



GIODO

Generalny Inspektor
Ochrony Danych Osobowych



INFORMACJA

Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechnienia danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi.

Czerwiec 2017



**20-LECIE PRAWA DO OCHRONY
DANYCH OSOBOWYCH W POLSCE**

1. Definicja danych biometrycznych

W celu jednoznacznego rozumienia biometrii i danych biometrycznych poniżej przytoczono różne, funkcjonujące obecnie definicje tych pojęć. Przedstawiono definicję zarówno samego pojęcia biometrii zawartą w normie ISO/IEC 2382 z 2015 roku oraz definicje danych biometrycznych dostępne w normie PN-ISO 19092:2008, na portalu Wobopedia, jak i rozporządzeniu Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływie tych danych, nazywanym RODO.

- W ISO/IEC 2382:2015 pojęcie „Biometria” – zdefiniowane zostało 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;*
- W PN-ISO 19092:2010 pojęcie „Dane biometryczne” zdefiniowano jako *informacje wyodrębnione z próbki biometrycznej i stosowane do utworzenia wzorca odniesienia, albo wzorca dopasowywanego;*
- W Webopedia (www.webopedia.com) pojęcie „Dane biometryczne” zdefiniowane zostało jako *ogólne określenie dowolnych danych komputerowych wytworzonych w procesie przetwarzania biometrycznego. Obejmuje to dane dotyczące próbki biometrycznej, modelu biometrycznego, wybranych cech charakterystycznych (fingerprints), wartości podobieństwa oraz wszystkie dane weryfikacyjne i identyfikacyjne takie jak imię i nazwisko oraz dane demograficzne;*
- W Opinii 4/2007 Grupy Roboczej Art. 29 (WP136) pojęcie „Dane biometryczne” zdefiniowane zostało jako *właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą wyłącznie danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopień prawdopodobieństwa;*
- W art. 3 pkt 14 RODO pojęcie „Dane biometryczne” zdefiniowane zostało jako *dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.*

Jak można było zauważyć, niektóre z wymienionych wyżej definicji, definiują dane biometryczne jako właściwości biologiczne, fizjologiczne lub czynnościowe (ruch, głos) w

formie, w jakiej one występują u źródła danych, tj. formie surowej, nieprzetworzonej (np. definicja zawarta w opinii 4/2007 Grupy Roboczej Art. 29). Inne zaś definiują dane biometryczne jako wybrane lub wyliczone cechy nieprzetworzonego (surowego) obrazu próbki biometrycznej przedstawione w formie kodu wzorca cyfrowego.

Zgodnie z definicją danych biometrycznych zawartą zarówno w wymienionych wyżej normach PN-ISO 19092:2008, ISO/IEC 2382:2015, jak i rozporządzeniu RODO, mówiąc o danych biometrycznych będziemy dalej mieć na myśli cechy charakterystyczne próbki biometrycznej uzyskane w wyniku ich komputerowego przetworzenia do postaci elektronicznej w formie tzw. wzorca cyfrowego. Właściwość tę wyraźnie podkreśla motyw 51 RODO, w którym wyjaśnia się, że np. „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”. Dane tego typu, zgodnie z art. 9 RODO, zaliczane są do szczególnych kategorii danych osobowych, których przetwarzanie dozwolone jest wyłącznie w przypadku wyrażenia zgody osoby, której dane dotyczą lub jeśli zezwala na to przepis prawa.

Warto zwrócić uwagę, że większość z wymienionych wyżej definicji, w tym RODO definiuje dane biometryczne w kontekście weryfikacji lub identyfikacji osób. Definicje te nie obejmują w związku z tym przetwarzania danych biologicznych, fizycznych, fizjologicznych, czy powtarzalnych czynności osoby, które nie umożliwiają weryfikacji lub identyfikacji osoby lecz mogą być wykorzystywane w innych celach, jak np. ocena zmęczenia, stresu, stanów emocjonalnych czy stanu zdrowia.

2. Specyfika danych biometrycznych

Specyfika przetwarzania danych biometrycznych była przedmiotem wielu dyskusji na forum Grupy Roboczej Art. 29¹. Wyniki tych dyskusji utrwalone zostały w takich dokumentach ww. Grupy jak:

- Working document on biometrics (WP80) przyjęty 1 sierpnia 2003 r.,

¹ Grupa Robocza Art. 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwana dalej Grupą Roboczą Art. 29, powołana została na mocy art. 29 Dyrektywy 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.

- Opinia 4/2007 w sprawie pojęcia danych osobowych (WP 136) przyjęta 20 czerwca 2007 r.
- Opinia 2/2012 w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych (WP 192) przyjęta 22 marca 2012 r.
- Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) przyjęta 27 kwietnia 2012 r.

Problemy związane z wykorzystaniem biometrii w procesach uwierzytelnienia się użytkowników w usługach online były ostatnio również w obszarze zainteresowań międzynarodowej grupy ds. ochrony danych osobowych i telekomunikacji², która opublikowała dokument zatytułowany „Working Paper on Biometrics in Online Authentication” (Dokument roboczy dotyczący Biometrii w usługach autoryzacji online), w którym przedstawiono zalety i obawy związane ze stosowaniem biometrii w systemach uwierzytelniania.

2.1. Źródła danych biometrycznych

Istnieje wiele różnych źródeł danych biometrycznych – mogą one obejmować fizyczne, fizjologiczne, behawioralne lub psychologiczne cechy danej osoby fizycznej. Jak stwierdzono w dokumencie roboczym na temat biometrii z 2003 r. WP80, istnieją dwie główne kategorie technik biometrycznych związanych z rodzajami próbek biometrycznych. Są to:

- techniki fizyczne i fizjologiczne, w ramach których mierzy się i porównuje fizyczne i fizjologiczne cechy danej osoby, takie jak: kształt i układ linii papilarnych palca, kształt i układ naczyń krwionośnych palca, obraz tęczówki lub siatkówki oka, kształt i rysy twarzy, kształt dłoni, ucha lub ust, zapach ciała, cechy charakterystyczne głosu, wzór DNA itp.;
- techniki behawioralne, przy pomocy których mierzy się zachowanie danej osoby i które obejmują: cechy charakterystyczne podpisu odręcznego (kształt liter oraz sposób i dynamika ich tworzenia), dynamikę pisania na klawiaturze, sposób poruszania się (chodu), cechy odzwierciedlające myśli podświadome, takie jak oszustwo, kłamstwo itp.

Wśród tych ostatnich należy zwrócić uwagę na pojawiające się techniki mające podstawy psychologiczne. Obejmują one pomiar reakcji na konkretne sytuacje lub testy w celu dopasowania do danego profilu psychologicznego³. Techniki te mogą być wykorzystywane

² International Working Group on Data Protection in Telecommunications.

³ Opinia 3/2012 Grupy roboczej art. 29 w sprawie zmian w dziedzinie technologii biometrycznych.

między innymi do rozpoznawania w tłumie osób mających określone zamiary, np. kradzież, czy stany emocjonalne związane z zamiarem popełnienia przestępstwa typu przemyt narkotyków czy atak terrorystyczny.

2.2. Wymagane właściwości danych biometrycznych

Do najważniejszych wymagań dotyczących właściwości źródeł danych biometrycznych mających istotne znaczenie dla jakości i niezawodności ich przetwarzania należą:

- uniwersalność - definiowana jako właściwość polegająca na możliwości pobrania próbki od możliwie największej grupy osób (np. kształt dłoni będzie bardziej uniwersalną cechą niż odcisk linii papilarnych, gdyż dla niektórych osób może być niemożliwe pobranie odcisku linii papilarnych określonego palca (np. brak palca) podczas, gdy możliwe będzie pobranie kształtu dłoni);
- unikalność – definiowana jako właściwość polegająca na posiadaniu cech wyróżniających daną próbkę od innych danego rodzaju próbek (np. układ linii papilarnych palca bardziej wyróżnia osobę niż jej kolor włosów);
- stałość (niezmiennność) – definiowana jako cecha polegająca na niezmienności danej cechy w czasie;
- łatwość pobrania (collectability) – łatwość i wygoda pobrania próbki;
- wydajność (performance) – solidność, pewność, szybkość i dokładność przetwarzania;
- akceptowalność – brak negatywnych skojarzeń, brak obaw wpływu na zdrowie, a także przyjazność i wygoda dla osób w procesie pobierania próbki (np. łatwiej jest pobrać odcisk palca niż kod DNA);
- łatwość obejścia (Circumvention) – definiowana jako możliwość oszukania systemu (np. łatwiej jest oszukać system podstawiając nagrany dźwięk niż kod DNA).

2.3. Dokładność wyników przetwarzania danych biometrycznych

Jak wskazano w opinii 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) przy stosowaniu systemów biometrycznych trudno uzyskać wyniki w 100% zgodne ze wzorcem. Wynika to z różnic dotyczących otoczenia przy pozyskiwaniu danych (oświetlenia, temperatury itp.) i różnic dotyczących zastosowanego sprzętu (kamer, urządzeń skanujących itp.) podczas odpowiednio tworzenia wzorca odniesienia i wzorca do

porównania. Do najczęściej stosowanych miar oceny skuteczności systemów biometrycznych należy wskaźnik fałszywej akceptacji i wskaźnik fałszywego odrzucenia, które zdefiniowane są następująco:

- Wskaźnik błędnych akceptacji (ang. False Accept Rate – FAR), jest to prawdopodobieństwo, że system biometryczny nieprawidłowo zidentyfikuje daną osobę fizyczną lub nie odrzuci oszusta. Wskaźnik pozwala na pomiar procentu nieważnych próbek dopasowania, które zostały nieprawidłowo zaakceptowane;
- Wskaźnik błędnych odrzuceń (ang. False Reject Rate – FRR), jest to prawdopodobieństwo, że w systemie dojdzie do błędnego odrzucenia. Do błędnego odrzucenia dochodzi, jeżeli osoba fizyczna nie zostaje dopasowana do jej własnego istniejącego wzorca biometrycznego.

W systemie doskonałym wartość wskaźników FAR i FRR wyniosłaby zero, ale częściej wykazują one korelację negatywną. Zmniejszenie wskaźnika FAR często powoduje wzrost poziomu wskaźnika FRR i odwrotnie.

Oceniając, czy dokładność danego systemu biometrycznego jest wystarczająca, bierze się pod uwagę zazwyczaj wiele czynników. Do najważniejszych z nich należą: cel przetwarzania, w tym skutki błędnej akceptacji (FAR) oraz błędnego odrzucenia (FRR), wielkości populacji oraz odporność na oszustwa. Wartości parametrów FAR i FRR silnie zależne są od rodzaju próbki biometrycznej. Tak np. w biometrii bazującej na układzie linii papilarnych czy układzie żył krwionośnych palca współczynnik błędnych uwierzytelnień (FAR) wynosi obecnie ok 0,0001 % zaś w biometrii opartej na układzie żył krwionośnych dłoni ten sam współczynnik wynosi około 0,00001%. Podawane wyżej wartości odnoszą się do najnowszych rozwiązań technologicznych. Parametry te w ostatnich latach ulegały szybkim zmianom. Dla przykładu wartość parametru FAR dla systemu uwierzytelniania bazującego na układzie żył krwionośnych dłoni (PalmSecure) firmy Fujitsu, którego obecna wartość, dla najnowszej generacji systemu wynosi 0,00001%, w poprzedniej generacji tego systemu wynosiła zaledwie 0,0118%. O tym, jak szybki był w ostatnich 10 latach postęp w doskonaleniu metod identyfikacji biometrycznej, najlepiej świadczyć może porównanie wyżej wymienionych wartości parametrów FAR i FRR z tymi, jakie odnotowywano w roku 2007, które wg Raportu zamieszczonego w Haking PL 7/2007, przedstawiono w tabeli 1.

Rodzaj biometrii	FAR (%)	FRR (%)
Linie papilarne	0,2000	0,0100
Geometria dłoni	0,2000	0,2000
Siatkówka oka	10,0000	0,0010
Tęczówka oka	0,0005	0,0005
Geometria twarzy	1,0000	0,5000

Tabela 1 *Porównanie dokładności popularnych metod biometrycznych wg. Raportu Hardware hacking – oszukiwanie zabezpieczeń biometrycznych, Haking PL, 7/2007.*

Ważnym dla bezpieczeństwa identyfikacji biometrycznej parametrem jest również odporność na różne próby obejścia poprzez np. wykonanie i użycie falsyfikatu próbki biometrycznej. Tak np. dla odcisków linii papilarnych jedną z metod „oszukiwania” czytnika jest użycie zamiast palca danej osoby, spreparowanego odlewu wykonanego z żelu, dla geometrii twarzy może to być np. odpowiednio wykonana fotografia.

Stąd we współczesnych czytnikach danych biometrycznych jednym z głównych zabezpieczeń jest weryfikacja, czy badana próbka pochodzi od człowieka za pośrednictwem różnych dodatkowych sensorów i analizatorów. Ich zadaniem jest weryfikacja, czy pobierana cecha biometryczna pochodzi od osoby żywej poprzez badanie rozkładu temperatury, wilgotności, współczynnika kwasowości pH, zmienności źrenicy pod wpływem światła czy przepływu krwi w badanej próbce.

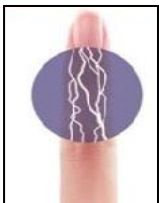
3. Przegląd najczęściej stosowanych technik przetwarzania danych biometrycznych – ich wady i zalety

3.1. Biometria linii papilarnych



W metodzie tej początkowo wzorce tworzone były przy użyciu układu optycznego, gdzie obraz oświetlonych linii papilarnych rejestrowany był przez matrycę CCD. Obecnie do pobierania próbek stosowane są układy sensorowe, dające w wyniku informację graficzną od razu w postaci cyfrowej. Obraz linii papilarnych jest rejestrowany na powierzchni dwuwymiarowej tablicy sensorów jako zmiany pojemności lub temperatury między zróżnicowaną powierzchnią palca (rowki i grzbiety linii papilarnych). Każdy piksel tablicy jest reprezentowany przez jednobajtową liczbę o wartości proporcjonalnej do odległości sensora od najbliższego elementu powierzchni palca. Uzyskany cyfrowy obraz linii papilarnych jest analizowany następnie pod kątem identyfikacji lokalnych nieciągłości we wzorze linii papilarnych nazywanych minucjami. We wzorze takim można wyróżnić około 100 charakterystycznych punktów (początki, zakończenia, rozwidlenia, oczka, haczyki, itp.) z których tworzony jest matematyczny wzorec odcisku palca. Utworzony matematyczny wzorec może być poddawany jeszcze kompresji lub kodowaniu i dopiero zostaje wykorzystywany do weryfikacji lub identyfikacji poprzez porównanie z innym wzorcem zapisanym w bazie danych. Metoda jest znana od dawna, jest wysoce niezawodna i nieszkodliwa, chociaż pojawiają się głosy kwestionujące niepowtarzalność linii papilarnych. Wiarygodność metody jest zależna od liczby minucji branych pod uwagę. Czytniki linii papilarnych są zwykle wyposażane dodatkowo w mechanizmy rozpoznawania imitacji (manekina) palca. Metoda ta zawodzi tam, gdzie osoby rozpoznawane mają brudne, wytarte lub skaleczone palce. Łatwa dostępność odcisków palca budzi obawy, że zostaną pobrane i wykorzystane bez wiedzy i zgody właściciela. Ze względu na wykorzystywanie tej metody w kryminalistyce, ma ona negatywne psychologiczne konotacje z policyjnymi metodami śledczymi.

3.2. Biometria układu żył krwionośnych palca



W metodzie tej obraz naczyń krwionośnych palca tworzy się wykorzystując oddziaływania światła o częstotliwości odpowiadającej bliskiej podczerwieni z hemoglobina we krwi. Wykorzystywane są obecnie trzy metody naświetlania palca przy użyciu diod LED (odbicie światła, transmisja, boczne naświetlanie).

Część promieniowania podczerwonego jest zaabsorbowana przez hemoglobinę, a reszta pada na kamerę CCD, tworząc obraz naczyń krwionośnych. Kopiowanie lub fałszowanie danych biometrycznych pozyskiwanych w tej technologii jest prawie niemożliwe. Żyła jest niewidoczna, ponieważ znajduje się w środku palca. Nawet jeśli uda się skopiować obraz palca, niemożliwe jest skopiowanie lub sfabrykowanie układu żył. Blizna ani żadna substancja nie ma wpływu na pobieranie danych biometrycznych, system pobiera wzorzec układu żył palca poprzez przeświecenie go promieniami podczerwieni. Nie mają na to wpływu żadne blizny, ani substancje na powierzchni palca. Technika ta jest skuteczna i akceptowalna społecznie. Różnorodność obrazów naczyń krwionośnych zapewnia wysoką dokładność rozpoznawania. Metoda ta nie ma negatywnych skojarzeń z metodami policyjnymi. Należy do technik, w których do pobrania wzorca trudno użyć manekina (pobrać bez wiedzy właściciela). Technologię tę na szeroką skalę wprowadziła firma Hitachi. Skomplikowany obraz układu żył palca, minimalizuje się w niej do postaci cyfrowego wzorca zajmującego niewielki obszar pamięci (ok. 500 Bajtów), co daje dużą prędkość identyfikacji przy zachowaniu wysokiej gwarancji bezpieczeństwa ($FAR = 0,0001\%$, $FRR = 0,1\%$). Metoda ta jest powszechnie stosowana przez banki japońskie (około 80 % wszystkich banków). W Polsce od stycznia 2013 r. metoda ta wykorzystywana jest w placówkach banku BPH jako opcjonalny środek uwierzytelniania klientów banku.

3.3. Biometria kształtu dłoni



Trójwymiarowy obraz kształtu dłoni oświetlonej promieniami podczerwonymi rejestrowany jest kamerą CCD. W obrazie tym dokonuje się pomiaru geometrycznych parametrów dłoni (długości i szerokości palców, szerokości i grubości śródręcza, proporcji śródręcza lub palców itp.) Na

podstawie zmierzonych parametrów i wyliczonych proporcji jest tworzony wzorzec (wektor cech, zajmujący od kilku do kilkunastu bajtów pamięci.) Do porównania badanej dłoni z wzorcem wykorzystuje się najczęściej ważoną metrykę euklidesową. Technika badania geometrii dłoni jest łatwa do wykonania, nieinwazyjna i społecznie

akceptowalna. Jest ona jednak podatna na oszustwa, ponieważ kształt dłoni bliźniaków może być identyczny, a krewnych bardzo podobny. U wielu osób pomiar budzi wątpliwości związane z higieną, gdyż dłoń należy przyłożyć do czytnika. Do wad tej metody należy również duży rozmiar czytnika, co ogranicza jej stosowanie.

3.4. Biometria układu żył krwionośnych dłoni



W technologii identyfikacji biometrycznej wykorzystującej układ żył krwionośnych dłoni, wprowadzonej przez japońską firmę Fujitsu, dane od identyfikowanej osoby pobierane są przez czytnik, do którego należy zbliżyć dłoń na odległość kilku centymetrów. Czujnik na wstępie poprzez analizę emitowanego ciepła bada, czy w dłoni występuje przepływ krwi, a następnie skanuje dłoń nieszkodliwym dla zdrowia promieniowaniem podczerwonym. Do odczytu obrazu układu żył krwionośnych wykorzystuje się właściwość polegającą na tym, że emitowane promieniowanie podczerwone przenika przez skórę i kości, a zatrzymuje się w znacznym stopniu na hemoglobinie. Na podstawie odczytanego obrazu w układzie czujnika tworzony jest wzorzec zawierający informacje o charakterystycznych punktach układu żył krwionośnych, które są unikatowe dla każdej osoby. W technologii tej brane jest pod uwagę ok. 5 milionów punktów charakteryzujących obrazu układu żył skanowanej dłoni. Pobieranie próbek biometrycznych na etapie identyfikacji lub weryfikacji osoby jest czynnością intuicyjną i szybką. Nie jest łatwe pobranie próbki bez wiedzy osoby, której dotyczy (jeśli osoba jest przytomna). Metoda pobierania próbki jest higieniczna (wystarczy zbliżyć dłoń) i neutralna dla zdrowia, co wpływa znacząco na jej społeczną akceptowalność. Metoda ma zastosowanie dla prawie każdej osoby (dla porównania zapis linii papilarnych jest niemożliwy dla 2-3% populacji). Charakteryzuje ją duża szybkość identyfikacji i wysoki poziom bezpieczeństwa ($FAR=0,00001\%$, $FRR=0,01\%$)⁴. Duże bezpieczeństwo przechowywania danych i odporność na kojarzenie danych z innymi zbiorami danych uzyskać można poprzez szyfrowania wzorców, gdzie dla każdego odrębnego systemu może być użyty inny klucz szyfrujący. Wymiary czytnika są niewielkie, co umożliwia ich stosowanie nawet w laptopach i smartfonach. Dostępne są różne obudowy czytników, w tym czytniki wbudowane w myszkę.

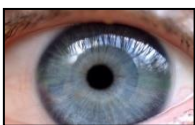
⁴ Whiter Paper, Fujitsu PalmSecure – rozwiązania biometryczne dla skutecznej identyfikacji.

3.5. Biometria tęczówki oka



W technologii identyfikacji biometrycznej wykorzystującej obraz tęczówki oka (kolorowego pierścienia tkanki otaczającej źrenicę). Do identyfikacji wykorzystuje się około 250 miniaturowych zmarszczek, rowków i punktów, które są charakterystyczne dla każdej osoby i nie ulegają zmianie na skutek starzenia się. Pomiar dokonywany jest z odległości od kilku do kilkudziesięciu centymetrów z wykorzystaniem kamer naprowadzających. Proces ekstrakcji cech biometrycznych tęczówki rozpoczyna się od jej zlokalizowania w obrazie przez określenie środka źrenicy. Stosowane obecnie metody ekstrakcji cech nie biorą pod uwagę koloru tęczówki. Utworzony na podstawie analizy obrazu siatkówki cyfrowy wzorzec zawierający informacje o charakterystycznych jej cechach zajmuje zwykle około 512 bajtów pamięci. Metoda jest nieinwazyjna i oceniana jako łatwa do użycia. Jej wadą jest czułość na ruchy oczu i odbicia światła. Zakłócenia w identyfikacji mogą być spowodowane stanami chorobowymi. Metoda wymaga dużej współpracy użytkownika lub drogich zaawansowanych kamer pobierających obraz. Wymaga zdjęcia okularów. Na obecnym etapie rozwoju metoda ta w porównaniu z innymi charakteryzuje się niewielkim poziomem bezpieczeństwa ($FAR=0,01\%$, $FRR=1,76\%$)⁵. Jej wadą jest możliwość pobrania próbki (przy zastosowaniu sprzętu wysokiej jakości) bez wiedzy osoby, której dotyczy. Metoda jest mało odporna na fałszerstwa. Wiele obecnie funkcjonujących systemów biometrycznych daje się oszukać nawet przy użyciu zdjęć wykonanych na zwykłej drukarce laserowej.

3.6. Biometria siatkówki oka



W technologii identyfikacji biometrycznej wykorzystującej obraz siatkówki oka wykorzystuje się niezmienność i unikalność dla każdej osoby rozkładu naczyń krwionośnych siatkówki. W technologii tej obraz próbki biometrycznej pobiera się przy użyciu kamery, która naświetla wnętrze oka promieniami bliskiej podczerwieni. W technologii tej wykrywa się soczewki transplanty czy sztuczne oko. Z uwagi na usytuowanie siatkówki wewnątrz oka, niepowtarzalny dla każdej osoby układ jej żył krwionośnych oraz brak możliwości skonstruowania fałszywej siatkówki ze względu na jej właściwości optyczne, technologia ta jest uważana za jedną z najmniej podatnych na oszustwa. Jej wadą są wysokie koszty aparatury pomiarowej (kamer) oraz mała społeczna akceptowalność, co wynika między

⁵ M. Plucińska, J. Wójtowicz; Analiza technik biometrycznych do uwierzytelniania osób; w Elektronika 4/2014 str. 64-66

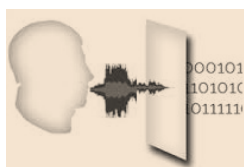
innymi z jej inwazyjność (wymaga oświetlenia wnętrza oka). Osoby, od których pobierana jest próbka obawiają się o swoje zdrowie.

3.7. Biometria rysów twarzy



W technologii identyfikacji biometrycznej wykorzystującej rysy twarzy zarejestrowany obraz poddawany jest odpowiedniej obróbce i matematycznemu przekształceniu do postaci wzorca cyfrowego. Obróbka obrazu polega na zlokalizowaniu twarzy i oczu, a następnie analizowana jest pozycja oczu w stosunku do całej twarzy. Na tym etapie następuje również rozpoznanie okularów czy zarostu. W kolejnym etapie tworzona jest geometryczna siatka charakterystycznych punktów twarzy, która zapisywana jest w określonej formie cyfrowej. Identyfikacja i weryfikacja wykorzystująca ten rodzaj biometrii do porównywania wykorzystuje nie obraz twarzy, ale jej charakterystyczne punkty. W celu wykrycia fałszyfikatów (fotografia, manekin), stosuje się kamery rejestrujące emitowane ciepło i jego rozkład niewidoczny optycznie. Zaletą obrazu termicznego jest to, że można go rejestrować bez oświetlenia, nie podlega on zmianom pod wpływem kierunku padania światła i występujących cieni. Zaletą tej metody jest łatwość stosowania, nieinwazyjność i dość duża akceptowalność społeczna. Należy jednak zaznaczyć, że metoda ta stosowana bez odczytu termicznego, np. z wykorzystaniem kamer użytych w laptopach czy telefonach komórkowych, jest podatna na fałszerstwa takie jak fotografia, maska, manekin. Wykorzystanie zaś systemu kilka kamer, w tym termicznych, które są w stanie rozróżnić nawet bliźniaków jest kosztowne i w związku z tym nie jest powszechnie stosowane.

3.8. Biometria głosu



W biometrii głosowej stosowanych jest kilka metod analizy i rozpoznawania. Jedną z najprostszych i najstarszych jest metoda polegająca na badaniu wypowiedzanego tekstu lub żądanej frazy z nagrany wzorcem. Inną metodą jest rozpoznawanie mówiącego na podstawie analizy brzmienia jego głosu i porównaniu wyznaczonych jego cech z wzorcem. Podczas analizy brzmienia głosu wyznaczane są takie parametry, jak częstotliwość podstawowa, dźwięk nosowy, intonacja, tj. zmiana modulacji, itp. Metoda ta może być wykorzystana do identyfikacji na odległość, np. do identyfikacji przez telefon. Jest wykorzystywana w aplikacjach na telefony komórkowe, internetowych usługach bankowych

oraz handlu elektronicznym. Najnowsze metody biometrii głosowej bazują na analizie cech charakterystycznych dla częstotliwościowego drgań fali głosowej. Analiza taka wymaga przetworzenia sygnału otrzymanego z mikrofonu na sygnał cyfrowy. W sygnale tym wydziela się odcinki mowy od odcinków ciszy, a następnie odcinki mowy poddaje się analizie w zakresie częstotliwości drgań fali głosowej. W analizie tej stosuje się przekształcenie uzyskanego widma transformatą Fouriera w celu utworzenia wzorców odpowiednio odniesienia i porównania. Do określenia podobieństwa zarejestrowanego wzorca odniesienia z wzorcem próbki głosu do porównania osoby poddawanej identyfikacji stosuje się różne algorytmy bazujące na modelach markowa lub wykorzystujące sieci neuronowe. Zaletą metod identyfikacji głosowej jest łatwość ich użycia, duża akceptowalność społeczna oraz niewielkie koszty. Ich wadą jest natomiast podatność na błędy spowodowane zmianą głosu np. chrypką czy stanem emocjonalnym. Ponadto pobierana próbka głosu może być zakłócana złymi warunkami akustycznymi, hałasem lub szumem. Metoda ta jest podatna na oszustwo przy użyciu odtworzonego nagrania.

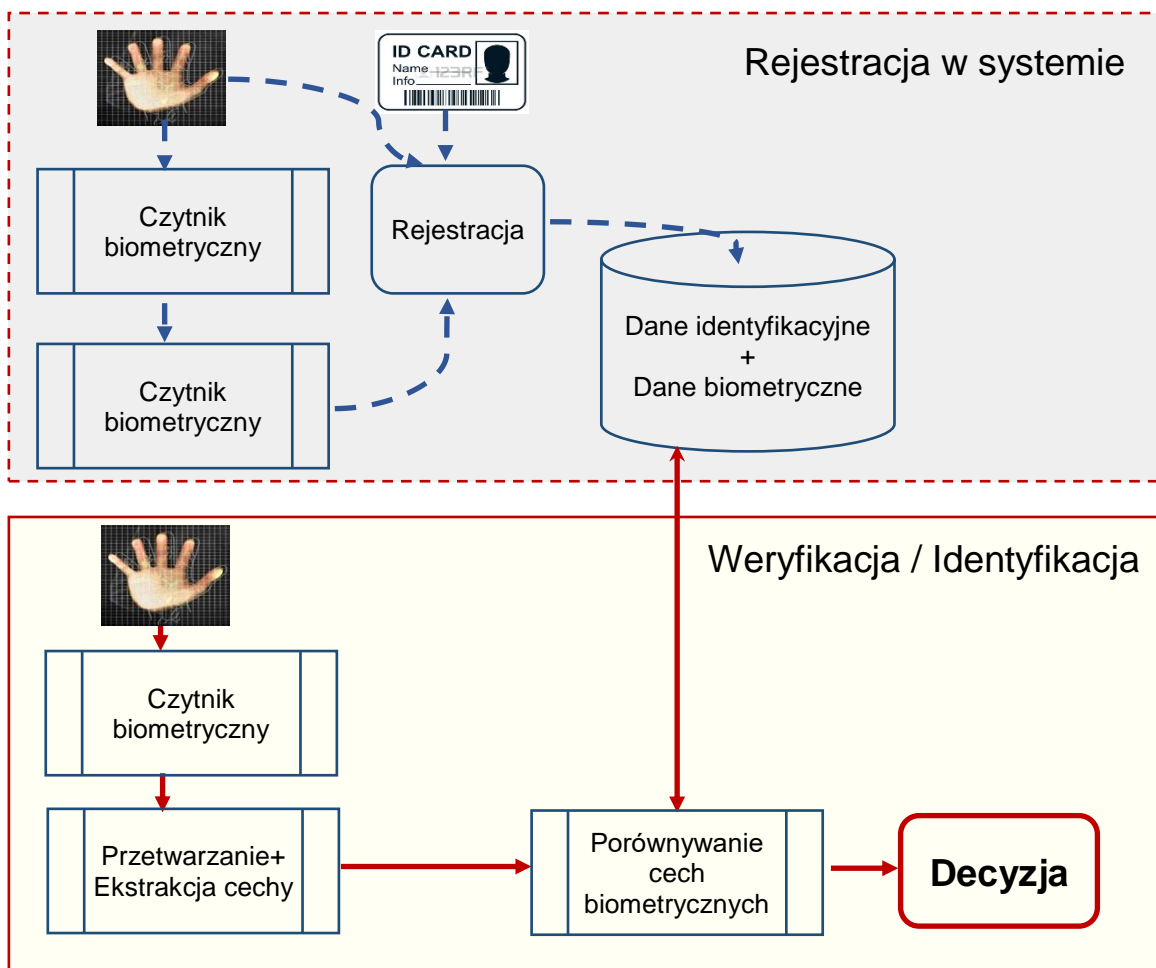
4. Główne etapy przetwarzania danych biometrycznych

Przetwarzanie danych w systemie biometrycznym zwykle obejmuje takie procesy, jak: rejestracja, przechowywanie i kojarzenie (identyfikacja lub weryfikacja), które można opisać następująco:

- Rejestracja danych biometrycznych określana jest jako wszystkie procesy przeprowadzane w systemie biometrycznym w celu wyodrębnienia danych biometrycznych ze źródła danych biometrycznych i powiązania tych danych z daną osobą fizyczną. Ilość i jakość danych wymaganych podczas rejestracji powinny być wystarczające, aby umożliwić zapewnienie dokładności przy identyfikacji, kategoryzacji, weryfikacji lub uwierzytelnieniu danej osoby bez rejestrowania zbyt wielu danych. Ilość danych wyodrębnionych ze źródła danych biometrycznych podczas rejestracji musi być odpowiednia ze względu na cel przetwarzania i poziom skuteczności systemu biometrycznego.
- Przechowywanie danych biometrycznych określane jest jako czynność ich przechowywania w celu późniejszego wykorzystania. Dane te mogą być przechowywane lokalnie, np. w czytniku urządzenia, za pomocą którego dokonano ich rejestracji, w centralnej bazie danych systemu biometrycznego lub urządzeniu noszonym przez osobę fizyczną, od której dane te zostały pobrane (np. na karcie elektronicznej).

- Kojarzenie danych biometrycznych jest to proces porównywania danych biometrycznych/wzorca biometrycznego (pobranych w procesie rejestracji) z danymi biometrycznymi/wzorcem biometrycznym pobranymi do celów identyfikacji, weryfikacji lub kategoryzacji.

W procesach przetwarzania biometrycznego wyżej wymienione etapy występują w różnych konfiguracjach, których ogólna struktura jest jak na rys. 1. Różnice poszczególnych konfiguracji mogą dotyczyć miejsca składowania próbek odniesienia pobranych w procesie rejestracji oraz miejsca wykonywania czynności obliczeniowych na danych, jak np. przetwarzanie surowego obrazu próbki do postaci cyfrowego wzorca czy procesu porównywania wzorców.



Rys. 1. Ogólna struktura systemu biometrycznego.

5. Zagrożenia związane z przetwarzaniem danych biometrycznych

Obawy i wątpliwości dotyczące zagrożeń związanych z zastosowaniem biometrii w procesach identyfikacji, weryfikacji czy klasyfikacji różnią się w zależności od rodzaju czynnika biometrycznego, stosowanej technologii czy konfiguracji systemu. Część zagrożeń jest jednak wspólna. Są to zagrożenia związane z naturalnymi właściwościami danego rodzaju cech biometrycznych i jakością stosowanej technologii. Do najważniejszych z nich należą:

- **Możliwość ujawnienia danych wrażliwych.** Właściwości niektórych źródeł danych biometrycznych, z których pobierane są próbki, takich jak siatkówka i źrenica oka, właściwości ruchowe (chód, sposób wypowiedzania się) mogą zdradzać poza cechami niezbędnymi do identyfikacji czy weryfikacji osoby także inne właściwości, jak np. zmęczenie, stres, stan zdrowia, w tym bycie pod wpływem narkotyków, czy alkoholu;
- **Ograniczone możliwości zmiany i unieważnienia wzorca.** Technologia biometryczna bazuje na indywidualnych cechach danej osoby, których nie można zmienić w przypadku nieupoważnionego pozyskania przez nieuprawnione osoby (w przeciwieństwie do przypadku ewentualnej utraty hasła czy posiadanej rzeczy, np. karty kredytowej, które w przypadku kompromitacji lub utraty można w każdej chwili zmienić na inne.) Tylko nieliczne systemy są skonstruowane w sposób umożliwiający odnawialność próbek biometrycznych (renewability), dając możliwość zmiany wzorców tak jak w przypadku haseł;
- **Możliwość użycia bez wiedzy osoby, której dane dotyczą.** Wiele danych biometrycznych, takich jak np. obraz twarzy, sposób chodzenia czy właściwości ruchowe, mogą być zarejestrowane i wykorzystane przez system biometryczny bez wiedzy osoby, której dotyczą. Zagrożenie to jest istotne zwłaszcza w kontekście użycia nowoczesnych kamer monitoringu wizyjnego, które wyposażone w specjalne oprogramowanie rozpoznawania twarzy, mogą nie tylko nagrywać obraz otoczenia w celach prewencyjnych i dowodowych na wypadek incydentu, ale również w innych, bliżej nieokreślonych;
- **Trudności pobrania próbki biometrycznej.** Niektóre rodzaje danych biometrycznych mogą być trudne do pobrania, jak np. linie papilarne z wytartych pracą lub skaleczonych palców. Inne dane, jak np. kształt twarzy, może być celowo zniekształcany ubiorem (zasłona, szalik, maska) lub zachowaniem, np. uśmiech, co w konsekwencji może

prowadzić do obniżenia jakości poprzez zwiększenie zawodności systemu (błędne rozpoznanie);

- **Podatność na łączenie danych.** Ograniczone możliwości zmiany danych biometrycznych tak jak np. hasła oraz ograniczona liczba źródeł danych biometrycznych (10 palców, dwie dłonie, jedna twarz) stwarzają ryzyko łączenia danych przetwarzanych przez tę samą osobę w różnych systemach. Dotyczy to sytuacji, kiedy w różnych systemach użyto np. tego samego rodzaju próbki biometrycznej (technologii biometrycznej) i tej samej metody przekształcania surowego obrazu próbki do postaci cyfrowego wzorca.
- **Brak przejrzystości.** Wielu producentów systemów biometrycznych wykorzystuje poufne, znane tylko sobie algorytmy wykorzystywane do przekształceń i porównywania wzorców biometrycznych, przez co nie można ich darzyć takim samym zaufaniem, jak tych, które poddawane są przeglądowi i ocenie stron trzecich. Mogą istnieć wówczas obawy, czy system wykorzystywany jest np. tylko do weryfikacji tożsamości, czy również np. do oceny trzeźwości, stanu zdrowia czy stanów emocjonalnych.
- **Możliwość błędnej identyfikacji, weryfikacji, klasyfikacji.** Technologia biometryczna identyfikacji bazuje na porównywaniu wyekstrahowanych cech biometrycznych pobranej próbki z wyekstrahowanymi w taki sam sposób cechami biometrycznymi próbki wzorca. Stąd różnica pobranych próbek może spowodować różnicę ich wyekstrahowanych cech, co w konsekwencji może prowadzić do błędnego rozpoznania (błędnej akceptacji lub błędnego odrzucenia);
- **Możliwość fałszerstwa.** Niektóre czynniki biometryczne podatne są na próby podrobienia próbki i oszukanie czytnika. Jedną z najbardziej podatnych na podrobienie próbek jest np. odciski linii papilarnych palca.

Waga wskazanych wyżej zagrożeń jest w dużym stopniu uzależniona od rodzaju czynnika biometrycznego, który w konkretnym systemie jest wykorzystywany oraz od architektury całego systemu. Stąd wagę poszczególnych rodzajów zagrożeń dla każdego rodzaju czynnika biometrycznego i architektury systemu biometrycznego należy oceniać odrębnie. Rodzaj i skala poszczególnych zagrożeń dla systemów biometrycznych są zależne, podobnie jak dla każdego innego systemu, od zastosowanych środków i procedur bezpieczeństwa.

Biorąc pod uwagę np. pierwsze z wymienionych wyżej zagrożeń, jakim jest możliwość ujawnienia danych wrażliwych, np. informacji o stanie zdrowia czy bycia pod wpływem środków odurzających na podstawie obrazu oka, zabezpieczeniem zmniejszającym

zagrożenia może być odpowiednia konstrukcja systemu i jego zabezpieczenie przed nieuprawnioną modyfikacją. Algorytm przetwarzania surowego obrazu próbki do formatu wzorca porównania powinien być tak skonstruowany, aby nie brał pod uwagę elementów zmiennych uzależnionych od stanu zdrowia czy bycia pod wpływem środków odurzających poza jedynie tymi, które pozwalają na ustalenie, że próbka pobierana jest od osoby żyjącej. Podobnie dla biometrii bazującej na ocenie wizerunku system powinien być tak skonstruowany, aby wynikiem jego weryfikacji było jedynie stwierdzenie tożsamości lub jej braku, a nie np. pochodzenie etniczne czy rasowe na podstawie informacji o kolorze skóry czy typu urody weryfikowanej osoby. Ponadto konstrukcja tych algorytmów powinna być odpowiednia zabezpieczona przed ich nieuprawnioną modyfikacją.

Inną cechą systemów biometrycznych, od których zależy akceptowalność ich stosowania, jest możliwość pobrania próbki bez wiedzy osoby, której dotyczy. Związane jest to często z właściwością charakteryzującą się łatwością i wygodą pobierania próbek. Są one zazwyczaj bardzo od siebie uzależnione. Tak np. zaletą jaką jest łatwość pobrania próbki biometrycznej w postaci obrazu twarzy (bez potrzeby odpowiedniego ustawiania się do kamery, gdyż system sam analizuje sytuację, naprowadza kamerę i wybiera odpowiednią chwilę pobrania obrazu) skutkuje z drugiej strony wadą, jaką jest zagrożenie jej pobrania bez wiedzy osoby, której dane dotyczą. Podobne relacje odnosić się będą do właściwości próbek behawioralnych osoby, takich jak głos, dynamika pisanie na klawiaturze czy sposób poruszania się.

Jedną z bardzo istotnych właściwości próbek biometrycznych jest ponadto ich niezmienność, co jest cechą pozytywną z punktu widzenia odporności na różnego rodzaju fałszerstwa, gdyż ich sklonowanie na inny organizm żywy nie jest na ogół procesem łatwym. Wymaga zazwyczaj skomplikowanych operacji chirurgicznych. Negatywną cechą takiej niezmienności jest jednak brak możliwości ich zmian w przypadkach, jeśli operacje przetwarzania wykonywane w różnych celach chcemy skutecznie od siebie odizolować. Użycie takiego samego rodzaju danych biometrycznych może prowadzić do skojarzenia danych dotyczących tej samej osoby pochodzących z różnych systemów. Brak możliwości zmian cech danego rodzaju próbki biometrycznej może ponadto utrudniać rozwiązywanie problemów, takich jak potrzeba zmiany czynnika weryfikującego tożsamość danej osoby na skutek np. udanej próby podrobienia jej próbki biometrycznej. Rozwiązaniem dla takich problemów jest stosowanie modyfikowalnych mechanizmów przekształcania surowego obrazu próbki do postaci cyfrowej. Mechanizmy te polegają na możliwości modyfikowania procesu transformacji surowego obrazu próbki do postaci cyfrowej.

Inną wadą systemu identyfikacji biometrycznej jest często brak przejrzystości w zakresie dotyczącym konstrukcji algorytmów, jakie stosowane są do przekształceń wzorców biometrycznych oraz ich porównywania. Algorytmy te, w niektórych przypadkach, objęte są ochroną praw autorskich i odnoszące się do nich szczegóły przetwarzania danych nie są ujawniane.

Biorąc pod uwagę powyższe, wagę każdego z wyżej wymienionych zagrożeń, należy oceniać odrębnie dla każdego rodzajów próbki biometrycznej, algorytmu transformacji surowego obrazu próbki do postaci cyfrowej, sposobu porównywania wzorców (miar ich podobieństwa) oraz architektury systemu biometrycznego.

6. Zalety stosowania danych biometrycznych do identyfikacji i uwierzytelniania

Przetwarzanie danych biometrycznych poza wymienionymi wyżej wadami, posiada również wiele zalet w porównaniu do innych metod identyfikacji, czy weryfikacji osób. Do najważniejszych z nich należą:

- **Brak możliwości dzielenia się danymi** biometrycznymi z inną osobą. Użycie danych biometrycznych zapobiega dzieleniu się użytkownikom danymi identyfikującymi np. podczas wejścia do ściśle chronionych obszarów wymagających bezwzględnej rozliczalności. Różne osoby nie mogą sobie tych danych przekazywać między sobą w celu np. wejścia do ściśle chronionego obszaru;
- **Brak możliwości zapomnienia.** Danych biometrycznych w przeciwieństwie do hasła nie można zapomnieć;
- **Większa odporność na ataki fałszerstwa.** Dane biometryczne są bardziej odporne na ataki fałszerstwa niż inne dane wykorzystywane w procesach uwierzytelniania. Nie można ich pozyskać poprzez ataki typu phishing, podglądnięcie czy odgadnięcie hasła, co może mieć miejsce w przypadku używania innych czynników uwierzytelnienia bazujących na znanym tylko danej osobie sekrecie (hasła) lub posiadanej rzeczy (karta kryptograficzna z nagrany certyfikatem).
- **Duża wiarygodność i niezawodność.** Najnowsze systemy biometryczne charakteryzują się bardzo dużą niezawodnością i dokładnością identyfikacji/weryfikacji.

Dokonując oceny systemu biometrycznego, zawsze należy mieć na uwadze nie tylko parametry charakteryzujące dany rodzaj biometrii (próbki biometrycznej), ale również cel

przetwarzania i związane z tym celem wymagania, takie jak poziom bezpieczeństwa czy szybkość weryfikacji. Na poszczególne techniki należy zatem spojrzeć pod kątem ich najlepszej użyteczności, społecznej akceptowalności, odporności na oszustwa, kosztów oraz bezpieczeństwa. Inne wymagania powinny być brane pod uwagę przy uwierzytelnianiu dostępu do danych bankowych i inne dla takich, jak np. wejście do siłowni. W kontekście różnych zastosowań różne znaczenia mają również wymienione wyżej ryzyka związane z przetwarzaniem danych biometrycznych. Tak np. o ile niewielkie zagrożenie może wynikać z pobrania danych biometrycznych przy wejściu do siłowni bez wiedzy osoby, której dotyczą, to rozwiązanie takie nie może mieć miejsca w odniesieniu do logowania się do systemu informatycznego np. banku, gdzie użytkownik musi być w pełni świadomy, że został w systemie uwierzytelniony, a wykonywane przez niego operacje są rejestrowane i ponosi on za nie określoną odpowiedzialność.

Biorąc zatem pod uwagę wymienione w rozdziale 4 zagrożenia związane z przetwarzaniem danych biometrycznych, cel i zakres ich przetwarzania, a także zakwalifikowanie ich w art. 9 ust. 1 RODO do szczególnych kategorii danych osobowych, każdy przypadek przetwarzania danych biometrycznych należy traktować indywidualnie i zgodnie z art. 35 RODO poprzedzić odpowiednią analizą skutków dla ochrony prywatności.

7. Trudności techniczne i organizacyjne związane z zastosowaniem biometrycznych technik uwierzytelniania, identyfikacji i weryfikacji

W odniesieniu do prawie wszystkich cech biometrycznych największym problemem z ich stosowaniem w praktyce jest to, że nie zawsze mogą one być dostępne. Brak dostępności danego rodzaju próbki może być spowodowana wadami wrodzonymi, kalectwem lub zniszczeniem. Ten ostatni przypadek odnosi się przede wszystkim do układu linii papilarnych, których zniszczenie spowodowane charakterem wykonywanej pracy może być tak duże, że praktycznie uniemożliwia ich wykorzystanie (średnio ich niedostępność ocenia się na 2-3% populacji). Dotyczy to w szczególności osób pracujących w górnictwie, rolnictwie oraz budownictwie.

Duże znaczenia ma również akceptowalność społeczna danego rodzaju technik biometrycznych. Z przeprowadzonych badań⁶ wynika, że strach przed przyłożeniem palca czy oka do urządzenia skanującego jest wciąż duży. Przy czym większą akceptowalnością cieszą

⁶ Badania przeprowadzone przez prof. Annę Koziczak z Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, prezentacja na konferencji Naukowej Biometria 2010 organizowanej przez IMM w Warszawie.

się nieinwazyjne metody pobierania próbki takie jak głos, analiza rysów twarzy, rozpoznawanie wzoru tęczówki oka i podpis odręczny. Duże obawy budzi natomiast pobieranie próbki siatkówki oka, które jest w pewnym stopniu procesem inwazyjnym i użytkownik obawia się o swoje zdrowie. Mało akceptowalne są również metody wymagające dotknięcia urządzenia pomiarowego, takie jak pobieranie odcisku linii papilarnych palca, pobieranie wzoru naczyń krwionośnych palca czy pobieranie kształtu dłoni, które budzą obawy ze względów higienicznych. Odcisk linii papilarnych dodatkowo kojarzy się negatywnie z działaniami policyjnymi.

W praktycznych zastosowaniach istotnymi elementami są dodatkowo wielkość pamięci niezbędna do zapamiętania wzorca, szybkość pobierania próbek i porównywania wzorców oraz łatwość użycia. Względna ocenę wymienionych wyżej parametrów i właściwości przeprowadzoną przez Instytut Maszyn Matematycznych⁷ przedstawiono w tabeli 2.

Parametr, właściwość	Oceny właściwości próbek biometrycznych od najbardziej do najmniej korzystnych
Akceptowalność	głos, rysy twarzy, naczynia krwionośne palca, linie papilarne, kształt dłoni, tęczówka, podpis odręczny, siatkówka
Łatwość użycia	głos, rysy twarzy, kształt dłoni, naczynia krwionośne palca i dłoni, linie papilarne, tęczówka, siatkówka
Czas weryfikacji	linie papilarne, naczynia krwionośne palca, tęczówka, kształt dłoni, naczynia krwionośne dłoni, siatkówka, głos
Czas rejestracji	linie papilarne, naczynia krwionośne palca, naczynia krwionośne dłoni, tęczówka
Wiarygodność	siatkówka, tęczówka, naczynia krwionośne palca, linie papilarne, kształt dłoni, głos, sposób pisania na klawiaturze
Wielkość wzorca	kształt dłoni, siatkówka, tęczówka, naczynia krwionośne palca, linie papilarne, sposób pisania na klawiaturze, głos, naczynia krwionośne dłoni

Tabela 2. *Klasyfikacja parametrów dla różnych technik biometrycznych.*

⁷ Mirosława Plucińska, Jarosław Wójtowicz, Analiza technik biometrycznych do uwierzytelniania osób, w ELEKTRONIKA 4/2014 str. 64-66

8. Zastosowanie biometrii wielomodalnej

Z uwagi na wymienione wyżej trudności, w tym brak dostępności niektórych próbek biometrycznych (zwłaszcza odcisków linii papilarnych) coraz częściej wprowadza się systemy wielomodalne, w których jest możliwość zastosowania różnych rodzajów próbek biometrycznych np. linii papilarnych palca i/lub kształtu twarzy. Niektóre z nich wprowadzane są w celu zwiększenia dostępności inne zaś w celu zwiększenia wiarygodności rozpoznania. W tych pierwszych użytkownik ma możliwość wyboru jednej z dwóch lub więcej możliwych rodzajów próbek biometrycznych. W tych ostatnich natomiast określone próbki biometryczne używane są łącznie w celu zwiększenia wiarygodności systemu. W ostatnim okresie obserwuje się bardzo szybki rozwój biometrii w takich usługach, jak bankowość (banki japońskie, tureckie, polskie) czy dostęp do usług medycznych (szpitale amerykańskie, tureckie), bazujących na biometrii układu żył krwionośnych palca lub dłoni z uwagi na duże jej bezpieczeństwo, dużą odporność na próbę oszustwa oraz trudność ich pobrania bez zgody osoby, której dotyczą (jeśli osoba jest przytomna).

9. Elementy prawne związane z przetwarzaniem danych biometrycznych

Z uwagi na fakt, iż art. 27 UODO nie kwalifikuje danych biometrycznych jako danych osobowych wrażliwych, obowiązki związane z przetwarzaniem danych biometrycznych należy obecnie oceniać na zasadach ogólnych, czyli takich, jakie odnoszą się do tzw. danych zwykłych. Warto przy tym pamiętać, że nie wszystkie dane dotyczące naszego organizmu stanowią dane biometryczne, np. ciśnienie krwi samo w sobie nie stanowi informacji biometrycznej, która odpowiada danym osobowym. Kierunek interpretacji w tym zakresie jednoznacznie wyznacza art. 6 ust. 3 UODO, w którym wskazuje się, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Choć UODO nie zawiera zakazu przetwarzania danych biometrycznych, to należy jednak pamiętać, iż w tego typu sprawach określona musi być celowość i adekwatność przetwarzania danych – ich przetwarzanie powinno pozwalać na osiągnięcie określonego celu, ale jak najmniej ingerować w sferę prywatności danej osoby. Podobne stanowisko zajęła Grupa Robocza Art. 29, która stwierdziła, iż dane biometryczne można przetwarzać, tylko jeżeli

istnieje ku temu podstawa prawna i jeżeli przetwarzane dane są prawidłowe, odpowiednie oraz nienadmierne w stosunku do celów, dla których zostały zgromadzone lub dalej przetworzone. Tak więc, jeżeli mamy do wyboru użycie linii papilarnych albo podpisywanie listy obecności, to jednak użycie linii papilarnych należy uznać jako metodę bardziej ingerującą w naszą prywatność. Z punktu widzenia zasady adekwatności i celowości, w takich sytuacjach nie będzie uzasadnione ich zbieranie i przetwarzanie. Istotne znaczenie dla rozstrzygania spraw dotyczących legalności przetwarzania danych biometrycznych ma orzecznictwo sądów krajowych w tym zakresie, przepisy sektorowe, jak również dotychczasowe stanowiska GODO.

Wkrótce kwestia charakteru danych biometrycznych ulegnie jednak znaczącej zmianie. Od 25 maja 2018 r. stosowane będzie bezpośrednio 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; dalej „RODO”).

RODO wprowadza nie tylko definicję danych biometrycznych, ale również zalicza dane biometryczne do tzw. szczególnych kategorii danych osobowych tzn. danych osobowych wrażliwych. Przesłanki legalizujące przetwarzanie tych danych będą w związku z tym bardziej rygorystyczne niż obecnie.

Zgodnie z art. 4 pkt 14 RODO, „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Określone informacje można uznać za dane biometryczne tylko wtedy, gdy łącznie spełnione zostaną następujące warunki:

- informacje dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej;
- informacje mają charakter danych osobowych;
- informacje są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.

Uregulowania RODO należy rozpatrywać całościowo. Przykładowo użyty w definicji danych biometrycznych „wizerunek twarzy” nie zawsze możemy traktować jako daną biometryczną. Motyw 51 preambuły RODO wyjaśnia, iż 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 potwierdzającej jej tożsamości.

Istotnym novum, jakie wnosi RODO jest wprowadzenie podstaw prawnych dla przetwarzania danych biometrycznych. Art. 9 ust. 1 RODO wprowadza generalny zakaz przetwarzania danych wrażliwych (w tym biometrycznych), z wyjątkiem przepisów szczególnych, które wskazują przesłanki dopuszczające przetwarzanie takich danych.

Zakaz przetwarzania szczególnych kategorii danych osobowych nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków (art. 9 ust. 2 RODO):

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba, że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba której dane dotyczą, nie może uchylić zakazu, o którym mowa w art. 9 ust. 1;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy.

Pośród przesłanek zezwalających na przetwarzanie danych biometrycznych brak jest przesłanki pozwalającej na przetwarzanie danych w związku z zawarciem umowy. Może to prowadzić do sytuacji, w której spośród ww. warunków legalnego przetwarzania danych biometrycznych, najczęściej będziemy mieli do czynienia ze zgodą podmiotu danych. Zgoda na przetwarzanie danych biometrycznych powinna być wyrażona w sposób wyraźny.

RODO wymaga również, aby zgoda ta była dobrowolna, konkretna i świadoma. Innymi słowy, chodzi o to, aby podmiot danych mógł swobodnie wyrazić przyzwolenie (lub nie) na konkretny

sposób wykorzystania lub ujawnienia jego danych osobowych, bez żadnej presji lub przymusu. Odmowa zgody nie może powodować negatywnych skutków dla podmiotu danych.

W odróżnieniu od ustawy o ochronie danych osobowych, która wymaga formy pisemnej dla wyrażenia zgody na przetwarzanie danych wrażliwych, RODO nie określa wprost tej formy. Najważniejsze jest, aby zgoda na przetwarzanie danych miała charakter aktywnego zachowania (*affirmative opt-in act*). Milczenie, „okienka” domyślnie zaznaczone lub niepodjęcie działania odznaczenia „okienka”, nie mogą zatem oznaczać zgody (Motyw 32 RODO). Wyrażna zgoda może mieć więc postać pisemnego (w tym elektronicznego) lub ustnego oświadczenia woli. Rozporządzenie o ochronie danych zastrzega jedynie (art. 7 ust. 1 RODO), że gdy podstawą przetwarzania danych jest zgoda, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła tę zgodę.

Oprócz ww. zasad, RODO dopuszcza wprowadzenie przez państwa członkowskie dalszych regulacji dotyczących przetwarzania danych biometrycznych (art. 9 ust. 4 RODO). Otóż państwa członkowskie mogą zachować lub wprowadzać dalsze warunki, w tym ograniczenia, przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia. Warunki te nie powinny jednak utrudniać swobodnego przepływu danych osobowych w Unii, jeżeli odnoszą się do transgranicznego przetwarzania takich danych (Motyw 53 RODO).

Zmiana przepisów dotyczących ochrony danych osobowych, wprowadzona przez RODO nakłada na administratorów danych wiele nowych – niemających odzwierciedlenia w obecnie występujących przepisach – obowiązków. Do takich obowiązków należy zasada uwzględnienia ochrony danych osobowych w fazie projektowania, tzw. *data protection by design*, w skrócie *privacy by design* (art. 25 ust. 1 RODO).

Ze względu na szczególne czynniki ryzyka związane ze stosowaniem danych biometrycznych, już na etapie projektowania procesu przetwarzania tych danych należy wdrożyć odpowiednie środki techniczne i organizacyjne zaprojektowane w celu skutecznej ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Stosowanie zasady *privacy by design* powinno uwzględniać takie elementy, jak: koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych.

Z przetwarzaniem danych biometrycznych wiąże się także obowiązek przeprowadzenia tzw. oceny skutków dla ochrony danych osobowych (art. 35 RODO). O potrzebie przeprowadzenia takiej oceny RODO informuje w motywie 89 preambuły. Dyrektywa 95/46/WE przewidywała

ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. RODO sugeruje zastąpienie ich skutecznymi procedurami i mechanizmami koncentrującymi się na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Do operacji takich zalicza się w szczególności użycie nowych technologii oraz operacje, które są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych (Motyw 98 preambuły). Oceny skutków dla ochrony danych należy także dokonywać w przypadkach, w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych środków bezpieczeństwa (Motyw 91 preambuły).

10. Dotychczasowe doświadczenia GIODO dotyczące stosowania biometrii

Inspektorzy Biura GIODO kilkakrotnie w czasie czynności kontrolnych spotykali się już z koniecznością oceny stosowanych przez podmioty sektora publicznego i prywatnego technologiami przetwarzania danych biometrycznych. Były to systemy wykorzystujące odciski linii papilarnych palca, obraz układu żył krwionośnych palca oraz obraz tęczówki oka. Przykładowe wyniki przeprowadzonych kontroli zestawiono w tabeli 3.

Przeprowadzone kontrole wskazują, na wiele przypadków, w których dane biometryczne przetwarzane są bez posiadania przez administratora stosownej podstawy prawnej. W 4 przypadkach administratorzy przetwarzali dane biometryczne w przekonaniu, że podstawą prawną legalizującą ich przetwarzanie jest zgoda uzyskana od pracowników, których dane dotyczą. Zgoda taka, z uwagi na relacje występujące między pracownikiem i pracodawcą, nie może być jednak uznana za wyrażoną dobrowolnie, i nie może być w związku z tym uznana za przesłankę legalizującą przetwarzanie danych biometrycznych.

We wszystkich przypadkach natomiast, gdzie celem przetwarzania danych osobowych było zastosowanie adekwatnych do istniejących zagrożeń środków bezpieczeństwa i zapewnienia w związku z tym ścisłej i niezawodnej kontroli tożsamości osób uprawnionych do wejścia do określonych pomieszczeń lub udzielenia dostępu do systemu informatycznego, GIODO uznał nie tylko za uzasadnione przepisem art. 23 ust. 1 pkt 5 UODO, ale również jako uzasadnione

obowiązkiem zapewnienia odpowiedniego poziomu bezpieczeństwa wynikającego z art. 36 ust. 1 UODO.

Rodzaj biometrii	Administrator danych	Cel przetwarzania	Podstawa prawna	Ocena zgodności
Odcisk linii papilarnych	Komenda Główna Policji	Identyfikacja osób podejrzanych i ocena ich udziału w przestępstwach	Przepis prawa art. 20 ust. 2 pkt 2 ustawy o policji	Brak zastrzeżeń
Odcisk linii papilarnych	Urzędy wojewódzkie, konsulaty	Wydawanie dokumentów identyfikacyjnych (paszportów)	Przepis prawa art. 18 ust. 1 pkt 11 ustawy o dokumentach paszportowych	Brak zastrzeżeń
Odciski linii papilarnych	Podmioty publiczne i prywatne	Kontrola wejścia osób zatrudnionych oraz rozliczanie czasu pracy	Brak podstawy prawnej. Nieważność uzyskanej zgody	Wydano decyzje nakazujące zaprzestanie przetwarzania (4 przypadki)
Odciski linii papilarnych	Podmiot prywatny	Kontrola dostępu i rozliczanie wykupionych usług	Brak podstawy prawnej. Brak zgody	Wydano decyzję usunięcia wad (1 przypadek)
Odciski linii papilarnych	Podmiot prywatny	Kontrola dostępu i rozliczanie wykupionych usług	Brak podstawy prawnej. Nieprawidłowo pozyskana zgody	Wydano decyzję usunięcia wad prawnych (1 przypadek)
Tęczówka oka	Podmioty prywatne (bank)	Kontrola dostępu do określonych stref bezpieczeństwa i usług	Przepis prawa art. 36 ust. 1 UODO	Brak zastrzeżeń (1 przypadek)
Układ żył krwionośnych palca	Podmioty prywatne (bank)	Kontrola dostępu do określonych stref bezpieczeństwa i usług	Przepis prawa art. 36 ust. 1 UODO	Brak zastrzeżeń (1 przypadek)

Tabela 3. Zestawienie przykładowych wyników przeprowadzonych kontroli, w zakresie przetwarzania danych biometrycznych.

We wszystkich przypadkach natomiast, gdzie celem przetwarzania danych osobowych było zastosowanie adekwatnych do istniejących zagrożeń środków bezpieczeństwa i zapewnienia w związku z tym ścisłej i niezawodnej kontroli tożsamości osób uprawnionych do wejścia do

określonych pomieszczeń lub udzielenia dostępu do systemu informatycznego, GODO uznał nie tylko za uzasadnione przepisem art. 23 ust. 1 pkt 5 UODO, ale również jako uzasadnione obowiązkiem zapewnienia odpowiedniego poziomu bezpieczeństwa wynikającego z art. 36 ust. 1 UODO.

11. Wnioski

Niewątpliwie obecnie coraz częściej i chętniej stosuje się nowoczesne systemy wykorzystujące dane biometryczne w celu identyfikacji osób. Jednocześnie jednak wykorzystywanie danych biometrycznych wywołuje i będzie również w najbliższych latach wywoływać dyskusję na temat zachowania równowagi pomiędzy wdrażaniem coraz nowocześniejszych technologii wykorzystujących dane biometryczne a prawem obywateli do prywatności zapisanym w Konstytucji RP.

Podwyższenie poziomu bezpieczeństwa dla niektórych systemów biometrycznych jest tą ich zaletą, która sprawia, że są one coraz częściej wprowadzane do zabezpieczenia bardzo ważnych dokumentów oraz kontroli dostępu do ściśle strzeżonych miejsc lub systemów informatycznych. Dostrzegły to zarazem podmioty prywatne, jak i publiczne. Od 2009 r. obywatele RP zostali wyposażeni w nowe paszporty biometryczne, tj. paszporty z wbudowaną kartą pamięci elektronicznej, w której zapisano zdjęcie biometryczne i wzorce cyfrowe linii papilarnych palców. Również w obecnych dowodach osobistych od 1 marca 2015 r. umieszczane są zdjęcia biometryczne. Z nowych technologii korzysta coraz śmielej również sektor prywatny. Prekursorem zmian jest przede wszystkim sektor bankowy. Wprowadza on do użytku nowe bankomaty wyposażone w technologię Finger Vein czy wykorzystuje dane biometryczne w dostępie klientów do skrytek bankowych.

Zastosowanie dowodu w postaci identyfikacji biometrycznej lub identyfikacji fotograficznej jest wymagane ponadto w procesach sprawdzania i weryfikacji tożsamości osób fizycznych podczas wydawania środków do identyfikacji elektronicznych oraz świadczenia usług identyfikacji elektronicznej, o których mowa w rozporządzeniu eIDAS⁸, dla których wymagany jest wysoki poziom bezpieczeństwa.

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

Dla uzyskania takiego poziomu, zgodnie z Rozporządzeniem Wykonawczym Komisji (EU) 2015/1502⁹ z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa, wymagany jest czynnik uwierzytelnienia na podstawie cech przyrodzonych, tj. czynnik, który opiera się na rzeczywistym atrybucie osoby fizycznej, w którego przypadku od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania, że tę cechę fizyczną posiada. Środkiem takim, jak wskazano w ww. rozporządzeniu 2015/1502, może być fotografia lub identyfikator biometryczny.

Z drugiej strony należy pamiętać, iż szerokie stosowanie biometrii w naszym życiu niesie wiele zagrożeń. Dana biometryczna, za pomocą której jesteśmy identyfikowani, nigdy się nie zmieni. Nie ma możliwości wymiany np. układu żył krwionośnych palca, w związku z czym już zawsze na jego podstawie możemy zostać zidentyfikowani. Innymi słowy, ceną za korzystanie z danych biometrycznych będzie częściowa utrata anonimowości wyrażająca się tym, że dane te będą przechowywane w systemach komputerowych administratora danych.

Z dotychczasowych doświadczeń GODO wynikających z przeprowadzonych kontroli zgodności przetwarzania danych biometrycznych z przepisami prawa wynika, że nie zawsze przetwarzanie danych biometrycznych znajdowało właściwe uzasadnienie. Wyniki przeprowadzonych kontroli wyraźnie wskazywały na brak podstaw prawnych lub niewłaściwe ich stosowanie. Wydawane przez GODO decyzje nakazujące zaprzestanie przetwarzania danych biometrycznych lub usunięcie związanych z ich przetwarzaniem uchybień nie wynikały ze złej woli czy niechęci GODO do przetwarzania danych biometrycznych, jak często donosi prasa¹⁰, lecz obiektywnej oceny zgodności z obowiązującymi obecnie przepisami prawa i nałożonego na GODO w art. 12 ust.1 i 2 UODO obowiązku jego egzekwowania.

Wskazane wyżej zagrożenia i zalety związane z przetwarzaniem danych biometrycznych oraz różnorodność możliwych do stosowania metod i sposobów rozwiązań wymagają, aby każdy projekt przetwarzania danych biometrycznych poddawany był analizie potencjalnego wpływu danego rozwiązania na prywatność. W określonych zastosowaniach bowiem, mając na uwadze charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub

⁹ Rozporządzenie Wykonawcze Komisji (EU) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

¹⁰ Marta Gadomska, Czy pracodawcy zeskanują linie papilarne zatrudnionych, Tygodnik Gazeta Prawna 21-23 kwietnia 2017 TGP nr 16(71)DGP nr 78 (4477)

wolności osób fizycznych, przeważać mogą wskazane wyżej zalety lub zagrożenia związane w wykorzystaniem danych biometrycznych.

Mając na uwadze wymienione w rozdziałach 5 i 6 zagrożenia oraz zalety technologii wykorzystujących biometrię, budowa każdego systemu przetwarzania danych biometrycznych powinna być poprzedzona przeprowadzeniem oceny skutków dla ochrony danych, o której mowa w art. 35 RODO, a ostateczna decyzja o jego budowie uwzględniać podstawowe zasady ochrony danych osobowych, takie jak niezbędność, celowość oraz proporcjonalność.

Duże wyzwanie w odniesieniu do przetwarzania danych biometrycznych w administracji i usługach publicznych jest również w najbliższej przyszłości dla ustawodawcy zarówno krajowego, jak i unijnego. W przypadku bowiem, jeśli tworzony jest przepis prawa, który będzie zezwalał na przetwarzanie danych biometrycznych i zastosowanie określonych rozwiązań, wówczas zgodnie z art. 36 ust. 10 RODO, ocena skutków dla ochrony danych powinna być przeprowadzona na etapie tworzenia przepisu. W przeciwnym razie określone w przepisie prawa procesy przetwarzania i przeprowadzona, przez podmiot zobowiązany do ich stosowania ocena skutków dla ochrony danych, mogą prowadzić do sytuacji konfliktowych. Może się np. okazać, że zastosowanie wskazanego w przepisie prawa projektu nie można zrealizować i wprowadzić do stosowania z uwagi na wysokie ryzyko naruszenia prywatności jakie zostanie oszacowane na etapie oceny jego skutków na ochronę danych.

Stosownie do potrzeb, w systemach przetwarzania danych biometrycznych powinny być ściśle przestrzegane zasady dotyczące uwzględnienia ochrony danych na etapie projektowania, stosowanie zasady domyślnej prywatności oraz retencji danych. W odniesieniu do rozwiązań opartych na biometrii w kontaktach obywateli z instytucjami publicznymi i prywatnymi dotyczy to w szczególności rozwiązań monitoringu wizyjnego wykorzystującego zaawansowane systemy przetwarzania obrazu oraz systemy kontroli i sterowania, takie jak np. systemy odcinkowej kontroli prędkości, systemy sterowania i rozliczeń parkingowych itp.

Biorąc pod uwagę fakt, że przy szacowaniu oceny skutków dla ochrony prywatności administrator danych powinien uwzględniać bardzo wiele czynników, w tym proporcjonalność skutków stosowania danej technologii w stosunku do celów, jakim ma służyć, akceptowalność społeczną pobierania danego rodzaju próbek biometrycznych, wagę i znaczenie zabezpieczanych informacji oraz kontekst, w jakim dana technologia będzie stosowana, każdy z przypadków powinien być analizowany i oceniany indywidualnie. Ponadto mając na uwadze różne interesy administratora danych, jako podmiotu decydującego o zastosowaniu danej technologii biometrycznej z jednej strony i interesy (obawy) osób, których dane będą

przetwarzane z drugiej strony, skład zespołu przeprowadzającego ocenę wpływu danego rozwiązania biometrycznego na prywatność powinien być interdyscyplinarny. W jego skład, zgodnie z rekomendacjami z badań zleconych przez Komisję Europejską w zakresie przeprowadzania oceny skutków dla ochrony prywatności¹¹, powinny być włączone osoby, które reprezentowałyby również interesy podmiotów danych.

Reasumując, biometria na dobre zdomowiała się w naszym życiu. Jednak z uwagi na fakt, iż dane biometryczne poprzez swoją immamentną cechę, tj. „niezmienność”, stanowią szczególny typ danych osobowych, pod znakiem zapytania stoi propagowanie sposobu uwierzytelniania tożsamości osób opartego na biometrii, w szczególności, jeśli istnieją alternatywne, mniej „inwazyjne” metody weryfikacji tożsamości osób.

Mając na uwadze wymienione w rozdziale 5-tym zagrożenia związane z przetwarzaniem danych biometrycznych oraz ograniczenia wprowadzone w RODO, ich stosowanie powinno być ograniczane do sytuacji, gdzie jest to niezbędne. Do przypadków takich można zaliczyć między innymi:

1. Wydawanie środków identyfikacji elektronicznej, dla których rozporządzenie eIDAS UE Nr 910/2014 wymaga zapewnienia wysokiego poziomu bezpieczeństwa, w tym potwierdzenia tożsamości osoby poprzez dowody identyfikacji fotograficznej lub biometrycznej (Rozporządzenie Wykonawcze Komisji (UE) 2015/1502;
2. Wydawanie dokumentów podróży (paszportów) i dokumentów tożsamości;
3. Dostępu do ściśle strzeżonych pomieszczeń (systemów) wymagających wysokiego poziomu bezpieczeństwa, w tym potwierdzenia tożsamości osoby poprzez dowody identyfikacji fotograficznej lub biometrycznej.

Przy czym w odniesieniu do punktu 3 tj. przypadków, gdzie podstawą prawną przetwarzania danych biometrycznych nie jest wprost przepis prawa, ich użycie musi być zgodne z ogólnie obowiązującymi przepisami prawa. Inna będzie w związku z tym sytuacja dla podmiotów reprezentujących organy władzy publicznej, które zobowiązane są do działania na podstawie i w granicach prawa i w związku z tym dane biometryczne mogą przetwarzać tylko wówczas gdy zezwala na to wprost przepis prawa i inna dla podmiotów prywatnych, dla których obowiązują obecnie ogólne zasady określone w przepisach UODO a w przyszłości będą obowiązywać przepisy RODO. W każdym jednak przypadku, mając na uwadze wymienione w

¹¹ Paul De Hert, Dariusz Kloza, David Wright, A Privacy Impact Assessment Framework for data protection and privacy rights, Deliverables D3 „Recommendations for a privacy impact assessment framework for the European Union”

rozdziale 5 zagrożenia przetwarzanie danych biometrycznych podjęcie decyzji w tym zakresie powinno być poprzedzone wykonaniem oceną skutków projektowanego rozwiązania dla ochrony danych. Zgodnie z przepisem art. 35 ust. 10 RODO ocena taka nie będzie wymagana jedynie w przypadkach jeśli przetwarzanie danych biometrycznych wymagane jest przez przepis prawa lub przetwarzanie tych danych jest nie zbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, a ocena skutków dla ochrony danych została przeprowadzona w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej.

W przeprowadzanej ocenie skutków dla ochrony danych osobowych, z uwagi na wymienione w rozdziale 5 zagrożenia i specyfikę danych biometrycznych należy rozważyć, czy przetwarzanie danych biometrycznych dla realizacji określonego celu jest rzeczywiście niezbędne, tj. związana z tym ingerencja w prywatność osoby fizycznej jest adekwatna i proporcjonalna do celu, w jakim dane te będą przetwarzane. Dotyczy to również sytuacji, w których podstawą przetwarzania danych biometrycznych jest dobrowolnie wyrażona zgoda osoby, której dane są przetwarzane.

W każdym przypadku przetwarzanie danych biometrycznych zobowiązuje administratora przetwarzanych danych do zachowania odpowiednich środków bezpieczeństwa.