajów danych, jednakże w przypadku danych biometrycznych zagrożenie wydaje się być zdecydowanie większe z racji informacji, jakie dane biometryczne mogą obejmować. Należy przy tym zauważyć, że zwykły system do rozpoznawania twarzy, wykorzystywany np. na lotnisku lub w innym miejscu publicznym, może mimochodem zbierać dodatkowe informacje będące również danymi szczególnej kategorii, np. dotyczące przynależności etnicznej czy dane o stanie zdrowia, nie wspominając o „tradycyjnych” danych osobowych⁶³.

W odniesieniu do oceny możliwości wykorzystania systemów opartych na danych biometrycznych podkreśla się istotną rolę balansu pomiędzy prywatnością osób fizycznych i bezpieczeństwem publicznym, które jest najczęściej wykorzystywanym argumentem do uzasadnienia możliwości korzystania z nich. Jednocześnie wielu badaczy zwraca uwagę, że debata dotycząca możliwości wdrożenia technologii biometrycznych wskazuje na niezbędność zachowania proporcjonalności w odniesieniu do prywatności⁶⁴. Jest to również jeden z elementów podkreślanych w ramach przywołanej już opinii w sprawie zmian sytuacji w dziedzinie technologii biometrycznych⁶⁵, a także jedna z wiodących zasad prawa ochrony danych osobowych i ich zabezpieczenia, zgodnie z analizowanymi przepisami. O tym, że takie zabezpieczenia mają sens, może świadczyć chociażby wnioskowanie przez FBI w 2016 r. o wyłączenie ich systemu danych biometrycznych z niektórych ograniczeń prawnych dotyczących prywatności⁶⁶. Stąd też w doktrynie wskazuje się częstokroć, że prywatność, która wydaje się być, w odniesieniu do analizowanej tematyki, wartością najbardziej zagrożoną

⁶⁰ Właściwie *Social Security Number*.

⁶¹ Co nawet było zaznaczone na kartach dokumentu *Social Security Number*.

⁶² E. Mordini, *Ethics and Policy of Biometrics*, (w:) M. Tistarelli, S. Z. Li, R. Chellappa (eds.), *Handbook of Remote Biometrics*, London 2009, s. 294.

⁶³ Podobnie: E. Mordini, S. Massari, *Body, biometrics and identity*, „Bioethics” 2008, Vol. 22, Issue 9, s. 491.

⁶⁴ Nuffield Council on Bioethics, *The Forensics Use of Bioinformatics: Ethical Issues*, Cambridge, Londyn 2007.

⁶⁵ Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) przyjęta 27 kwietnia 2012 r., s. 8.

⁶⁶ N. Boy, E. K. U. Jacobsen, K. Lidén, *Societal Ethics of Biometric Technologies*, Oslo 2018, s. 8.

w kontekście oceny z etycznego punktu widzenia⁶⁷, należy do problematyk natury prawniczej w większym stopniu aniżeli etycznej, wzięwszy pod uwagę ustawodawstwo zapewniające liczne zabezpieczenia dla praw jednostki, w tym prywatności⁶⁸.

5. PODSUMOWANIE I WNIOSKI

Rozwój rynku rozwiązań opartych na technologii biometrii jest bardzo dynamiczny. Zgodnie z najnowszymi raportami do 2025 r. jego przychód wzrośnie do ponad 68 bilionów dolarów⁶⁹. Wskazuje się przy tym, że oprócz ciągłego i dynamicznego rozwoju technologii ma na to wpływ również na otoczenie prawne. Powyższe jest jednak spowodowane nie ze względu na zniesienie ograniczeń prawnych, lecz wprowadzenie dodatkowych wymagań, które uzasadniają poszukiwanie nowych rozwiązań technologicznych umożliwiających ich wypełnienie, jak np. dyrektywa PSD2⁷⁰. Dyrektywa ta wprowadza dodatkowe wymagania autoryzacyjne dla sektora bankowego, które bezpośrednio przełożyły się na rozwój w obszarze metod autoryzacji, w tym wykorzystania technologii biometrycznych. Zgodnie z badaniami przeprowadzonymi na zlecenie jednego z dostawców rozwiązań płatniczych, aż 92% ankietowanych konsumentów w Polsce uważa, że odcisk palca jest najbezpieczniejszą metodą uwierzytelniania płatności⁷¹. W ramach innych badań rozpoznano podobne rezultaty, podkreślając dodatkowo, że dla większości użytkowników metod biometrycznej weryfikacji tożsamości nie powoduje ona obaw o bezpieczeństwo wykorzystywanych danych osobowych⁷².

⁶⁷ Zaznaczenia wymaga również, że analiza etyczna rozwiązań biometrycznych wydaje się koncentrować wokół tematyki prywatności z uwagi na fakt, że dane biometryczne są uznawane po prostu za bardziej wrażliwy rodzaj danych. Tak np.: R. Evans, M. McNamee, G. Owen, *Ethics, nanobiosensors and elite sport: The need for a new governance framework*, "Science and Engineering Ethics" 2017, Vol. 23, Issue 6, s. 1487–1505.

⁶⁸ L. Royakkers, J. Timmer, L. Kool, E. Rinie van, *Societal and ethical issues of digitization*, "Ethics and Information Technology" 2018, Vol. 20, Issue 2, s. 127–142.

⁶⁹ Biometric System Market with COVID-19 Impact by Authentication Type, Offering, Type, Vertical And Region – Global Forecast to 2025, Marketsandmarkets, 2020.

⁷⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L nr 337 z 2015 r., s. 35).

⁷¹ Badanie dotyczące technologii biometrycznych w Polsce, Fabrizio Ward LLC na zlecenie Visa, przeprowadzone w lipcu 2019 r., <https://www.visa.pl/visa-everywhere/blog/bdp/2020/06/19/biometria-jak-to-1592575916129.html> (dostęp: 2.03.2022 r.).

⁷² T. Mendyk-Krajewska, *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, „Roczniki Kolegium Analiz Ekonomicznych” 2019, nr 54, s. 44.

Co ciekawe, potwierdzają to również badania przeprowadzone w czasach, w których nie było powszechnie dostępnych wielu mechanizmów związanych z wykorzystaniem danych biometrycznych⁷³.

W tym samym czasie zgłaszane są jednak poważne obawy związane z wykorzystaniem niektórych technologii związanych z danymi biometrycznymi na szeroką skalę, w tym np. technologii rozpoznawania twarzy. Choć technologia ta jest już obecnie wykorzystywana w szczególności do zapewnienia bezpieczeństwa w miejscach publicznych, takich jak porty lotnicze, to jej powszechne wykorzystanie, jak się wydaje, jest możliwe jedynie w państwach, w których prawa człowieka nie są odpowiednio traktowane lub respektowane. Przywołać można przykład Chin, które wprowadzają rozwiązania tego rodzaju w celu umożliwienia wykorzystania systemu punktacji obywatelskiej. W ramach przykładu nie-spotykanej skali wykorzystania danych biometrycznych należy przywołać także Kuwejt, w którym po atakach terrorystycznych z 2015 r. ogłoszono ogromne inwestycje w stworzenie narodowej bazy biometrycznej. Jest to obecnie pierwsze państwo, w którym obowiązkowe jest poddanie się powszechnemu badaniu DNA dla jego rezydentów, jak również osób podróżujących do tego państwa pod groźbą kary pozbawienia wolności⁷⁴.

Zauważa się, że największymi etycznymi zagrożeniami i jednocześnie ograniczeniami do wykorzystania technologii opartych na danych biometrycznych są jednocześnie te, które stanowią wyzwania prawne i znajdują swoje odzwierciedlenie w obowiązujących przepisach, jak w szczególności prywatność. Jak się wydaje, najwięcej obiekcji wobec szerokiego zastosowania metod biometrycznych przynosi obawa o bezpieczeństwo zasobu ich wzorców czy możliwość naruszenia zasady proporcjonalności poprzez stworzenie takiego centralnego zbioru. Aby bowiem umożliwić szerokie korzystanie z takich metod, musi istnieć szybka możliwość identyfikacji lub weryfikacji konkretnej osoby, do czego niezbędne jest porównanie jej cechy z wcześniej posiadanym i zagregowanym w odpowiedniej bazie wzorcem. Na ten aspekt powołuje się wiele dokumentów międzynarodowych⁷⁵.

Oprócz wymagań prawnych, które wprowadzają wiele ograniczeń mających na celu ochronę prywatności osób fizycznych przed dostępem do danych biometrycznych osób niepowołanych, z pomocą może przychodzić również technologia,

⁷³ Podobnie P. J. Trocchia, T. L. Ainscough, *Characterizing consumer concerns about identification technology*, "International Journal of Retail and Distribution Management" 2006, Vol. 34, Issue 8, s. 609–620.

⁷⁴ N. Boy, E. K. U. Jacobsen, K. Lidén, *Societal Ethics...*, s. 2.

⁷⁵ Począwszy chociażby od opinii 3/2005 Grupy Roboczej Art. 29 w sprawie wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie. Tak również: E. Kindt, *Biometric applications and the data protection legislation. The legal review and the proportionality test*, "Datenschutz und Datensicherheit" 2007, Vol. 31, s. 166.

a dokładniej ograniczenia technologiczne. Wydaje się bowiem, że ograniczeniem możliwości wystąpienia kolejnej etycznej wątpliwości tzw. *function creep*, oprócz przepisów prawnych⁷⁶, jest również fakt, że bazy danych biometrycznych zajmują duże przestrzenie dyskowe, a ich późniejsze przeszukanie w zadowalającym czasie wymaga ogromnych mocy obliczeniowych. W związku z powyższym ograniczenie ilości zbieranych danych może być⁷⁷ wymogiem technicznym niezbędnym do odpowiedniego funkcjonowania systemów wykorzystujących dane biometryczne w czasie rzeczywistym⁷⁸.

Ponieważ aspekt technologiczny może być szybko zagospodarowany, a wątpliwości natury moralnej i etycznej zasadniczo przekładają się następnie na wymagania prawne, wydaje się, że to właśnie ograniczenia związane z przetwarzaniem danych biometrycznych stanowią obecnie najważniejszy mechanizm bezpieczeństwa gwarantujący w pewnej mierze ochronę praw jednostki, w tym w szczególności prywatności. Jednocześnie, co zauważa część badaczy, szeroki zakres regulacji zdaje się odpowiadać na podnoszone w ramach badań nad etyką zagrożenia wiążące się z wykorzystaniem technologii biometrycznych.

REFERENCES

- Alterman A., *A piece of yourself: Ethical issues in biometric identification*, "Ethics and Information Technology" 2003, Vol. 5(3)
- Bolle R. M., Connell J. H., Pankanti S., Ratha N. K., Senior A. W., *Biometria*, Warszawa 2016
- Boy N., Jacobsen E. K. U., Lidén K., *Societal Ethics of Biometric Technologies*, Oslo 2018
- Evans R., McNamee M., Owen G., *Ethics, nanobiosensors and elite sport: The need for a new governance framework*, "Science and Engineering Ethics" 2017, Vol. 23, Issue 6
- Gutfeter W., Pacut A., *Człowiek w systemie biometrycznym*, (w:) M. Tomaszewska-Michalak, T. Tomaszewski (red.), *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, Warszawa 2015
- Jain A. K., Kumar A., *Biometric recognition: an overview. In Second generation biometrics: The ethical, legal and social context*, New York 2012
- Jain A. K., Ross A., Nandakumar K., *Introducing to biometrics*, New York 2011
- Jain A. K., Ross A., Prabhakar S., *An introduction to biometric recognition*, "IEEE Transactions on Circuits and Systems for Video Technology" 2004, Vol. 14(1)
- Jasserand C. A., *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*, "European Data Protection Law Review" 2016, Vol. 2, Issue 3

⁷⁶ W szczególności zasady minimalizmu z RODO.

⁷⁷ Przynajmniej jeszcze przez pewien czas, dopóki technologia nie znajdzie odpowiedzi na ten problem.

⁷⁸ Tak również: E. Mordini, S. Massari, *Body...*, s. 492.

- Jóźwiak I. J., Szczepanik M., *Wydajność i niezawodność wielomodułowych systemów biometrycznych*, „Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie” 2013, z. 64
- Kindt E. J., *Biometric applications and the data protection legislation. The legal review and the proportionality test*, „Datenschutz und Datensicherheit” 2007, Vol. 31
- Kindt E. J., *Having Yes, Using No? About the New Legal Regime for Biometric Data*, “Computer Law & Security Review” 2018, Vol. 34, Issue 3
- Kindt E., *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Dordrecht, Leuven 2013
- Krassowski K., Sołtyszewski I., *Biometria – zarys problematyki*, „Problemy Kryminalistyki” 254/06
- Litwiński P. (red.), *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)*, (w:) P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021
- Małobęcka-Szwast I., Syska K., *Podwójne podstawy prawne przetwarzania danych wrażliwych*, „ABI Expert” 2019, nr 4
- Mendyk-Krajewska T., *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, „Roczniki Kolegium Analiz Ekonomicznych” 2019, nr 54
- Mordini E., *Ethics and Policy of Biometrics*, (w:) M. Tistarelli, S. Z. Li, R. Chellappa (eds.), *Handbook of Remote Biometrics*, London 2009
- Mordini E., Massari S., *Body, biometrics and identity*, “Bioethics” 2008, Vol. 22, Issue 9
- Mordini E., Ottolini C., *Body identification, biometrics and medicine: ethical and social considerations*, “Annali dell’Istituto Superiore di Sanità” 2007, Vol. 43, Issue 1
- Mordini E., Tzovaras D. (eds.), *The Second Generation Biometrics: The Ethical, Legal and Social Context*, London 2012
- North-Samardzic A., *Biometric Technology and Ethics: Beyond Security Applications*, “Journal of Business Ethics” 2020, Vol. 167
- Nuffield Council on Bioethics, *The Forensics Use of Bioinformatics: Ethical Issues*, Cambridge, Londyn 2007
- Porzeżyński M., *Własność danych w dobie internetu rzeczy*, „Państwo i Prawo” 2021, z. 2
- Porzeżyński M., *Wycena danych – złota XXI wieku*, (w:) M. Jankowska, M. Pawełczyk, S. Augustyn, M. Panfil (red.), *Znaczenie wyceny własności intelektualnej. Proving the worth. Putting a value on intellectual property*, Warszawa 2019
- Royakkers L., Timmer J., Kool L., Rinie van E., *Societal and ethical issues of digitization*, “Ethics and Information Technology” 2018, Vol. 20, Issue 2
- Schuelke-Leech B.-A., *A model for understanding the orders of magnitude of disruptive technologies*, “Technological Forecasting and Social Change” 2018, Vol. 129
- Selinger E., Leong B., *The Ethics of Facial Recognition Technology*, (w:) C. Véliz (ed.) *The Oxford Handbook of Digital Ethics*, London 2022
- Sprokkereef A., Hert P. de, *Biometrics, privacy and agency. In Second generation biometrics: The ethical, legal and social context*, New York 2012
- Sprokkereef A., Hert P. de, *Ethical practice in the use of biometric identifiers within the EU*, “Law, Science and Policy” 2007, Vol. 3

- Stasiak Ł., Czajka A., Strzelczyk P., Chochowski M., Pacut A., *Od biometrii do bezpiecznej biometrii*, SECURE 2006, Bezpieczeństwo – czas na przełom, Warszawa, 17–18 października 2006 r.
- Tistarelli M., Li S. Z., Chellappa R. (eds.), *Handbook of Remote Biometrics*, 2009
- Trocchia P. J., Ainscough T. L., *Characterizing consumer concerns about identification technology*, “International Journal of Retail and Distribution Management” 2006, Vol. 34, Issue 8
- Wayman J. L., Jain A. K., Maltoni D., Maio D., *Biometric Systems. Technology, Design and Performance Evaluation*, London 2005
- Zajkowska A., Zimnoch W., *Technologie biometryczne – istota i możliwości wykorzystania w MSP*, (w:) S. Lachiewicz, M. Matejun (red.), *Problemy współczesnej praktyki zarządzania*, t. 2, Łódź 2007

Inne:

- Decyzja Prezesa Urzędu Ochrony Danych osobowych z dnia 18 lutego 2020 r., nr ZSZZS.440.768.2018
- Dokument Rady Unii Europejskiej nr 15395/14 z 19 grudnia 2014 r.
- Informacja Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechnienia danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi, Warszawa 2017
- Opinia 2/2012 w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych (WP 192) przyjęta 22 marca 2012 r.
- Opinia 3/2005 Grupy Roboczej Art. 29 w sprawie wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie
- Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) przyjęta 27 kwietnia 2012 r.
- Opinia 4/2007 w sprawie pojęcia danych osobowych (WP 136) przyjęta 20 czerwca 2007 r.
- Working document on biometrics (WP80) przyjęty 1 sierpnia 2003 r.