GRUPA ROBOCZA ART. 29

00720/12/PL
WP193

Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych

przyjęta w dniu 27 kwietnia 2012 r.

Streszczenie

Systemy biometryczne są ściśle związane z daną osobą, ponieważ dzięki nim możliwe jest wykorzystanie określonej niepowtarzalnej cechy danej osoby fizycznej do celów identyfikacji lub uwierzytelnienia. O ile dane biometryczne danej osoby można usunąć lub zmienić, to jednak źródła, z którego pochodzą, nie da się zasadniczo ani zmienić, ani usunąć.

Dane biometryczne stosuje się z powodzeniem i skutecznie w badaniach naukowych oraz stosuje się je jako kluczowy element w dziedzinie kryminalistyki i wartościowy element systemów kontroli dostępu. Mogą one przyczynić się do podniesienia poziomu bezpieczeństwa oraz sprawić, że przeprowadzanie procedur identyfikacji i uwierzytelnienia stanie się prostsze, szybsze i wygodniejsze. W przeszłości korzystanie z tej technologii było kosztowne i z racji tych barier ekonomicznych wpływ na prawa osób fizycznych do ochrony danych był ograniczony. W ostatnich latach sytuacja ta uległa zdecydowanej zmianie. Przeprowadzenie analizy DNA stało się szybsze i może sobie na nie pozwolić prawie każdy. Dzięki postępowi technologicznemu przechowywanie danych i moc obliczeniowa stały się tańsze; zmiana ta umożliwiła tworzenie internetowych albumów z fotografiami i portali społecznościowych, na których można zamieszczać miliardy fotografii. Czytniki linii papilarnych i urządzenia do nadzoru wideo stały się niedrogimi gadżetami. Dzięki rozwojowi tych technologii przeprowadzanie wielu operacji stało się wygodniejsze, rozwiązano wiele spraw dotyczących przestępstw i zwiększono wiarygodność systemów kontroli dostępu, jednakże wraz z rozwojem tych technologii pojawiły się również nowe zagrożenia dla praw podstawowych. Prawdziwym problemem stała się dyskryminacja genetyczna. Kradzież tożsamości przestała już być zagrożeniem teoretycznym.

O ile inne nowe technologie ukierunkowane na duże populacje i wzbudzające ostatnio obawy w zakresie ochrony danych niekoniecznie skupione są na ustanowieniu bezpośredniego związku z konkretną osobą fizyczną lub ustanowienie takiego związku wymagałoby znacznych wysiłków, dane biometryczne z samej swojej natury bezpośrednio wiążą się z konkretną osobą fizyczną. Taki związek nie zawsze stanowi atut, ma on także szereg wad. Przykładowo wyposażanie systemów nadzoru wideo i smartfonów w systemy rozpoznawania twarzy oparte na bazach danych portali społecznościowych mogłoby położyć kres anonimowości i niemonitorowanemu przemieszczaniu się osób fizycznych. Z drugiej strony czytniki linii papilarnych, czytniki układu żył lub zwykły uśmiech do kamery mogą zastąpić karty, kody, hasła i podpisy.

Niniejsza opinia dotyczy tych oraz innych niedawnych zmian sytuacji i ma na celu zwiększenie świadomości wśród zainteresowanych osób oraz organów ustawodawczych. Jeżeli nie zostaną wdrożone żadne odpowiednie zabezpieczenia, stosowanie omawianych innowacji technicznych, które bardzo często przedstawia się jako technologie jedynie zwiększające zadowolenie użytkownika i wygodę korzystania z aplikacji, może doprowadzić do stopniowej utraty prywatności. W związku z tym w niniejszej opinii określa się środki techniczne i organizacyjne mające na celu ograniczenie czynników ryzyka dla ochrony danych i prywatności oraz mogące przyczynić się do uniknięcia negatywnego wpływu na prywatność obywateli europejskich i na ich podstawowe prawo do ochrony danych.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i art. 30 ust. 1 lit. a) i ust. 3 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. Zakres niniejszej opinii

W dokumencie roboczym dotyczącym biometrii z 2003 r. (WP80) Grupa Robocza Art. 29 (grupa robocza) zbadała kwestie dotyczące ochrony danych związane ze stosowaniem nowych technologii umożliwiających elektroniczne odczytanie i przetworzenie danych biometrycznych. W kolejnych latach na szeroką skalę wdrożono tę technologię zarówno w sektorze publicznym, jak i prywatnym oraz opracowano szereg zyskujących na znaczeniu usług. Technologie biometryczne, które kiedyś wymagały znacznych zasobów finansowych i obliczeniowych, stały się nieporównywalnie tańsze i szybsze. Obecnie stosowanie czytników linii papilarnych jest powszechną praktyką. Przykładowo niektóre laptopy posiadają czytnik linii papilarnych do biometrycznej kontroli dostępu. Postępy w dziedzinie analizy DNA oznaczają, że obecnie wyniki takiej analizy uzyskuje się już po kilku minutach. Niektóre z nowo opracowanych technologii, takie jak rozpoznawanie układu żył lub rozpoznawanie twarzy, zostały już w pełni dopracowane. Ich stosowanie w różnych miejscach naszego codziennego życia jest na wyciągnięcie ręki. Technologie biometryczne są ściśle związane z określonymi cechami osób fizycznych i niektóre z nich można wykorzystywać do ujawniania danych szczególnie chronionych. Ponadto wiele z nich umożliwia automatyczne śledzenie, namierzanie lub ustalanie profilu osób, co sprawia, że ich potencjalny wpływ na prywatność osób fizycznych i ich prawo do ochrony danych jest duży. Wpływ ten zwiększa się wraz z rosnącym rozpowszechnieniem wspomnianych technologii. W odniesieniu do każdej osoby fizycznej istnieje prawdopodobieństwo, że zostanie zarejestrowana w co najmniej jednym systemie biometrycznym.

Celem niniejszej opinii jest zapewnienie zmienionych i zaktualizowanych ram ujednoliconych ogólnych wytycznych i zaleceń w sprawie wdrażania zasad prywatności i ochrony danych w zakresie zastosowań danych biometrycznych. Niniejsza opinia jest skierowana do europejskich i krajowych organów ustawodawczych, do branży systemów biometrycznych i do użytkowników takich technologii.

2. Definicje

Technologie biometryczne nie stanowią nowości i były już przedmiotem różnych opinii grupy roboczej. Niniejsza część ma służyć zebraniu odpowiednich definicji i w razie potrzeby zapewnienie aktualizacji.

Dane biometryczne: jak już wskazano w opinii grupy roboczej 4/2007 (WP136), dane biometryczne można zdefiniować następująco:

„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".

Dane biometryczne bezpowrotnie zmieniają związek między ciałem a tożsamością, ponieważ dzięki nim cechy ciała ludzkiego można automatycznie odczytywać i podlegają one dalszemu wykorzystaniu.

Dane biometryczne można przechowywać i przetwarzać w różnych formach. Niekiedy informacje biometryczne pobrane od danej osoby przechowuje się i przetwarza w formie nieprzetworzonej umożliwiającej rozpoznanie źródła, z którego pochodzą, bez konieczności posiadania specjalistycznej wiedzy, na przykład informacje te mogą mieć formę fotografii twarzy, fotografii odcisku palca lub nagrania głosowego. W niektórych innych przypadkach pobrane nieprzetworzone informacje biometryczne zostają przetworzone tak, że jedynie niektóre cechy lub identyfikatory biometryczne zostają wyodrębnione i zachowane jako wzorzec biometryczny.

Źródło danych biometrycznych: istnieje wiele różnych źródeł danych biometrycznych – mogą obejmować one fizyczne, fizjologiczne, behawioralne lub psychologiczne cechy danej osoby fizycznej. Zgodnie z opinią 4/2007 (WP136):

„źródeł danych biometrycznych (np. próbek tkanek ludzkich) nie można uznać za dane biometryczne same w sobie, lecz mogą być wykorzystane do gromadzenia danych biometrycznych (w drodze wyodrębnienia z nich informacji)".

Jak stwierdzono w dokumencie WP80, istnieją dwie główne kategorie technik biometrycznych:

- po pierwsze, istnieją techniki fizyczne i **fizjologiczne**, w ramach których mierzy się fizyczne i fizjologiczne cechy danej osoby, takie jak: sprawdzanie zgodności linii papilarnych, analiza obrazu palca, rozpoznawanie tęczówki, analiza siatkówki, rozpoznawanie twarzy, analiza kształtu dłoni, rozpoznawanie kształtu ucha, wykrywanie zapachu ciała, rozpoznawanie głosu, analiza wzoru DNA, analiza położenia porów itp.;
- po drugie, istnieją techniki **behawioralne**, przy pomocy których mierzy się zachowanie danej osoby i które obejmują sprawdzanie podpisu odręcznego, analizę dynamiki pisania na klawiaturze, analizę chodu, sposób chodzenia lub poruszania się, wzory wskazujące na myślenie podświadome, takie jak kłamanie itp.

Należy również wziąć pod uwagę pojawiające techniki mające podstawy **psychologiczne**. Obejmują one pomiar reakcji na konkretne sytuacje lub testy w celu dopasowania do danego profilu psychologicznego.

Wzorzec biometryczny: z danych biometrycznych w formie nieprzetworzonej można wyodrębnić kluczowe identyfikatory biometryczne (np. wymiary twarzy z fotografii), które można przechowywać do celów późniejszego przetworzenia zamiast samych danych nieprzetworzonych. Na podstawie takich cech tworzy się wzorzec biometrycznych danych. Zasadniczą kwestią jest określenie wielkości (ilości informacji) wzorca. Z jednej strony

wzorzec powinien być wystarczająco szeroki, aby zapewnić bezpieczeństwo (aby nie dochodziło do pokrywania się różnych danych biometrycznych lub zastępowania tożsamości), z drugiej strony, wzorzec nie powinien być zbyt duży tak, aby uniknąć ryzyka odtworzenia danych biometrycznych. Tworzenie wzorca powinno być procesem jednokierunkowym tak, aby a jego podstawie nie można było odtworzyć nieprzetworzonych danych biometrycznych.

Systemy biometryczne: zgodnie z dokumentem WP80 systemy biometryczne są to:

> „aplikacje wykorzystujące technologie biometryczne, które umożliwiają automatyczną identyfikację lub uwierzytelnienie/weryfikację danej osoby. Aplikacje służące do uwierzytelnienia/weryfikacji często są stosowane do różnych zadań w zupełnie różnych obszarach, do różnych celów i w ramach odpowiedzialności szerokiego grona różnych podmiotów".

Dzięki ostatnim osiągnięciom technologicznym systemy biometryczne można obecnie stosować również do celów kategoryzacji/segregacji.

Ryzyko związane z systemami biometrycznymi wynika z charakteru przetwarzanych danych biometrycznych. W związku z tym zgodnie z ogólniejszą definicją system biometryczny oznaczałby system, w ramach którego dane biometryczne są wyodrębniane i poddawane dalszemu przetworzeniu.

Przetwarzanie danych biometrycznych w systemie biometrycznym zwykle obejmuje różne procesy, takie jak rejestracja, przechowywanie i kojarzenie:

- rejestracja danych biometrycznych: obejmuje 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.

Zwykle faza rejestracji stanowi pierwszy kontakt osoby fizycznej z konkretnym systemem biometrycznym. W większości przypadków rejestracja wymaga osobistego uczestnictwa danej osoby fizycznej (np. w przypadku pobierania odcisków palców), a zatem etap ten może stanowić odpowiednią okazję przekazania informacji i rzetelnego powiadomienia o przetwarzaniu. Możliwe jest jednak również rejestrowanie osób fizycznych bez ich wiedzy i zgody (np. w przypadku systemów CCTV z wbudowaną funkcją rozpoznawania twarzy). Dokładność i bezpieczeństwo procesu rejestracji ma zasadnicze znaczenie dla skuteczności całego systemu. Osoba fizyczna może mieć możliwość ponownej rejestracji w systemie biometrycznym w celu dokonania aktualizacji zapisanych danych biometrycznych;

- przechowywanie danych biometrycznych: dane uzyskane w czasie rejestracji można przechowywać lokalnie w centrum operacyjnym, w którym dokonano rejestracji (na przykład w czytniku), w celu późniejszego wykorzystania lub w urządzeniu noszonym przez osobę fizyczną (na przykład na karcie elektronicznej), lub dane te można przesyłać i przechowywać w scentralizowanej bazie danych dostępnej dla co najmniej jednego systemu biometrycznego;

- **kojarzenie danych biometrycznych:** jest to proces porównywania danych biometrycznych/wzorca biometrycznego (pobranych w trakcie rejestracji) z danymi biometrycznymi/wzorcem biometrycznym pobranymi z nowej próbki do celów identyfikacji, weryfikacji/uwierzytelnienia lub kategoryzacji.

Identyfikacja biometryczna: identyfikacja osoby fizycznej w systemie biometrycznym stanowi zwykle proces polegający na porównaniu danych biometrycznych danej osoby fizycznej (uzyskanych w czasie identyfikacji) z szeregiem wzorców biometrycznych przechowywanych w bazie danych (tj. proces kojarzenia „jeden do wielu").

Weryfikacja biometryczna/uwierzytelnienie biometryczne: weryfikacja osoby fizycznej w systemie biometrycznym stanowi zwykle proces polegający na porównaniu danych biometrycznych danej osoby fizycznej (uzyskanych w czasie weryfikacji) z pojedynczym wzorcem biometrycznym przechowywanych w urządzeniu (tj. proces kojarzenia „jeden do jednego").

Kategoryzacja/segregacja biometryczna: kategoryzacja/segregacja osób fizycznych w systemie biometrycznym stanowi zwykle proces polegający na określeniu, czy dane biometryczne danej osoby fizycznej należą do grupy o wcześniej ustalonych cechach, służący podjęciu określonego działania. W tym przypadku nie jest istotna identyfikacja lub weryfikacja danej osoby fizycznej, lecz istotne jest automatyczne przyporządkowanie jej do określonej kategorii. Przykładowo w okienku reklamowym mogą pojawiać się różne reklamy w zależności osoby fizycznej, która na nie patrzy, uwzględniając jej wiek lub płeć.

Biometria multimodalna: biometrię mulimodalną można zdefiniować jako połączenie różnych technologii biometrycznych w celu zwiększenia dokładności lub skuteczności systemu (ten rodzaj biometrii zwany jest również biometrią wielopoziomową). W systemach biometrycznych w procesie kojarzenia wykorzystuje się co najmniej dwie cechy/modalności biometryczne tej samej osoby fizycznej. Systemy takie mogą działać na różne sposoby – poprzez gromadzenie różnych danych biometrycznych za pomocą różnych czujników albo poprzez gromadzenie wielu jednostek tego samego identyfikatora biometrycznego. W niektórych badaniach do tej kategorii zalicza się również systemy działające na zasadzie wykonywania wielu odczytów tego samego identyfikatora biometrycznego lub systemy, w których do celów wyodrębnienia identyfikatorów biometrycznych stosuje się wiele algorytmów do tej samej próbki biometrycznej. Przykładem multimodalnych systemów biometrycznych jest paszport biometryczny na szczeblu UE oraz system US-VISIT Biometric Identification Services w Stanach Zjednoczonych.

Dokładność: przy stosowaniu systemów biometrycznych trudno uzyskać wyniki w 100% niezawierające żadnych błędów. Może to wynikać z różnic dotyczących otoczenia przy pozyskiwaniu danych (oświetlenia, temperatury itp.) i różnic dotyczących zastosowanego sprzętu (kamer, urządzeń skanujących itp.). Do najczęściej stosowanych sposobów pomiaru oceny skuteczności należy wskaźnik fałszywej akceptacji i wskaźnik fałszywego odrzucenia, które można dostosować do stosowanego systemu:

- wskaźnik błędnych akceptacji (ang. *False Accept Rate – FAR*): istnieje prawdopodobieństwo, że system biometryczny nieprawidłowo zidentyfikuje daną osobę fizyczna lub nie odrzuci oszusta. Wskaźnik pozwala na pomiar procentu nieważnych wpisów, które są nieprawidłowo zaakceptowane. Jest on również znany jako wskaźnik wyników fałszywie dodatnich;

- 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. Parametr ten znany jest również jako wskaźnik wyników fałszywie ujemnych.

Dokonując prawidłowej kalibracji systemu i dostosowania ustawień, można zminimalizować błędy krytyczne systemu biometrycznego do poziomu dozwolonego do celów stosowania operacyjnego poprzez zmniejszenie ryzyka nieprawidłowej oceny. W systemie doskonałym wartość wskaźników FAR i FRR wyniosłaby zero, ale częściej wykazują one korelację negatywną. Wzrost wskaźnika FAR często powoduje spadek poziomu wskaźnika FRR.

Oceniając, czy dokładność danego systemu biometrycznego jest dopuszczalna, ważne jest, aby dokonać oceny celu przetwarzania, wskaźników FAR i FRR oraz wielkości populacji. Ponadto, oceniając dokładność danego systemu biometrycznego, można również uwzględnić zdolność do wykrycia próbki żywej. Przykładowo ślady linii papilarnych palca można skopiować i wykorzystać do stworzenia fałszywych odcisków palców. W takiej sytuacji nie może istnieć możliwość oszukania czytnika linii papilarnych tak, aby dokonał pozytywnej identyfikacji.

3. Analiza prawna

Właściwe ramy prawne stanowi dyrektywa o ochronie danych (95/46/WE). Już w dokumencie WP80 grupa robocza stwierdziła, że w większości przypadków dane biometryczne stanowią dane osobowe. Dane te można zatem 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.

Cel

Wymogiem wstępnym korzystania z danych biometrycznych jest wyraźne określenie celu, w którym takie dane biometryczne są gromadzone i przetwarzane, z uwzględnieniem czynników ryzyka dla ochrony podstawowych praw i wolności osób fizycznych.

Przykładowo dane biometryczne można gromadzić w celu zapewnienia lub zwiększenia bezpieczeństwa systemów przetwarzania danych poprzez wdrożenie odpowiednich środków ochrony danych osobowych przed nieuprawnionym dostępem. Zasadniczo nie ma żadnych przeszkód dla wdrożenia odpowiednich środków bezpieczeństwa opartych na identyfikatorach biometrycznych osoby odpowiadającej za przetwarzanie w celu zapewnienia poziomu bezpieczeństwa odpowiadającego czynnikom ryzyka związanym z przetwarzaniem i charakterowi chronionych danych osobowych. Należy jednak pamiętać, że stosowanie danych biometrycznych samo przez się nie zapewnia większego bezpieczeństwa, gdyż wiele danych biometrycznych można gromadzić bez wiedzy zainteresowanej osoby. Im wyższy przewidziany poziom bezpieczeństwa, tym mniej samych danych biometrycznych będzie można zastosować w tym celu.

Zasady celowości należy przestrzegać wraz z innymi zasadami w zakresie ochrony danych, w szczególności przy określaniu różnych celów danej aplikacji należy pamiętać o zasadzie proporcjonalności, konieczności i minimalizacji danych. W miarę możliwości osoba, której dane dotyczą, musi mieć wybór pomiędzy szeregiem celów aplikacji posiadającej wiele

funkcji, w szczególności, jeżeli co najmniej jeden z nich wymaga przetwarzania danych biometrycznych.

Przykład:
Zalecono stosowanie urządzeń elektronicznych zapewniających szczególne procedury uwierzytelniania oparte na danych biometrycznych w związku ze środkami bezpieczeństwa podejmowanymi w następujących przypadkach:
- przetwarzania danych osobowych gromadzonych przez operatorów telefonicznych w ramach prowadzenia podsłuchu, na który zezwolenie wydał sąd;
- dostępu do danych o ruchu (i danych dotyczących lokalizacji) zatrzymywanych do celów sądowych przez dostawców publicznie dostępnych usług łączności elektronicznej lub dostawców publicznej sieci łączności oraz dostępu do odpowiednich pomieszczeń, w których takie dane są przetwarzane;
- gromadzenia i przechowywania danych genetycznych i próbek biologicznych.

Fotografie zamieszczane w internecie, mediach społecznościowych, internetowych aplikacjach służących do zarządzania fotografiami lub ich wymiany nie mogą być dalej przetwarzane w celu wyodrębnienia wzorców biometrycznych lub ich rejestracji w systemie biometrycznym do celów automatycznego rozpoznawania osób widocznych na tych fotografiach (rozpoznawanie twarzy) bez konkretnej podstawy prawnej (na przykład zgody) w odniesieniu do tego nowego celu. Jeżeli istnieje podstawa prawna dotycząca tego dodatkowego celu, przetwarzanie musi być również prawidłowe, odpowiednie oraz nienadmierne w stosunku tego celu. Jeżeli osoba, której dane dotyczą, udzieliła zgody na przetwarzanie fotografii, na których widnieje, w celu automatycznego oznaczania jej w internetowym albumie z fotografiami za pomocą algorytmu rozpoznawania twarzy, tego rodzaju przetwarzania należy dokonywać w sposób sprzyjający ochronie danych: należy usunąć dane biometryczne, które nie są już potrzebne po oznaczeniu obrazów nazwiskiem, przydomkiem lub jakimkolwiek innym tekstem określonym przez osobę, której dane dotyczą. Do tego celu tworzenie stałej bazy danych biometrycznych nie jest a priori konieczne.

Proporcjonalność

Z korzystaniem z danych biometrycznych wiąże się kwestia proporcjonalności każdej kategorii przetwarzanych danych w świetle celu, w którym przetwarza się dane. Ponieważ dane biometryczne można stosować tylko, jeżeli są one prawidłowe, odpowiednie oraz nienadmierne , oznacza to, że należy dokonać ścisłej oceny konieczności i proporcjonalności przetwarzanych danych oraz tego, czy zamierzony cel można osiągnąć w sposób w mniejszym stopniu ingerujący w prywatność.

Analizując proporcjonalność proponowanego systemu biometrycznego, należy rozważyć w pierwszym rzędzie kwestię, czy dany system jest konieczny dla spełnienia określonej potrzeby, tj. czy ma zasadnicze znaczenie dla spełnienia tej potrzeby, a nie jest tylko najdogodniejszy lub najbardziej opłacalny. Drugim czynnikiem, który należy rozważyć, jest prawdopodobieństwo skuteczności systemu pod względem spełnienia tej potrzeby z uwzględnieniem szczególnych cech technologii biometrycznej, którą planuje się zastosować[1].

[1] Dane biometryczne będą stosowane do celów weryfikacji lub identyfikacji: można uznać, że dany identyfikator biometryczny jest odpowiedni pod względem technicznym do jednego z tych celów, jednak nie do innego (np. technologie charakteryzujące się niskim wskaźnikiem błędnego odrzucenia powinny być

Trzecim aspektem, który należy rozważyć, jest to, czy utrata prywatności wynikająca z zastosowania systemu jest proporcjonalna do wszystkich przewidywanych korzyści. Jeżeli korzyść jest stosunkowo niewielka, np. zyskuje się większą wygodę lub nieznaczną oszczędność, utrata prywatności nie jest właściwa. Czwartym aspektem oceny adekwatności systemu biometrycznego jest rozważenie kwestii, czy pożądany cel można osiągnąć za pomocą środków w mniejszym stopniu ingerujących w prywatność[2].

Przykład:
W klubie fitness i odnowy biologicznej zostaje zainstalowany scentralizowany system biometryczny oparty na gromadzeniu odcisków palców w celu udzielania dostępu do pomieszczeń gimnastycznych i związanych z nimi usług jedynie klientom, którzy dokonali opłat.
Do obsługi takiego systemu konieczne byłoby przechowywanie odcisków palców wszystkich klientów i członków personelu. Taka aplikacja biometryczna wydaje się nieproporcjonalna w stosunku do potrzeby kontrolowania dostępu do klubu i ułatwienia zarządzania opłatami wpisowymi. Można przypuszczać, że równie praktyczne i skuteczne są inne środki, które nie wymają przetwarzania danych biometrycznych, takie jak zwykła lista kontrolna lub identyfikatory RFID, lub karta magnetyczna.

Grupa robocza ostrzega przed ryzykiem wiążącym się ze stosowaniem danych biometrycznych do celów identyfikacji w dużych scentralizowanych bazach danych ze względu na potencjalnie szkodliwe skutki dla zainteresowanych osób.

Należy uwzględnić znaczny wpływ tego rodzaju systemów na godność ludzką osób, których dane dotyczą, oraz ich skutki w zakresie praw podstawowych. W świetle europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz orzecznictwa Europejskiego Trybunału Praw Człowieka w sprawie art. 8 konwencji grupa robocza podkreśla, że na jakąkolwiek ingerencję w prawo do ochrony danych można zezwolić pod warunkiem, że jest ona zgodna z prawem i konieczna, w społeczeństwie demokratycznym, dla ochrony ważnego interesu publicznego[3].

Aby zapewnić przestrzegania tych warunków, konieczne jest określenie celu, który ma spełniać system, oraz dokonanie oceny proporcjonalności danych, które mają być wprowadzane do systemu w stosunku do tego celu.

W tym celu administrator danych musi ustalić, czy przetwarzanie i jego mechanizmy, kategorie gromadzonych i przetwarzanych danych oraz przekazywanie informacji zawartych w bazach danych są konieczne i niezbędne. Przyjęte środki bezpieczeństwa muszą być odpowiednie i skuteczne. Administrator danych musi uwzględnić prawa przyznawane osobom fizycznym, których dotyczą dane osobowe, oraz dopilnować, aby dana aplikacja zawierała odpowiedni mechanizm egzekwowania takich praw.

---

rozwiązaniem preferowanym w systemach opracowanych do stosowania do celów identyfikacji w dziedzinie ochrony porządku publicznego).

2 Przykładowo za pomocą kart elektronicznych lub innych metod, które nie wymagają gromadzenia lub centralizacji informacji biometrycznych do celów uwierzytelnienia.

3 Zob. wyrok Trybunału Sprawiedliwości z dnia 20 maja 2003 r., sprawy połączone C-465/00, C-138/01 i C-139/01 (Rechnungshof przeciwko Österreichischer Rundfunk i in.), wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 grudnia 2008 r., skargi nr 30562/04 i 30566/04 (S. i Marper przeciwko Zjednoczonemu Królestwu) oraz wyrok z dnia 19 lipca 2011 r., skargi nr 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 i 64027/09 (Goggins i in przeciwko Zjednoczonemu Królestwu).

Przykład:
Zastosowanie danych biometrycznych do celów identyfikacji. Systemy analizujące twarz danej osoby oraz systemy analizujące DNA danej osoby mogą bardzo skutecznie przyczynić się do walki z przestępczością i skutecznie ujawniać tożsamość nieznanej osoby podejrzanej o popełnienie poważnego przestępstwa. Stosowanie takich systemów na szeroką skalę prowadzi jednak do powstawania poważnych skutków ubocznych. W przypadku rozpoznawania twarzy, dzięki któremu dane można z łatwością pobrać bez wiedzy osoby, której dane dotyczą, rozpowszechnione stosowanie takiej technologii oznaczałoby koniec anonimowości w miejscach publicznych i umożliwiłoby stałe śledzenie osób fizycznych. W przypadku danych dotyczących DNA korzystanie z tej technologii wiąże się z ryzykiem ujawnienia danych szczególnie chronionych dotyczących zdrowia danej osoby.

Dokładność

Przetwarzane dane biometryczne muszą być dokładne i odpowiednie w stosunku do celu, w którym zostały zgromadzone. Dane muszą być dokładne przy rejestracji i w czasie ustanawiania związku między daną osobą a danymi biometrycznymi. Dokładność przy rejestracji ma również znaczenie dla zapobiegania oszustwom dotyczącym tożsamości.

Dane biometryczne są niepowtarzalne i większość z nich tworzy niepowtarzalny wzorzec lub obraz. Jeżeli dane biometryczne stosuje się na szeroką skalę, w szczególności w odniesieniu do znacznego odsetka ludności, można je uznać za identyfikator ogólnego stosowania w rozumieniu dyrektywy 95/46/WE. Do takich danych miałby zatem zastosowanie art. 8 ust. 7 dyrektywy 95/46/WE i państwa członkowskie musiałyby określić warunki ich przetwarzania.

Minimalizacja danych

Szczególna trudność może pojawiać się w związku z tym, że dane biometryczne zawierają często więcej informacji niż jest to konieczne do celów kojarzenia. Administrator danych musi egzekwować zasadę minimalizacji danych. Po pierwsze, oznacza to, że przetwarzać, przekazywać i przechowywać należy jedynie informacje wymagane, a nie wszystkie dostępne informacje. Po drugie, administrator danych powinien dopilnować, aby konfiguracja domyślna sprzyjała ochronie danych bez konieczności jej egzekwowania.

Okresy zatrzymywania

Administrator danych powinien określić okres zatrzymywania danych biometrycznych, który nie powinien być dłuższy, niż jest to konieczne do celów, do których dane zostały zgromadzone lub do których są poddawane dalszemu przetwarzaniu. Administrator danych musi zapewnić trwałe usunięcie danych lub profili uzyskanych na podstawie takich danych po upływie takiego uzasadnionego okresu.

Należy wyraźnie zaznaczyć różnicę między ogólnymi danymi osobowymi, które mogą być niezbędne przez dłuższy czas, a danymi biometrycznymi, które nie mają już zastosowania, na przykład gdy osoba, której dane dotyczą, nie ma już dostępu do konkretnego obszaru.

Przykład:
Pracownik obsługuje system biometryczny służący do kontroli dostępu do obszaru o ograniczonym dostępie. Funkcja danego pracownika nie wymaga już, aby posiadał on dostęp do obszaru o ograniczonym dostępie (np. wskutek zmiany zakresu jego odpowiedzialności lub pracy). W takim przypadku dane biometryczne takiego pracownika należy usunąć, ponieważ cel, w którym dane te zostały zgromadzone, przestał mieć zastosowanie.

3.1. Uzasadniona podstawa

Przetwarzanie danych biometrycznych musi być oparte na jednej z podstaw legalności przewidzianych w art. 7 dyrektywy 95/46/WE.

3.1.1. Zgoda, art. 7 lit. a)

Pierwszą taką podstawą legalności określoną w art. 7 lit. a) jest wyrażenie zgody na przetwarzanie przez osobę, której dane dotyczą. Zgodnie z art. 2 lit. h) dyrektywy o ochronie danych zgoda musi stanowić dobrowolne, konkretne i świadome wskazanie przez osobę, której dane dotyczą, jej woli. Należy wyraźnie stwierdzić, że takiej zgody nie można uzyskać w sposób dobrowolny poprzez obowiązkową akceptację ogólnych warunków lub poprzez zapewnienie możliwości rezygnacji. Ponadto musi istnieć możliwość cofnięcia udzielonej zgody. W tym względzie grupa robocza w swojej opinii dotyczącej definicji zgody podkreśla różne istotne aspekty tego pojęcia: ważność zgody, prawo osób fizycznych do cofnięcia udzielonej zgody, udzielanie zgody przed rozpoczęciem przetwarzania, wymogi dotyczące jakości i dostępności informacji[4].

W wielu przypadkach, w których dane biometryczne przetwarza się bez zapewnienia dopuszczalnego rozwiązania alternatywnego, takiego jak stosowanie hasła lub karty magnetycznej, nie można uznać, że zgoda została udzielona dobrowolnie. Przykładowo systemu zniechęcającego osoby, których dane dotyczą, do jego stosowania (np. poprzez nadmierny czas marnowany przez użytkownika lub złożoność systemu) nie można uznać za dopuszczalne rozwiązanie alternatywne, a zatem jego za stosowanie nie prowadzi do udzielenia ważnej zgody.

Przykłady:
W przypadku braku innych alternatywnych uzasadnionych podstaw zastosowanie biometrycznego systemu uwierzytelniania w celu kontroli dostępu do klubu wideo byłoby możliwe tylko, jeżeli klienci mogliby dobrowolnie podjąć decyzję w sprawie korzystania z tego systemu. Oznacza to, że właściciel klubu filmowego musi udostępnić alternatywne mechanizmy w mniejszym stopniu ingerujące w prywatność. W takim systemie klient, który nie chce lub nie może przejść pobierania odcisków palców ze względu na jego osobiste okoliczności, będzie mógł odmówić udzielenia zgody. Sam wybór między nieskorzystaniem z usługi a podaniem swoich danych biometrycznych stanowi wyraźny wskaźnik, że zgody nie udzielono dobrowolnie, i nie można go uznać za uzasadnioną podstawę.

W przedszkolu zostaje zainstalowany skaner układu żył w celu sprawdzenia, czy każda dorosła osoba wchodząca (rodzice i członkowie personelu) jest uprawniona do wejścia. Do obsługi takiego systemu niezbędne byłoby przechowywanie odcisków palców wszystkich rodziców i członków personelu. Udzielenie zgody stanowiłoby tutaj podważalną podstawę prawną szczególnie w przypadku pracowników, którzy w praktyce mogliby nie mieć możliwości odmówienia korzystania z tego systemu. Taka zgoda budziłaby wątpliwości

[4] WP 187, Opinia 15/2011 w sprawie definicji „zgody” .

również w przypadku rodziców, o ile nie zapewniono by alternatywnych metod wejścia do przedszkola.

Chociaż może istnieć silne domniemanie, iż zgoda jest niedostateczna ze względu na zwykły brak równowagi między pracodawcą a pracownikiem, grupa robocza nie wyklucza jej w zupełności „pod warunkiem, że istnieją wystarczające gwarancje, że zgoda jest faktycznie dobrowolna”[5].

W kontekście zatrudnienia zgodę należy zatem zweryfikować i należycie uzasadnić. Pracodawcy, zamiast dążyć do uzyskania zgody pracowników, mogliby zbadać, czy istnieje możliwa do wykazania konieczność stosowania danych biometrycznych pracowników w uzasadnionym celu i zestawić taką konieczność z podstawowymi prawami i wolnościami pracowników. W przypadkach, w których można odpowiednio uzasadnić taką konieczność, podstawę prawną takiego przetwarzania mógłby stanowić uzasadniony interes administratora danych określony w art. 7 lit. f) dyrektywy 95/46/WE. Pracodawca musi zawsze dążyć do zastosowania środków w jak najmniejszym stopniu integrujących w prywatność, wybierając w miarę możliwości proces, w ramach którego nie stosuje się danych biometrycznych.

Jak opisano w pkt 3.1.3, mogą jednak wystąpić przypadki, w których zastosowanie systemu biometrycznego może leżeć w uzasadnionym interesie administratora danych. W tych sytuacjach zgoda nie byłaby wymagana.

Zgoda jest ważna tylko w sytuacjach, w których udziela się wystarczających informacji o zastosowaniu danych biometrycznych. Ponieważ dane biometryczne można stosować jako niepowtarzalny i powszechny identyfikator, zapewnienie wyraźnych i łatwo dostępnych informacji dotyczących sposobu wykorzystania konkretnych danych należy uznać za bezwzględnie konieczne dla zagwarantowania rzetelnego przetwarzania. Stanowi to zatem zasadniczy wymóg w odniesieniu do udzielenia ważnej zgody na stosowanie danych biometrycznych.

Przykłady:
Udzielenie ważnej zgody na stosowanie systemu kontroli dostępu, w ramach którego stosuje się odciski palców, wymaga informacji, czy w systemie biometrycznym tworzony jest wzorzec unikalny dla tego systemu. Jeżeli stosuje się algorytm tworzący ten sam wzorzec biometryczny w różnych systemach biometrycznych, osoba, której dane dotyczą, musi wiedzieć, że może zostać rozpoznana w wielu różnych systemach biometrycznych.

Określona osoba przesyła swoją fotografię do internetowego albumu z fotografiami. Rejestracja tej fotografii w systemie biometrycznym wymaga wyraźnej zgody udzielonej w oparciu o wyczerpujące informacje dotyczące tego, co dzieje się z danymi biometrycznymi, oraz czasu i celu ich przetwarzania.

Ponieważ zgodę można w każdym momencie cofnąć, administratorzy danych muszą wdrożyć środki techniczne, dzięki którym możliwe jest zaprzestanie stosowania danych biometrycznych w ich systemach. Musi zatem istnieć możliwość skutecznego usunięcia wszystkich elementów powiązanych z tożsamością stworzonych w systemie biometrycznym działającym na podstawie zgody.

[5] WP 187, Opinia 15/2011 w sprawie definicji „zgody”.

3.1.2. Umowa, art. 7 lit. b)

Przetwarzanie danych biometrycznych może być konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy. Należy jednak zauważyć, że ma to zastosowanie zasadniczo tylko w sytuacji, w której świadczone usługi mają charakter czysto biometryczny. Ta podstawa prawna nie może służyć do uzasadnienia usługi mającej charakter wtórny, która polega na rejestracji danej osoby w systemie biometrycznym. Jeżeli możliwe jest oddzielenie takiej usługi od usługi głównej, umowa dotycząca usługi głównej nie może stanowić uzasadnienia dla przetwarzania danych biometrycznych. Dane osobowe nie są towarami, których można domagać się w zamian za usługę, dlatego umowy, w których przewiduje się taką wymianę, lub umowy, w których oferuje się usługi tylko pod warunkiem udzielenia zgody danej osoby na przetwarzanie jej danych biometrycznych do celów innej usługi, nie mogą stanowić podstawy prawnej takiego przetwarzania.

Przykłady:
a) Dwaj bracia oddają do laboratorium próbki włosów w celu wykonania badania DNA, aby dowiedzieć się, czy na prawdę są braćmi. Umowa zawarta z laboratorium dotycząca wykonania tego badania jest wystarczającą podstawą prawną do rejestracji i przetwarzania danych biometrycznych.

b) Osoba zamieszcza fotografię, aby pokazać ją swoim przyjaciołom w albumie fotograficznym na portalu społecznościowym. Jeżeli w umowie (w warunkach świadczenia usługi) przewiduje się, że korzystanie z tej usługi wiąże się z rejestracją tego użytkownika w systemie biometrycznym, takie postanowienie nie jest wystarczającą podstawą prawną do dokonania takiej rejestracji.

3.1.3. Zobowiązanie prawne, art. 7 lit. c)

Inna podstawa prawna przetwarzania danych osobowych występuje, jeżeli przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega. Ma to na przykład miejsce w niektórych państwach w związku z wydawaniem lub stosowaniem paszportów[6] i wiz[7].

---

[6] Odciski palców zostały włączone do paszportów zgodnie z rozporządzeniem Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. i do dokumentów pobytowych zgodnie z rozporządzeniem Rady (WE) nr 1030/2002 z dnia 13 czerwca 2002 r.

[7] Rejestracja identyfikatorów biometrycznych w wizowym systemie informacyjny (VIS) przewidziana jest na mocy rozporządzenia (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS). Zob. również opinię nr 3/2007 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego Wspólne Instrukcje Konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczące wiz w związku z wprowadzeniem technologii biometrycznych, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków wizowych (COM(2006)269 wersja ostateczna). WP134; opinię 2/2005 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych COM (2004) 835 wersja ostateczna WP 110; opinię 7/2004 w sprawie włączenia elementów biometrycznych do dokumentów pobytowych i wiz z uwzględnieniem ustanowienia europejskiego wizowego systemu informacyjnego (VIS) WP 96.

3.1.4. Uzasadnione interesy administratora danych, art. 7 lit. f)

Zgodnie z art. 7 dyrektywy 95/46/WE przetwarzanie danych biometrycznych może być również uzasadnione, jeżeli jest ono „konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą".

Oznacza to, że mogą wystąpić przypadki, w których stosowanie systemów biometrycznych może leżeć w uzasadnionym interesie administratora danych. Tego rodzaju interes jest uzasadniony tylko, jeżeli administrator danych może wykazać, że jego interes jest obiektywnie nadrzędny względem prawa osoby, której dane dotyczą, do nierejestrowania jej w systemie biometrycznym. Przykładowo, jeżeli należy w sposób szczególny zapewnić bezpieczeństwo stref wysokiego ryzyka, stosując mechanizm umożliwiający dokładne sprawdzenie, czy dane osoby mają prawo dostępu do tych stref , zastosowanie systemu biometrycznego może leżeć w uzasadnionym interesie administratora danych. W poniższym przykładzie dotyczącym biometrycznego systemu kontroli dostępu do laboratorium administrator danych nie może zapewnić pracownikowi alternatywnego mechanizmu bez wywierania bezpośredniego wpływu na bezpieczeństwo tego obszaru o ograniczonym dostępie, ponieważ nie istnieją alternatywne, w mniejszym stopniu naruszające prywatność środki odpowiednie do osiągnięcia właściwego poziomu bezpieczeństwa tej strefy. Wdrożenie systemu i zarejestrowanie w nim ograniczonej liczby pracowników leży zatem w uzasadnionym interesie administratora danych. Nie musi on uzyskiwać zgody tych pracowników. Jednak także w przypadku, w którym uzasadniony interes administratora danych stanowi ważną podstawę prawną przetwarzania, jak zawsze wszystkie inne zasady w zakresie ochrony danych nadal mają zastosowanie, w szczególności zasada proporcjonalności i zasada minimalizacji danych.

Przykład:
W przedsiębiorstwie prowadzącym badania nad groźnymi wirusami laboratorium jest zabezpieczone drzwiami, które otwierają się tylko w przypadku pomyślnej weryfikacji odcisków palców i skanu tęczówki. System ten jest wdrożono w celu dopilnowania, aby eksperymenty z użyciem tych niebezpiecznych materiałów mogły przeprowadzać wyłącznie osoby zapoznane ze szczególnym ryzykiem, przeszkolone w zakresie procedur i uznane za godne zaufania przez przedsiębiorstwo. Uzasadniony interes przedsiębiorstwa polegający na dopilnowaniu, aby wyłącznie właściwe osoby mogły wchodzić do obszaru o ograniczonym dostępie, w celu zapewnienia ograniczenia czynników ryzyka dla bezpieczeństwa związanych z dostępem do tej konkretnej strefy o ograniczonym dostępie, jest wyraźnie nadrzędny względem życzenia osób, aby nie przetwarzano ich danych biometrycznych.

Zgodnie z zasadą ogólną nie można uznać, że wykorzystanie biometrii do celów ogólnych wymogów bezpieczeństwa własności i osób fizycznych wynika z uzasadnionego interesu nadrzędnego względem interesów lub podstawowych praw i wolności osób, których dane dotyczą. Wręcz przeciwnie, przetwarzanie danych biometrycznych może być uzasadnione jako konieczne narzędzie zabezpieczające własność lub osoby fizyczne, tylko jeżeli istnieją dowody oparte na obiektywnych i udokumentowanych okolicznościach na występowanie konkretnego znacznego ryzyka. W tym celu administrator danych musi udowodnić, że wskutek szczególnych okoliczności powstaje konkretne, znaczne ryzyko, które administrator danych ma obowiązek ocenić z zachowaniem szczególnej dbałości. Aby zachować zgodność z zasadą proporcjonalności, administrator danych w tego rodzaju sytuacjach wysokiego ryzyka ma obowiązek sprawdzić, czy ewentualne alternatywne środki byłyby równie

skuteczne, a jednocześnie w odniesieniu do realizowanych celów ingerowałyby w prywatność w mniejszym stopniu, oraz powinien wybrać takie środki alternatywne.
Należy również regularnie weryfikować występowanie wspomnianych okoliczności. Na podstawie wyników tej weryfikacji należy zakończyć lub wstrzymać wszystkie operacje przetwarzania danych, co do których uznano, że przestały być zasadne

3.2. Administrator danych i przetwarzający

W dyrektywie 95/46/WE na administratorów danych nakłada się obowiązki związane z przetwarzaniem przez nich danych osobowych. W kontekście biometrii administratorem danych mogą być różne rodzaje podmiotów, na przykład pracodawcy, organy ścigania lub organy migracyjne.

Grupa robocza przypomina wytyczne przedstawione w jej opinii w sprawie pojęć „administrator danych" i „przetwarzający"[8], zawierające skuteczne wyjaśnienia sposobu interpretacji tych podstawowych definicji zawartych w dyrektywie.

3.3. Zautomatyzowane przetwarzanie (art. 15 dyrektywy)

W przypadku stosowania systemów opartych na przetwarzaniu danych biometrycznych należy zwracać szczególną uwagę na ewentualne skutki dyskryminujące osoby odrzucone przez system. Ponadto w celu ochrony prawa osoby fizycznej do nieobjęcia jej środkiem mającym na nią wpływ opartym wyłącznie na zautomatyzowanym przetwarzaniu danych, należy wprowadzić właściwe zabezpieczenia, takie jak interwencje ludzkie, środki ochrony prawnej lub mechanizmy umożliwiające wyrażenie opinii przez osobę, której dane dotyczą.

Zgodnie z art. 15 dyrektywy 95/46/WE „państwa członkowskie przyznają każdej osobie prawo do nieobjęcia jej decyzją, która wywołuje skutki prawne, które jej dotyczą lub mają na nią istotny wpływ, oraz która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ją aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność, sposób zachowania itp.".

3.4. Przejrzystość i informowanie osoby, której dane dotyczą

Zgodnie z zasadą rzetelnego przetwarzania osoby, których dane dotyczą, muszą być świadome gromadzenia lub wykorzystywania ich danych biometrycznych (art. 6 dyrektywy 95/46/WE). Należy unikać stosowania jakiegokolwiek systemu, w którym takie dane gromadzono by bez wiedzy osób, których dane dotyczą.

Administrator danych musi upewnić się, że osoby, których dane dotyczą, są odpowiednio informowane o kluczowych elementach przetwarzania danych zgodnie z art. 10 dyrektywy o ochronie danych, takich jak informacje o tożsamości administratora danych, cele przetwarzania danych, rodzaj danych, okres przetwarzania danych, prawa osób, których dotyczą dane, do wglądu do danych, poprawiania lub usuwania danych oraz prawa do cofnięcia zgody, a także informacje o odbiorcach lub kategoriach odbiorców, którym dane są ujawniane. Ponieważ administrator danych systemu biometrycznego ma obowiązek poinformować osobę, której dane dotyczą, nie można pobierać danych biometrycznych osoby bez jej wiedzy.

---

8 WP169, Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający".

3.5. Prawo dostępu do danych biometrycznych

Osoby, których dane dotyczą, mają prawo do uzyskania od administratora danych dostępu do ich danych w ogóle, w tym w ich danych biometryczne. Osoby, których dotyczą dane, mają również prawo dostępu do ewentualnych profili opartych na tych danych biometrycznych. Jeżeli w celu zezwolenia na dostęp do danych administrator danych musi upewnić się co do tożsamości osób, których dane dotyczą, ważne jest, aby taki dostęp został zapewniony bez przetwarzania dodatkowych danych osobowych.

3.6. Bezpieczeństwo danych

Administratorzy danych muszą wprowadzić odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania[9].

Wszystkie gromadzone i przechowywane dane należy odpowiednio zabezpieczyć. Autorzy systemów muszą nawiązać współpracę z właściwymi ekspertami ds. bezpieczeństwa w celu zapewnienia skutecznego wyeliminowania słabych punktów zabezpieczeń, w szczególności w przypadku migracji istniejących systemów do internetu.

3.7. Gwarancje dla osób o specjalnych potrzebach

Korzystanie z danych biometrycznych może mieć poważny wpływ na godność, prywatność i prawo do ochrony osób wymagających szczególnej troski, takich jak małe dzieci, osoby w podeszłym wieku i osoby, które fizycznie nie są w stanie pomyślnie przejść procesu rejestracji. Ze względu na potencjalnie szkodliwe konsekwencje dla zainteresowanych osób, aby dany środek ingerujący w godność osoby fizycznej można było uznać za dopuszczalny, konieczne jest spełnienie surowszych wymogów w ramach procesu oceny skutków tego środka pod względem badania jego konieczności i proporcjonalności oraz możliwości osoby fizycznej do wyegzekwowania jej prawa do ochrony danych. Należy zapewnić właściwe środki zabezpieczające przed ryzykiem stygmatyzacji lub dyskryminacji tych osób fizycznych ze względu na ich wiek lub na ich niezdolność do dokonania rejestracji.

W odniesieniu do wprowadzenia ogólnego prawnego obowiązku gromadzenia identyfikatorów biometrycznych w przypadku tych grup, w szczególności w przypadku małych dzieci i osób w podeszłym wieku, do celów identyfikacji w ramach kontroli granicznych grupa robocza jest zdania, że „w trosce o godność osobistą i zapewnienie niezawodności procedury, pobieranie i przetwarzanie obrazów odcisków palców dzieci i osób starszych powinno podlegać ograniczeniom, a granica wiekowa powinna być taka sama, jak granica wiekowa ustalona dla innych dużych baz danych biometrycznych UE (w szczególności Eurodac)”[10].

W każdym przypadku należy wdrożyć szczególne środki zabezpieczające (takie jak właściwe procedury awaryjne) w celu zapewnienia poszanowania godności ludzkiej i praw podstawowych każdej osoby fizycznej, która nie jest w stanie pomyślnie przejść procesu

---

[9] Art. 17 ust. 1 dyrektywy 95/46/WE.

[10] WP134 – Opinia nr 3/2007 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego Wspólne Instrukcje Konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczące wiz w związku z wprowadzeniem technologii biometrycznych, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków wizowych (COM(2006)269 wersja ostateczna).

rejestracji, unikając w ten sposób obciążania takiej osoby niedoskonałościami systemu technicznego[11].

3.8. Dane szczególnie chronione

Niektóre dane biometryczne można uznać za szczególnie chronione w rozumieniu art. 8 dyrektywy 95/46/WE, a w szczególności dane ujawniające pochodzenie rasowe lub etniczne lub dane dotyczące zdrowia. Przykładowo dane dotyczące DNA danej osoby często obejmują dane dotyczące zdrowia lub mogą ujawniać pochodzenie rasowe lub etniczne. W tym przypadku dane dotyczące DNA stanowią dane szczególnie chronione i należy stosować szczególne środki zabezpieczające przewidziane w art. 8 dodatkowo w stosunku do ogólnych zasad ochrony danych przewidzianych w dyrektywie. W celu dokonania oceny stopnia szczególnej ochrony danych przetwarzanych w systemie biometrycznym należy uwzględnić również kontekst przetwarzania[12].

3.9. Rola krajowych organów ochrony danych

Uwzględniając coraz szerzej zakrojoną normalizację technologii biometrycznych do celów interoperacyjności, powszechnie uznaje się, że scentralizowane przechowywanie danych biometrycznych zwiększa zarówno ryzyko stosowania danych biometrycznych jako kluczowego czynnika połączenia wielu baz danych (co mogłoby doprowadzić do tworzenia szczegółowych profili danej osoby fizycznej), jak i szczególne zagrożenia związane z ponownym zastosowaniem takich danych niezgodnym z celami ich gromadzenia, szczególnie w przypadku nieuprawnionego dostępu.

Grupa robocza zaleca wprowadzenie wymagania, aby systemy, w których stosuje się dane biometryczne jako kluczowy czynnik połączenia wielu baz danych, posiadały dodatkowe środki zabezpieczające, ponieważ tego rodzaju przetwarzanie może stwarzać szczególne zagrożenia dla praw i wolności osób, których dane dotyczą (art. 20 dyrektywa 95/46/WE). W celu zapewnienia odpowiednich środków zabezpieczających, a w szczególności w celu ograniczenia ryzyka dla osób, których dane dotyczą, przed wprowadzeniem takich środków administrator danych powinien skonsultować się z właściwym krajowym organem ochrony danych.

4. Nowe osiągnięcia i trendy technologiczne, nowe scenariusze

4.1. Wprowadzenie

Technologie biometryczne są stosowane od dawna głównie przez organy rządowe, jednak ostatnio sytuacja stopniowo uległa zmianie i obecnie główną rolę w stosowaniu tych technologii i opracowywaniu nowych produktów odgrywają organizacje komercyjne.

Jednym z kluczowych czynników powodujących taką sytuację jest fakt, że rozwój technologii przebiegał w taki sposób, iż systemy biometryczne, które wcześniej działały prawidłowo jedynie w warunkach kontrolowanych, zostały udoskonalone i mają obecnie szerokie zastosowanie w wielu różnych środowiskach. W tym sensie w niektórych przypadkach biometrię stosuje się w celu zastąpienia się lub usprawnienia konwencjonalnych metod identyfikacji, w szczególności metod opartych na wielu czynnikach identyfikacji niezbędnych w solidnych systemach uwierzytelnienia. Technologie biometryczne coraz częściej stosuje się

[11] Zob. WP134 – Opinia nr 3/2007, s. 8.

[12] Por. WP 29 Dokument doradczy w sprawie szczególnych kategorii danych („danych szczególnie chronionych") ref. Ares (2011)444105 - 20/04/2011.

w aplikacjach, dzięki którym można szybko i wygodnie zidentyfikować daną osobę kosztem niższego stopnia dokładności.

Wykorzystanie technologii biometrycznych stopniowo wychodzi poza ich pierwotną sferę zastosowania: od identyfikacji i uwierzytelnienia do analizy zachowań, nadzoru i zapobiegania oszustwom.

Postępy w zakresie technologii i sieci komputerowych prowadzą również do powstawania dziedziny uznawanej za drugą generację biometrii opartą na stosowaniu cech behawioralnych i psychologicznych, która występuje samodzielnie lub w połączeniu z innymi klasycznymi systemami, tworząc systemy multimodalne. Obraz dopełnia stopniowe przechodzenie na stosowanie biometrii w inteligentnym otoczeniu technologicznym i wszechobecnych osiągnięciach technologii obliczeniowych.

4.2. Nowe tendencje w biometrii

Istnienie szereg technologii biometrycznych, które można uznać za technologie rozwinięte mające szereg zastosowań w systemach ochrony porządku publicznego i administracji elektronicznej oraz w systemach komercyjnych. Niewyczerpujący ich wykaz obejmowałby wykorzystanie odcisków palców, geometrii dłoni, skanów tęczówki i niektórych rodzajów rozpoznawania twarzy. Pojawiają się również technologie biometryczne umożliwiające analizę określonych cech ciała. Niektóre z tych technologii są nowe, jednak tradycyjne technologie biometryczne również uzyskują nowy impuls dzięki nowym możliwościom w dziedzinie przetwarzania danych.

Do typowych elementów tych nowych systemów należy wykorzystanie cech ciała umożliwiających kategoryzację/identyfikację osób fizycznych i zdalne gromadzenie danych dotyczących takich cech. Zgromadzone dane stosuje się do tworzenia profili, prowadzenia zdalnego nadzoru lub do realizacji jeszcze bardzie złożonych zadań, takich jak tworzenie inteligentnego otoczenia technologicznego.

Stało się to możliwe dzięki stałemu rozwojowi czujników umożliwiających gromadzenie danych dotyczących nowych cech fizjologicznych oraz nowym sposobom przetwarzania tradycyjnych danych biometrycznych.

Należy również wspomnieć stosowanie tak zwanej biometrii miękkiej (ang. *soft biometrics*) oznaczającej wykorzystywanie bardzo powszechnych cech, które nie są odpowiednie do jednoznacznego odróżnienia lub identyfikacji danej osoby fizycznej, ale za to umożliwiają poprawę skuteczności innych systemów identyfikacji.

Kolejnym podstawowym elementem nowych systemów biometrycznych jest możliwość gromadzenia informacji na odległość lub w ruchu bez konieczności współpracy lub działania ze strony danej osoby fizycznej. Chociaż nadal nie jest to jeszcze technologia w pełni rozwinięta, podejmuje się znaczne wysiłki w tym kierunku, w szczególności do celów ochrony porządku publicznego.

Dziedziną, w której następuje szybki rozwój, jest stosowanie systemów multimodalnych, w których wykorzystuje się jednocześnie różne dane biometryczne lub wiele odczytów/jednostek tych samych danych biometrycznych, które można dostosować w celu optymalizacji stosunku bezpieczeństwa i wygody stosowania systemów biometrycznych. Dzięki temu można obniżyć wskaźnik błędnej akceptacji, poprawić wyniki systemu rozpoznawania lub ułatwić gromadzenie danych dotyczących dużej populacji, równoważąc

brak uniwersalności jednego źródła danych biometrycznych poprzez połączenie go z innym źródłem.

Systemy biometryczne coraz częściej stosują zarówno podmioty publiczne, jak i prywatne. Tradycyjnie w sektorze publicznym organy ścigania regularnie wykorzystują dane biometryczne. W sektorach finansowym, bankowym i w sektorze e-zdrowia wykorzystanie danych biometrycznych szybko wzrasta, tak jak w innych sektorach, takich jak sektory kształcenia, handlu detalicznego i telekomunikacji. Rozwój ten przyspieszą nowe właściwości uzyskane w wyniku konwergencji/połączenia istniejących technologii. Przykładem tego jest stosowanie systemów telewizji przemysłowej (CCTV) umożliwiających zarówno gromadzenie, jak i analizę danych biometrycznych i właściwości zachowań ludzkich.

Powyższą praktykę można również postrzegać jako zmianę kierunku rozwoju systemów biometrycznych – od poszukiwania narzędzi do identyfikacji przechodzi się do celów związanych z rozpoznawaniem „miękkim", co innymi słowy oznacza odejście od identyfikacji na rzecz wykrywania zachowania lub szczególnych potrzeb ludzi. Dzięki temu możliwe stają się również zastosowania znacznie różniące się od stosowanych na szeroką skalę aplikacji zabezpieczających: udoskonalona interakcja między człowiekiem a maszyną, która daje większe możliwości niż tylko identyfikacja lub kategoryzacja osoby fizycznej, przyniesie korzyści w odniesieniu do bezpieczeństwa osobistego, gier i handlu detalicznego.

4.3. Wpływ na prywatność i ochronę danych

Od samego początku wdrażania systemów biometrycznych uznaje się, że mogą one budzić poważne obawy w szeregu obszarów, w tym w dziedzinie prywatności i ochrony danych, co z pewnością wpłynęło na społeczną akceptację takich systemów i pobudziło debatę na temat legalności i granic ich stosowania oraz na temat środków zabezpieczających i gwarancji niezbędnych do ograniczenia zidentyfikowanych czynników ryzyka.

Tradycyjna niechęć do systemów biometrycznych była i pozostaje związana z ochroną praw indywidualnych. Nowe systemy i rozwój istniejących systemów budzą jednak szereg obaw. Obawy te dotyczą między innymi możliwości niejawnego gromadzenia, przechowywania i przetwarzania oraz gromadzenia materiału zawierającego informacje szczególnie chronione, które to czynności mogą naruszyć najintymniejsze sfery prywatności osób fizycznych.

Od samego początku stosowania technologii i systemów biometrycznych poważny problem stanowi potencjalne ich nadużywanie. Mimo że w tradycyjnej biometrii kwestia tego ryzyka jest dobrze znana i podejmowana, nie ma wątpliwości, że z wyższym potencjałem technicznym nowych systemów komputerowych wiąże się ryzyko wykorzystywania danych w sposób niezgodny z ich pierwotnym celem.

Niejawne techniki umożliwiają identyfikację osób fizycznych bez ich wiedzy, co powoduje poważne zagrożenie dla prywatności i utratę kontroli nad danymi osobowymi. Ma to z kolei poważne konsekwencje dla możliwości udzielania przez osoby fizyczne dobrowolnej zgody lub zwyczajnego uzyskania informacji na temat przetwarzania. Ponadto w ramach niektórych systemów możliwe jest potajemne gromadzenie informacji związanych ze stanem emocjonalnym lub z charakterystycznymi cechami ciała oraz ujawnianie informacji dotyczących zdrowia, co skutkuje nieproporcjonalnym przetwarzaniem danych oraz przetwarzaniem danych szczególnie chronionych w rozumieniu art. 8 dyrektywy 95/46/WE.

Ze względu na fakt, że w ramach technologii biometrycznych nie można zapewnić pełnej dokładności, zawsze istnieje ukryte ryzyko wynikające z nieprawidłowej identyfikacji. Tego rodzaju wyniki fałszywie dodatnie skutkują podejmowaniem decyzji mających wpływ na

prawa indywidualne. Kradzież tożsamości dokonana w oparciu o podstawione lub skradzione źródła danych biometrycznych może powodować poważne szkody. W odróżnieniu od innych systemów identyfikacji nie można po prostu zapewnić osobie fizycznej nowej identyfikacji, dlatego tylko, że ważność dotychczasowej została podważona.

W kontekście podejmowania automatycznych decyzji lub przewidywania zachowania lub preferencji w określonej sytuacji należy odnieść się do tworzenia profili. Niektóre dane biometryczne mogą ujawniać informacje na temat cech fizycznych dotyczące danej osoby fizycznej. Możliwość tę można wykorzystywać do celów tworzenia grup docelowych lub profili, jednak może to również doprowadzić do dyskryminacji, stygmatyzacji lub niechcianej konfrontacji z nieoczekiwanymi/niepożądanymi informacjami.

4.4. Odniesienie do konkretnych systemów i technologii biometrycznych

4.4.1. Układ żył i połączone zastosowania

Dwie główne stosowane technologie opierają się na rozpoznawaniu układu żył: rozpoznawanie układu żył dłoni i rozpoznawanie układu żył palca; obie te techniki są obecnie powszechnie stosowane, szczególnie w Japonii.

Z technicznego punktu widzenia rozpoznawanie układu żył opiera się na wzorcu żył pobranym z użyciem kamery termowizyjnej w momencie oświetlenia podczerwienią z bliska palca lub dłoni. Uzyskany obraz zostaje przetworzony w celu zobrazowania cech charakterystycznych układu żył, wskutek czego powstaje przetworzony obraz sieci naczyniowej. Główną zaletą takiej technologii jest fakt, że żadna osoba fizyczna nie zostawia śladu swojego identyfikatora biometrycznego[13], ponieważ „dotykanie" czytnika nie jest wymagane. Obecnie trudno jest również gromadzić dane biometryczne bez zgody osoby, której dane dotyczą. Ponadto technikę tę można również stosować do wykrycia, czy podmiot, wobec którego stosuje się system jest żywy poprzez zbadanie, czy zachodzi przepływ krwi.

Rozpoznawanie układu żył można stosować w aplikacjach dostępu logicznego i do celów dostępu fizycznego do obiektów. Producenci oferują również możliwość zamieszczania czujnika w innych produktach, szczególnie do celów bankowych.

Czynniki ryzyka w zakresie ochrony danych związane ze stosowaniem systemów rozpoznawania układu żył można opisać następująco:

- dokładność: poziom skuteczności rozpoznawania układu żył jest wysoki, jako że technologię tę postrzega się jako realną alternatywę dla odcisków palców. Z rozpoznawaniem układu żył wiąże się również niski wskaźnik niepowodzenia rejestracji (ang. *Failure to Enrol Rate – FER*), ponieważ nie ma nią wpływu pogorszenie stanu palca lub dłoni. Do tej pory nie prowadzono doświadczeń z tymi technologiami ani nie stosowano ich w odniesieniu do rejestru bardzo dużej populacji (w Japonii wzorzec porównuje się z wzorcem przechowywanym na karcie elektronicznej). W niektórych przypadkach na technologie tę mogą oddziaływać warunki klimatyczne wpływające na układ naczyniowy (wysoka temperatura, ciśnienie itp.);

[13] Według niektórych autorów za pomocą technologii związanych z rozpoznawaniem układu żył możliwe jest ujawnianie chorób, takich jak nadciśnienie lub wady naczyniowe.

- wpływ: wpływ systemów rozpoznawania układu żył na ochronę danych jest ograniczony, ponieważ gromadzenie danych biometrycznych nie jest łatwe, a wykorzystanie układu żył jest obecnie ograniczone do zastosowań w sektorze prywatnym;

- zgoda i przejrzystość: ponieważ dane dotyczące układu żył można gromadzić tylko stosując bliską podczerwień i kamery termowizyjne, można uznać, że dana osoba ma świadomość przetwarzania i udziela swojej zgody, przykładając palec lub dłoń do czytnika. Jak w przypadku każdego systemu biometrycznego założenie to należy przyjmować z większą ostrożnością w niektórych szczególnych okolicznościach, na przykład, gdy dana osoba jest pracownikiem administratora danych;

- dalszy cel lub dalsze cele przetwarzania: obecnie czynniki ryzyka związane z danymi dotyczącymi układu żył są ograniczone, jeśli chodzi o wykorzystanie tych danych do dalszych celów. Ryzyko to może ulec zwiększeniu, jeżeli ten rodzaj przetwarzania zostanie rozpowszechniony i jeżeli łatwiejsze stanie się podszywanie się pod inną osobę;

- możliwość tworzenia powiązań: dane dotyczące układu żył nie dostarczają informacji, które można powiązać z innymi danymi, z wyjątkiem danych dotyczących układu żył pochodzących z innego przetwarzania;

- śledzenie/tworzenie profili: ryzyko śledzenia/tworzenia profili z zastosowaniem danych dotyczących układu żył jest ograniczone tak długo, jak długo ten rodzaj danych biometrycznych nie jest powszechnie stosowany, na przykład w centralnych bazach danych na potrzeby kart płatniczych;

- przetwarzanie danych szczególnie chronionych: jedynymi danymi szczególnie chronionymi, które można uzyskać na podstawie danych dotyczących układu żył są dane dotyczące stanu zdrowia, jednak do tej pory nie przeprowadzono żadnej formalnej oceny w tym względzie;

- odwoływalność: wydaje się, że dane dotyczące układu żył są w bardzo dużym stopniu niezmienne w czasie, takie twierdzenie należy jednak potwierdzić doświadczalnie (systemy rozpoznawania układu żył są zbyt nowe, aby mogły dawać potwierdzone wyniki). Dane dotyczące układu żył należy zatem uznać za nieodwołalne;

- ochrona przed podszywaniem się: nie zbadano jeszcze w znacznym stopniu kwestii podszywania się z wykorzystaniem danych dotyczących układu żył, jednak z ostatnich badań wynika, że możliwe jest oszukanie czytnika układu żył dłoni[14]. Największą trudnością w takim podszywaniu się jest zdobycie próbki danych biometrycznych.

4.4.2. Odciski palców i połączone zastosowania

Rozpoznawanie linii papilarnych należy do najstarszych, najpowszechniej badanych i najbardziej rozpowszechnionych systemów biometrycznych. W dziedzinie ochrony porządku publicznego identyfikację za pomocą odcisków palców stosuje się od ponad 100 lat zarówno

[14] Zob.: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

do zadań z zakresu weryfikacji, jak i identyfikacji. Identyfikacja na podstawie odcisków palców opiera się na fakcie, że każda osoba fizyczna posiada niepowtarzalne linie papilarne wykazujące konkretne charakterystyczne cechy, które można zmierzyć w celu stwierdzenia, czy dany odcisk palca pasuje do zarejestrowanej próbki.

Rejestracja próbki wymaga fizycznej obecności danej osoby, a także, w zależności od przewidywanego zastosowania, należycie przeszkolonego personelu mającego zapewnić dobrą jakość danych. Pobranie odcisków palców nie jest zadaniem błahym. W związku z tym dokładność porównania będzie zależeć od jakości obrazu związanej z techniką tworzenia obrazu. Stosowane są różne techniki od pobierania odcisku jednego lub dwóch palców, do pobierania odcisków wszystkich dziesięciu palców w trybie płaskich odcisków palców lub w trybie odbitek przetoczonych. W zależności od systemu odciski palców można stosować jedynie do weryfikacji (1:1) lub do identyfikacji i kojarzenia ze śladami (1:n). Jak wynika z niektórych badań, część populacji z różnych przyczyn nie jest jednak w stanie zarejestrować swoich odciski palców, co stanowi problem wymagający istnienia właściwych procedur awaryjnych, w szczególności w przypadku dużych systemów, w celu uniknięcia pozbawienia osób fizycznych korzystania z czegoś, co im przysługuje.

Chociaż jest to metoda, która zasadniczo nie narusza w znacznym stopniu prywatności, może być jednak jako taka postrzegana, ponieważ kojarzy się z traktowaniem ludzi jak podejrzanych ze względu na jej powszechne stosowanie w dziedzinie ochrony porządku publicznego.

Odciski palców wykazują różne cechy, które można wykorzystywać do celów weryfikacji/identyfikacji, chociaż analiza minucji nadal pozostaje techniką najczęściej stosowaną. Rozwój nowych technik (takich jak skanery o wysokiej rozdzielczości) umożliwi wykorzystanie innych cech. Dalszy rozwój techniki nastąpił również w zakresie zdolności identyfikacyjnych umożliwiających wykorzystanie dużych baz danych do celów identyfikacji.

W tym zakresie najbardziej zaawansowanymi systemami są tak zwane automatyczne systemy identyfikacji daktyloskopijnej (AFIS) stosowane do celów ochrony porządku publicznego, które można wykorzystywać do odpowiedniej wymiany danych, przeszukując różne repozytoria danych w wymiarze transgranicznym. Wymiana danych wiąże się z problemami dotyczącymi różnych lokalizacji, formatów i poziomów jakości.

Przykładowymi systemami AFIS na szczeblu UE są Eurodac i wizowy system informacyjny, które – jak się oczekuje – będą zaliczać się do największych baz danych na świecie, biorąc pod uwagę, że w systemach tych będzie przechowywanych około 70 milionów odcisków palców. W swoich poprzednich opiniach grupa robocza podniosła szereg kwestii dotyczących stosowania wielkoskalowych baz danych, uwzględniając konieczność zapewnienia proporcjonalności. W szczególności należy rozwiązać problemy dotyczące wiarygodności w związku z uzyskiwaniem wyników fałszywie dodatnich i fałszywie ujemnych, problem skutecznej kontroli dostępu do tych baz danych oraz problemy związane ze stosowaniem odcisków palców dzieci i osób w podeszłym wieku.

W systemach biometrycznych opartych na pobieraniu odcisków palców powszechnie stosuje się wzorce, które dostawcy systemów uznają zwykle za sposób ochrony osoby fizycznej. W zależności od systemu/algorytmu zastosowanego do wygenerowania wzorca istnieje jednak potencjalne ryzyko związane z możliwością powiązania wzorców z innymi bazami danych daktyloskopijnych w celu identyfikacji osób fizycznych.

Istotną kwestią jest również stosowanie systemów mających na celu obchodzenie systemów rozpoznawania linii papilarnych z wykorzystaniem sztucznych palców lub odcisków palców wykonanych ze sztucznego materiału, co umożliwia dokonywanie kradzieży tożsamości. Istnieją różne sposoby zmniejszenia stopnia narażenia tych systemów, takie jak detekcja żywej tkanki, systemy oparte na rozpoznawaniu wielu palców, a także stosownie właściwego nadzoru sprawowanego przez człowieka nad zadaniami związanymi z rejestracją oraz identyfikacją/weryfikacją.

Występujące problemy w zakresie ochrony danych związane ze stosowaniem odcisków palców można zwięźle opisać następująco:

- dokładność: chociaż ostatecznie odciski palców cechują się wysokim wskaźnikiem dokładności, to jednak można tę dokładność zakwestionować ze względu na problemy związane z niewystarczającymi informacjami (niską jakością danych lub niespójnym procesem pozyskiwania odcisków) lub interpretacją (wyborem cech lub jakością algorytmów wyodrębniania danych). Może to prowadzić do przypadków błędnego odrzucenia lub błędnego dopasowania;

- wpływ: ze względu na nieodwracalność procesu może dochodzić do ograniczenia możliwości wyegzekwowania przez osobę fizyczną jej praw lub do ograniczenia możliwości cofnięcia decyzji podjętej w oparciu o błędną identyfikację. Poleganie na dokładności identyfikacji odcisków palców może sprawiać, że trudniejsze staje się skorygowanie ewentualnych błędów, co może mieć daleko idące konsekwencje dla danej osoby fizycznej. Czynniki te należy uwzględniać przy dokonywaniu oceny proporcjonalności przetwarzania danych w stosunku do konkretnej decyzji podejmowanej na podstawie rozpoznania odcisków palców. Należy również stwierdzić, że brak środków bezpieczeństwa może prowadzić do kradzieży tożsamości, która może mieć poważne skutki dla danej osoby fizycznej;.

- możliwość tworzenia powiązań: stosowanie odcisków palców daje możliwość ich niewłaściwego użycia, ponieważ dane te można powiązać z innymi bazami danych. Możliwość powiązania z innymi bazami danych może prowadzić do zastosowań niezgodnych z pierwotnymi celami. Istnieją pewne techniki, takie jak zamienne dane biometryczne lub kodowanie danych biometrycznych, które można stosować w celu ograniczenia tego ryzyka;

- przetwarzanie danych szczególnie chronionych: zgodnie z niektórymi badaniami obrazy odcisków palców mogą ujawniać informacje dotyczące pochodzenia etnicznego danej osoby fizycznej[15];

- dalszy cel lub dalsze cele przetwarzania: centralne przechowywanie danych, szczególnie w dużych bazach danych, oznacza ryzyko związane z bezpieczeństwem danych, możliwością ich powiązania i nadużyciami. Przy braku zabezpieczeń umożliwia to wykorzystywanie odcisków palców do celów innych niż cele, które pierwotnie uzasadniały przetwarzanie;

- zgoda i przejrzystość: zgoda jest podstawową kwestią w przypadku wykorzystywania odcisków palców do celów innych niż ochrona porządku publicznego. Odciski palców

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm oraz http://www.crime-scene-investigator.net/fingerprintpatterns.html.

można z łatwością skopiować ze śladów odcisków palców, a nawet z fotografii, bez wiedzy danej osoby fizycznej. Inne kwestie dotyczące zgody związane są z uzyskaniem zgody dziecka i roli rodzica w tym względzie (np. w przypadku pobierania odcisków palców w szkołach) oraz ważności zgody w przypadku oddawania odcisków palców w kontekście stosunku pracy;

- odwoływalność: dane daktyloskopijne są w bardzo dużym stopniu niezmienne w czasie i należy je uznać za nieodwołalne. Wzorzec linii papilarnych można unieważnić na określonych warunkach;

- ochrona przed podszywaniem się: odciski palców można z łatwością pobrać ze względu na wiele śladów odcisków palców pozostawianych przez osobę fizyczną. Ponadto w przypadku wielu systemów i czujników można stosować sztuczne odciski palców, szczególnie jeżeli takie systemy nie posiadają szczególnej ochrony przed takim procederem. Powodzenie ataku w dużym stopniu zależy od rodzaju czujnika (optyczny, pojemnościowy itp.) i materiału zastosowanego przez atakującego.

Przykład:
W szpitalu wykorzystuje się odciski palców w centralnej bazie danych do uwierzytelniania pacjentów korzystających z usługi radioterapeutycznej, aby mieć pewność, że właściwy pacjent jest leczony we właściwy sposób. Preferuje się stosowanie odcisków palców w stosunku do układu żył, ponieważ leczenie wpływa na układ naczyniowy. Ponadto korzysta się z centralnej bazy danych, ponieważ stan pacjentów (wiek, patologia) oznacza wysokie ryzyko utraty plakietki, co zablokowałoby dostęp do leczenia. W takiej sytuacji stosowanie odcisków palców wydaje się rozwiązaniem proporcjonalnym.

4.4.3 Rozpoznawanie twarzy i połączone zastosowania

Twarz, tak jak odciski palców, od wielu lat powszechnie wykorzystuje się jako źródło danych biometrycznych. Od niedawna twarz może służyć już nie tylko do określenia tożsamości, ale również charakterystycznych cech fizjologicznych i psychologicznych, takich jak pochodzenie etniczne, emocje i samopoczucie. Zdolność do wyodrębniania takiej ilości danych z obrazu oraz fakt, że fotografię można wykonać z pewnej odległości bez wiedzy osoby, której dane dotyczą, wskazuje na wagę kwestii związanych z ochroną danych, mogących powstać wskutek stosowania takich technologii.

Rozpoznawanie twarzy jako sposób identyfikacji i weryfikacji nie uszło uwadze organów ścigania, innych organów publicznych, a także organizacji prywatnych. Od wielu lat fotografie widnieją w paszportach, prawach jazdy, krajowych dowodach tożsamości i w kartotekach policyjnych. Fotografie powszechnie drukuje się na kartach kontroli dostępu lub innych organizacyjnych kartach potwierdzających tożsamość. Fotografie te są zwykle wykonywane w kontrolowanym oświetleniu i ograniczają się do widoku twarzy osoby fizycznej z przodu lub z profilu. Stosowanie tego rodzaju kontrolowanego zestawu fotografii w naturalny sposób stało się punktem wyjścia dla automatycznego przetwarzania danych i rozpoznawania osób fizycznych. Od tamtej pory nastąpił postęp wykraczający poza tę możliwość i obecnie technologia znajduje się w punkcie, w którym możliwe jest dokonywanie identyfikacji przy użyciu szeregu różnych kamer, punktów widzenia i w różnych warunkach oświetlenia. Istnieje również ogromna liczba fotografii dostępnych publicznie w internecie, takich jak fotografie zamieszczane na portalach społecznościowych i w innych publicznie dostępnych galeriach. Związane z tym ryzyko nie ogranicza się do tradycyjnych fotografii, ponieważ rozpoznawanie twarzy z powodzeniem zintegrowano z

materiałami wideo uzyskiwanymi w czasie rzeczywistym. Administratorzy danych muszą zdawać sobie sprawę, że dodawanie nowych zdolności przetwarzania danych do istniejącego systemu (np. rozpoznawanie twarzy w systemie CCTV) może zmienić określony cel lub cele pierwotnego systemu oraz muszą dokonać ponownej oceny wpływu tej zmiany na prywatność.

Czynniki ryzyka w zakresie ochrony danych związane ze stosowaniem systemów rozpoznawania twarzy można opisać następująco:

- dokładność: jeżeli nie można zagwarantować jakości fotografii, istnieje ryzyko braku dokładności. Oczywiste jest, że, jeżeli twarz nie zostanie uchwycona (zasłonięta przez włosy lub nakrycie głowy), nie można dokonać porównania lub kategoryzacji bez uniknięcia wysokiego poziomu błędu. Dużym wyzwaniem w zakresie rozpoznawania twarzy pozostają zmiany postawy i oświetlenia, które mają duży wpływ na dokładność;

- wpływ: szczególny wpływ określonego systemu rozpoznawania twarzy na ochronę danych będzie zależeć od jego celu i konkretnych okoliczności. System kategoryzacji służący do liczenia cech demograficznych osób odwiedzających daną atrakcję bez możliwości nagrywania będzie miał inny wpływ na ochronę danych niż system stosowany przez organy ścigania do potajemnego nadzoru w celu identyfikacji osób mogących sprawiać problemy;

- zgoda i przejrzystość: ryzyko w zakresie ochrony danych niewystępujące w wielu innych rodzajach przetwarzania danych biometrycznych stanowi fakt, że obrazy można pobrać i przetworzyć z wielu różnych punktów widzenia, w różnych warunkach otoczenia i bez wiedzy osoby, której dane dotyczą. W opinii nr 15/2011 dotyczącej definicji zgody grupa robocza podkreśliła, że, aby zgoda mogła stanowić podstawę prawną przetwarzania, musi ona być „świadoma”. Osoba, której dane dotyczą, nie może udzielić świadomej zgody, jeżeli nie wie o przetwarzaniu obrazów do celów rozpoznawania twarzy. Nawet, jeżeli osoba, której dane dotyczą, jest świadoma działania kamery, mogą nie istnieć żadne wizualne wskazówki odróżniające system CCTV rejestrujący na żywo lub nagrywający od soczewek pobierających obrazy do systemu rozpoznawania twarzy;

- dalszy cel lub dalsze cele przetwarzania: pobrane, zgodnie lub niezgodnie z prawem, obrazy cyfrowe można łatwo wymieniać lub kopiować w celu przetwarzania w systemach odmiennych od systemów, do których obrazy te zostały pierwotnie przeznaczone. Jest to oczywiste w rzeczywistości mediów społecznościowych, w których użytkownicy przesyłają swoje osobiste fotografie w celu dzielenia się nimi z rodziną, przyjaciółmi i współpracownikami. W momencie, w którym fotografie znajdują się na platformie mediów społecznościowych, są one dostępne do ponownego wykorzystania przez samą platformę do szeregu różnych celów, przy czym niektóre spośród tych celów mogą zostać określone w platformie po pewnym czasie od wykonania fotografii lub jej wysłania;

- możliwość tworzenia powiązań: w ramach wielu usług internetowych umożliwia się użytkownikom wysłanie fotografii w celu powiązania jej z profilem użytkownika. Rozpoznawanie twarzy można wykorzystywać do łączenia profili tworzonych w ramach różnych usług internetowych (poprzez obraz profilowy), a także między

światem wirtualnym a światem rzeczywistym. Istnieje możliwość zrobienia fotografii osoby na ulicy i określenia jej tożsamości w czasie rzeczywistym poprzez przeszukanie takich publicznych obrazów profilowych. Przeglądanie publicznie dostępnych fotografii profilowych i innych w celu tworzenia zbiorów fotografii służących powiązaniu tożsamości w świecie rzeczywistym z takimi fotografiami możliwe jest również w ramach usług osób trzecich;.

- śledzenie/tworzenie profili: system identyfikacji można również stosować, jeżeli tożsamość danej osoby fizycznej w świecie rzeczywistym nie jest znana. System rozpoznawania twarzy w centrum handlowym lub podobnej przestrzeni publicznej można wykorzystać do śledzenia trasy i nawyków poszczególnych klientów. Mogłoby to służyć skutecznemu zarządzaniu kolejkami lub lokowaniu produktu w celu zapewnienia klientowi lepszych zakupów. Ze zdolnością śledzenia lub lokalizowania konkretnej osoby fizycznej wiąże się jednak zdolność tworzenia profilu i zapewniania ukierunkowanej reklamy lub innych szczególnych usług;

- przetwarzanie danych szczególnie chronionych: jak już wspomniano, przetwarzanie danych biometrycznych można wykorzystywać do ustalenia danych szczególnie chronionych, w szczególności danych związanych z widocznymi cechami, takimi jak rasa, grupa etniczna lub nawet stan zdrowia;

- odwoływalność: osoba fizyczna może z łatwością zmienić wygląd twarzy (za pomocą brody, okularów, nakrycia głowy itp.), co może być wystarczającym sposobem na zmylenie systemów rozpoznawania twarzy, szczególnie jeżeli takie systemy działają w niekontrolowanym otoczeniu. Główne cechy twarzy osoby fizycznej są jednak niezmienne w czasie; w systemach możliwe jest też usprawnienie rozpoznawania poprzez gromadzenie i łączenie różnych znanych „twarzy" danej osoby fizycznej;

- ochrona przed podszywaniem się: wiele systemów rozpoznawania twarzy można z łatwością zwieść, jednak producenci starają się usprawnić ochronę przed taką możliwością za pomocą technik, takich jak tworzenie obrazu trójwymiarowego lub nagrywanie wideo. Najbardziej podstawowe systemy stosowane w aplikacjach publicznych nie zawierają jednak tego rodzaju ochrony.

Przykład:
Skrajnym przykładem, jaki można sobie wyobrazić, byłby stosowany w centrach handlowych system nadzoru wideo nowej generacji rozpoznający osoby, automatycznie śledzący ruch, rozróżniający charakterystyczne cechy twarzy, takie jak uśmiech lub złość. Taki system mógłby rozpoznawać regularnych klientów wjeżdżających na parking centrum handlowego i skierować ich do ich ulubionych miejsc parkingowych. W momencie, w którym klienci wchodzą do centrum handlowego, system mógłby dokonywać identyfikacji odzieży w celu zasugerowania sklepów, które warto odwiedzić, w zależności od dostępnej oferty sklepów, wcześniej dokonane zakupy lub przewidziany zestaw wskaźników. Można również zorganizować wyświetlanie ukierunkowanych reklam w witrynach sklepowych lub automatyczną odmowę wstępu do sklepów, restauracji i innych miejsc. Można byłoby identyfikować i namierzać potencjalnych złodziei samochodów zanim nawet zdołają dotknąć samochodu. W razie potrzeby podejrzanych można by było śledzić, stosując zdalnie sterowane statki powietrzne (bezpilotowe statki powietrzne) z zamieszczonymi kamerami i

innymi czujnikami, do czasu rozwiania lub potwierdzenia podejrzenia. Można by było wykrywać przedmioty schowane w odzieży (noże lub przedmioty skradzione). Ta technologia nie opiera się wyłącznie na nowych systemach biometrycznych. Łączy ona i przetwarza informacje, które są już dostępne w ramach innych danych pochodzących z szeregu różnych systemów.

Podobną aplikację zaprojektowano w ramach projektu INDECT (Inteligentny system informacyjny wspierający obserwację, wyszukiwanie i wykrywanie dla celów bezpieczeństwa obywateli w środowisku miejskim), w ramach którego łączy się technologie w celu walki z potencjalnymi aktami terroryzmu i przestępstwami zanim do nich dojdzie. Grupa robocza zdecydowanie podkreśla, że tego rodzaju zastosowanie danych biometrycznych wymagałoby odpowiedniej podstawy prawnej oraz rygorystycznego rozważenia konieczności i proporcjonalności takich środków.

4.4.4. Rozpoznawanie głosu i wspólne zastosowania

Oprócz stosowania rozpoznawania głosu jako identyfikatora biometrycznego do celów identyfikacji stosunkowo powszechnie stosuje się identyfikację szczególnych cech wzorca głosu w celu przypisania osoby mówiącej do konkretnej kategorii. Przykładem tego może być analiza odpowiedzi udzielanych przez daną osobę podczas rozmowy telefonicznej, mająca na celu określenie sposobu akcentowania wyrazów oraz wad wymowy, aby zwrócić uwagę na potencjalne przypadki oszustwa.

Z wypowiedzi opublikowanych przez producentów wynika, że dzięki wdrożeniu takiej technologii przedsiębiorstwa świadczące usługi finansowe zwiększyły poziom wykrywalności oszustw i mogły skrócić czas rozpatrywania rzeczywistych wniosków.

W przypadku zastosowań w systemie kategoryzacji czynniki ryzyka dotyczące ochrony danych są nieco inne niż w przypadku systemu identyfikacji biometrycznej ze względu na brak etapu rejestracji oraz brak potrzeby długoterminowego przechowywania wzorca biometrycznego. Jeżeli jednak rozmowa telefoniczna jest rejestrowana, co jest zwykłą praktyką w instytucjach finansowych, należy wprowadzić odpowiednie kontrole zapewniające bezpieczeństwo tych danych.

- dokładność: jeden z czynników ryzyka dotyczących ochrony danych związany z takim systemem odnosi się do poziomów wykrywalności, w szczególności wyników fałszywie dodatnich i fałszywie ujemnych, tj. ustalenia, ile osób zidentyfikowano błędnie jako oszustów lub ile wniosków stanowiących oszustwo nie zostało zidentyfikowanych? Chociaż system kategoryzacji może tolerować wyższe poziomy błędu niż systemy weryfikacji lub identyfikacji, to wciąż konieczne jest wprowadzenie odpowiednich procesów zapewniających szybkie zajęcie się przypadkami, które mogły zostać nieprawidłowo przypisane do danej kategorii.

- zgoda i przejrzystość: w odniesieniu do takich technologii można zastosować podejście sprzyjające ochronie prywatności, takie jak zadbanie o zapewnienie kontroli rozmów telefonicznych pod kątem odpowiedniości oraz o poinformowanie osób, których dane dotyczą, o przeprowadzonej procedurze. Podczas jednego z badań sytuacyjnych uznano za nieodpowiednie na potrzeby próby osoby, których pierwszym językiem nie jest język angielski, osoby z zaburzeniami słuchu lub funkcji poznawczej a także osoby nieposiadające dostępu do telefonu. Osoby zgłaszające wnioski mogły odmówić odbycia rozmowy telefonicznej i przekazać informacje w tradycyjny sposób,

ale również, w przypadku osób, których dane dotyczą, niewyrażających chęci lub niebędących w stanie uczestniczyć w takim systemie bez stawiania się w niekorzystnej sytuacji.

- dalszy cel lub dalsze cele przetwarzania: chociaż w większości przypadków technologia ta wymagałaby wdrożenia konkretnych zmian infrastrukturalnych, ponieważ sektory publiczny i prywatny konsolidują swoje infrastruktury IT, aby włączyć do nich technologie takie jak telefonia internetowa, technologie rozpoznawania głosu mogą stać się łatwiejsze w integracji bez należytego uwzględnienia obowiązków administratora danych w zakresie ochrony danych.

- odwoływalność: chociaż określona osoba fizyczna może celowo zmieniać swój głos, wzorce głosu są dość niezmienne i mogą być skuteczne w jednoznacznej identyfikacji osoby, w szczególności jeżeli nie została ona o tym poinformowana (i dlatego nie była skłonna do zmieniania swojego głosu).

- ochrona przed podszywaniem się: zarejestrowane głosy mogą być wykorzystywane do oszukania systemów rozpoznawania głosu. Techniki zapobiegania temu zjawisku obejmują pytania/odpowiedzi kontekstowe (prośbę o podanie daty lub powtórzenie rzadkich słów).

4.4.5. DNA

Udoskonalenia urządzeń stosowanych do sekwencjonowania i stwierdzania zgodności DNA oraz dostępność cenowa sprzętu do analizy DNA powodują konieczność ponownego rozważenia niektórych założeń zawartych we wcześniejszym dokumencie roboczym w sprawie biometrii (WP80).

Jednym z największych wyzwań dotyczących technologii profilowania DNA jest skrócenie czasu wymaganego do przeprowadzenia operacji sekwencjonowania i kojarzenia DNA. Ciągłe postępy, jakie przez lata czyniono dzięki badaniom naukowym oraz pracy twórców rozwiązań w dziedzinie biotechnologii, skróciły czas potrzebny do utworzenia profilu DNA z dni do godzin, a nawet części godziny.

Ukształtowanie się rynku usług internetowych opartych na DNA stanowi zagrożenie dla praw jednostki do ochrony danych, w szczególności jeżeli dana usługa wymaga przekazywania próbek danych biometrycznych oraz danych biometrycznych między różnymi państwami (w tym państwami spoza UE), wielu przetwarzających oraz braku odpowiednich zabezpieczeń w ramach przetwarzania danych genetycznych lub danych na temat zdrowia.

Istnieje duże prawdopodobieństwo, że w niedalekiej przyszłości możliwe będzie profilowanie DNA i kojarzenie próbek w czasie rzeczywistym przy użyciu urządzeń przenośnych, co stanie się punktem wyjścia dla opracowania systemów identyfikacji/uwierzytelniania biometrycznego DNA o większej dokładności w porównaniu z uwierzytelnianiem przy użyciu odcisków palców oraz rozpoznawania głosu i twarzy.

Postępy w zakresie profilowania DNA wynikają również z rosnącego zainteresowania biotechnologią ze strony rządów, sądów oraz organów ścigania na potrzeby dochodzeń. Ze względu na wiarygodność stwierdzania zgodności DNA oraz fakt, iż próbki DNA mogą być gromadzone bez wiedzy osoby, której dane dotyczą, z czasem szereg państw członkowskich utworzyło scentralizowane banki danych zawierających profile DNA osób skazanych oraz próbki pobrane w miejscach popełnienia przestępstw lub rozpoczęło inicjatywy mające na celu utworzenie takich banków.

W maju 2005 r. siedem państw członkowskich UE podpisało porozumienie znane jako konwencja z Prüm mające na celu poprawę współpracy w zakresie transgranicznych dochodzeń i transgranicznego wymiaru sprawiedliwości poprzez wymianę informacji. W porozumieniu tym ustalono nowe podstawy współpracy, ponieważ zapewnia ono sygnatariuszom określone prawa dostępu do krajowych baz danych DNA jedynie w kontekście represji (ściganie przestępstw), do danych daktyloskopijnych, danych osobowych i nieosobowych, a także do danych rejestracyjnych pojazdów. Od tego czasu do konwencji przystąpiła większa liczba państw, a zasadnicze postanowienia tego porozumienia zawarto w decyzji Rady 2008/615/WSiSW.

Na mocy tych ram prawnych szereg państw członkowskich UE posiada lub w niedługim czasie będzie posiadać działający krajowy bank danych zawierający profile DNA osób skazanych oraz dowody z miejsc popełnienia przestępstw, co budzi pewne obawy dotyczące przetwarzania tych konkretnych danych.

Jedną z najważniejszych kwestii, które wiążą się z tworzeniem banków danych DNA, jest fakt, że dane genetyczne uzyskane z próbek DNA (loci) mogą ujawniać – nie bezpośrednio na etapie gromadzenia – informacje na temat stanu zdrowia, predyspozycji do chorób lub pochodzenia etnicznego. Z tego powodu tworzenie baz danych DNA stwarza poważne ryzyko dla godności ludzkiej i praw podstawowych. Kwestię tę uwzględniono w rezolucji Rady 2009/C 296/01. Istnieją szczegółowe przepisy ograniczające analizy DNA do stref chromosomów, w których nie dochodzi do ekspresji genów, przy użyciu specjalnego zestawu markerów DNA, co do których nie wiadomo, aby dostarczały informacji na temat specyficznych cech dziedzicznych (jest on znany również jako tzw. Europejski Standardowy Zestaw).

Możliwość, że jeden z wyodrębnionych markerów zawartych w jednej z krajowych baz danych DNA może w przyszłości ujawnić pewne cechy dziedziczne lub inne dane szczególnie chronione, wymaga jednak ciągłego śledzenia zmian sytuacji w dziedzinie biologii, czego skutkiem, w przypadku takiego nieszczęśliwego zdarzenia, powinno być niezwłoczne usunięcie pewnych informacji zawartych w bazie danych. Ponadto, ponieważ w takich bazach danych DNA gromadzone są profile osób skazanych, należy ściśle ograniczyć analizy statystyczne danych, aby uniknąć profilowania na podstawie płci lub rasy.

Jeżeli chodzi o bazy danych DNA dla potrzeb policji oraz wymiaru sprawiedliwości w sprawach karnych, Europejski Trybunał Praw Człowieka orzekł, że należy dokonać wyraźnego rozróżnienia między przetwarzaniem danych osobowych i profili genetycznych osób podejrzanych oraz osób skazanych za popełnienie przestępstwa[16].

Istnieje również potencjalne ryzyko, że analizy DNA mogą być wykorzystywane do identyfikacji członków rodziny lub krewnych związanych z niewyjaśnionym przestępstwem lub osobami skazanymi, ponieważ profile DNA można wyszukiwać w bazie danych za pomocą częściowych zestawów markerów lub symboli zastępczych. W związku z tą funkcją powstaje kwestia dotycząca skutków dalszego wykorzystywania informacji uzyskanych na podstawie wyszukiwania rodzinnego.

Należy również zauważyć, że istnieją szczególne czynniki ryzyka związane z wykorzystywaniem zbiorów danych na temat genomów do celów badawczych. Grupa

[16] Europejski Trybunał Praw Człowieka, wyrok z 4.12.2008, w szczególności S. i Marper przeciwko Zjednoczonemu Królestwu (skargi nr 30562/04 i 30566/04), pkt 125.

robocza uważa, że dostęp do próbek i danych powinien być ściśle ograniczony do środowiska badawczego i dozwolony wyłącznie w celach badawczych; ponadto należy sprecyzować, w jakich okolicznościach ustalenia i wyniki badań będą ujawniane osobom fizycznym (biorąc również pod uwagę ich prawo do niewiedzy) lub będą włączane do dokumentacji medycznej.

Czynniki ryzyka w zakresie ochrony danych związane ze stosowaniem DNA jako identyfikatora biometrycznego można opisać następująco:

- dokładność: chociaż DNA charakteryzuje się bardzo wysokim poziomem dokładności, należy wziąć pod uwagę fakt, że będzie ona zależeć od liczby zanalizowanych markerów (loci). Systemy sprawdzające powinny zapewniać najwyższy poziom dokładności;

- wpływ: można uznać, że wykorzystywanie DNA w skrajnym stopniu ingeruje w prywatność osoby fizycznej. Dane genetyczne mogą ujawniać dane szczególnie chronione. Analizy statystyczne danych mogą być wykorzystywane również do celów profilowania i mogą mieć dyskryminujące skutki dla zainteresowanych osób;

- dalszy cel lub dalsze cele przetwarzania: nowe technologie pozwalają obecnie na zwiększanie ilości danych podlegających wymianie. Z tego powodu należy wyraźnie określić, kto może mieć dostęp do informacji zawartych w bazie danych DNA. Wyszukiwanie rodzinne i ukierunkowanie rasowe można uznać za nową technologię, która podważa pierwotny cel przetwarzania w ramach obecnie dostępnych baz danych DNA;

- zgoda i przejrzystość: obecnie oferuje się usługi w zakresie analiz DNA na próbkach materiału biologicznego przesyłanych pocztą (np. śliny), których wyniki udostępnia się w internecie. Niewystarczające kontrole tożsamości mogą umożliwiać osobom fizycznym lub podmiotom oddawanie próbek innych osób i w efekcie uzyskiwanie danych szczególnie chronionych, które dotyczą innych osób;

- możliwość tworzenia powiązań: z uwagi na ilość i różnorodność informacji, które można uzyskać w wyniku sekwencjonowania DNA, DNA stwarza dużą możliwość nadużyć, ponieważ wyodrębnione dane można w łatwy sposób powiązać z innymi bazami danych umożliwiającymi ustalenie profilu danej osoby. Również wyszukiwanie rodzinne umożliwia tworzenie powiązań z osobami spokrewnionymi;

- przetwarzanie danych szczególnie chronionych: DNA może ujawniać informacje na temat stanu zdrowia, predyspozycji do chorób lub pochodzenia etnicznego danej osoby. Niezwykle istotne jest zatem stosowanie zasady minimalizacji danych przy wyborze odpowiednich loci. Informacje z kodu DNA można wyodrębniać z wielu próbek przez długi okres czasu, a zatem wskazane jest dopilnowanie, aby dostęp do próbek był ściśle ograniczony do upoważnionych użytkowników i wyłącznie dla dozwolonych zastosowań;

- odwoływalność: DNA jest nieodwołalne;

- ochrona przed podszywaniem się: podszywanie się w odniesieniu do DNA jest *a priori* bardzo trudne, jednak w wielu przypadkach można bez trudu pobrać próbki DNA danej osoby (np. włosy) bez jej wiedzy.

4.4.6. Biometria podpisu odręcznego

Biometrię podpisu odręcznego można uznać za przykład nowych zastosowań tradycyjnych technologii biometrycznych. Mianem biometrii podpisu odręcznego określa się techniki biometrii behawioralnej, które pozwalają na mierzenie zachowania danej osoby wyrażającego się w dynamice podpisu odręcznego. Tradycyjne rozpoznawanie podpisu jest oparte na analizie cech statycznych lub geometrycznych widzialnego obrazu podpisu (jak podpis wygląda), natomiast biometria podpisu odręcznego odnosi się do analizy dynamicznych cech podpisu (w jaki sposób złożono podpis), przez co techniki te są często określane jako techniki „podpisu dynamicznego".

Typowymi cechami dynamicznymi mierzonymi przez system biometrii podpisu odręcznego (taki jak tablet graficzny) są: stopień nacisku, kąt nachylenia pisma, prędkość i przyspieszenie narzędzia pisarskiego, kształt liter, kierunek pisma oraz inne niepowtarzalne cechy dynamiczne. Cechy te różnią się pod względem zastosowania i znaczenia między sprzedawcami i zwykle są gromadzone przy użyciu urządzeń reagujących na kontakt. Niektóre urządzenia służące do rozpoznawania podpisów mogą dokonywać weryfikacji, łącząc zarówno cechy statyczne (widzialny obraz), jak dynamiczne (nacisk, kąt nachylenia, prędkość itp.) podpisu.

Czynniki ryzyka w zakresie ochrony danych związane z wykorzystywaniem biometrii podpisu odręcznego można opisać następująco:

- dokładność: ludzie nie zawsze składają podpis w ten sam sposób, a zatem mogliby napotykać problemy w trakcie procesu rejestracji, jak również przy weryfikacji ich tożsamości;

- wpływ: dane biometryczne oparte na cechach behawioralnych, takich jak podpis, nie muszą być niepowtarzalne w czasie i osoba, której dane dotyczą, może je zmieniać. Zmiany podpisu mogą mieć również podłoże fizjologiczne i wykluczać skuteczną weryfikację, powodując konieczność wprowadzenia alternatywnych procedur weryfikacji tożsamości osób;

- ochrona przed podszywaniem się: o ile obraz graficzny tradycyjnego podpisu może zostać w łatwy sposób powielony i sfałszowany przez wyszkoloną osobę, przy pomocy fotokopiarki lub komputerowego programu graficznego, podpis dynamiczny jest bardziej bezpieczny, ponieważ podczas procesu weryfikacji sprawdza się również cechy dynamiczne, które są złożone i niepowtarzalne dla charakteru pisma danej osoby.

5. Ogólne wytyczne, zalecenia sektorowe oraz środki techniczne i organizacyjne

Wdrażanie systemu biometrycznego opiera się na współpracy szeregu podmiotów:

- producentów: projektowanie i badanie czujników biometrycznych oraz określenie skuteczności technologii biometrycznych;
- integratorów: projektowanie produktu końcowego, który zostanie sprzedany klientowi – wybierają technologię biometryczną i określają częściowo cele systemu (wybierając klientów docelowych);
- sprzedawców: sprzedaż produktu końcowego klientowi; zasadniczo informują klienta o skuteczności, czynnikach ryzyka i ewentualnie o ramach prawnych;
- instalatorów: zainstalowanie produktu u klienta;

- klientów: podjęcie decyzji o zakupie systemu biometrycznego – określają cel i środki przetwarzania i w związku z tym są administratorami danych;
- osób, których dane dotyczą: dostarczanie danych biometrycznych do sytemu.

Niektóre podmioty pełnią jedną lub kilka z opisanych wyżej ról. Każda z tych ról wiąże się z obowiązkiem zapewnienia stosowania systemów biometrycznych w sposób sprzyjający ochronie prywatności: przykładowo instalator nie może wdrożyć funkcji bezpieczeństwa zdefiniowanej przez integratora.

5.1. Zasady ogólne.

W przypadku danych biometrycznych bezpieczeństwo powinno mieć pierwszorzędne znaczenie, ponieważ dane biometryczne są nieodwołalne: w związku z tym naruszenie dotyczące danych biometrycznych zagraża dalszemu bezpiecznemu stosowaniu tych danych jako identyfikatora oraz stanowi zagrożenie dla prawa do ochrony zainteresowanych osób, w przypadku których nie ma możliwości ograniczenia skutków naruszenia.

Ryzyko rośnie wraz z liczbą aplikacji stosujących takie dane (w szczególności ryzyko naruszeń oraz nadużyć). Im większa jest ilość wykorzystywanych danych biometrycznych, tym większe jest prawdopodobieństwo kradzieży tych danych.

Grupa robocza dostrzega panującą obecnie tendencję polegającą na zezwalaniu na zdalny dostęp do systemów biometrycznych, na przykład interfejsy udostępniane w internecie. Tendencja ta powoduje nowe problemy dotyczące bezpieczeństwa, z których wiele jest już dobrze znanych w branży IT. We wdrażanie takiego systemu, już na etapie projektowania, należy zaangażować odpowiedni personel techniczny ds. bezpieczeństwa z branży IT.

Grupa robocza zaleca wysoki poziom ochrony technicznej przy przetwarzaniu danych biometrycznych z wykorzystaniem najnowszych możliwości technicznych. W tym kontekście grupa robocza zaleca postępowanie zgodnie z normami sektorowymi w odniesieniu do ochrony systemów, w których przetwarzane są informacje biometryczne.

5.2. Ochrona prywatności w fazie projektowania (*privacy by design*)

Ochrona prywatności w fazie projektowania jest koncepcją polegającą na aktywnym uwzględnianiu prywatności w samej technologii.

W kontekście systemów biometrycznych ochrona prywatności w fazie projektowania dotyczy całego łańcucha wartości systemów biometrycznych:

- producenci powinni wdrożyć zasady ochrony prywatności w fazie projektowania przy projektowaniu nowych technologii i czujników: może to obejmować automatyczne usuwanie nieprzetworzonych danych po obliczeniu wzorca lub stosowanie szyfrowania w przypadku przechowywania danych biometrycznych (zarówno w centralnej bazie danych, jak i na karcie elektronicznej). Producenci powinni skoncentrować się również na opracowywaniu technologii biometrycznych, które sprzyjają ochronie prywatności;
- integratorzy i sprzedawcy powinni również wdrożyć zasady ochrony prywatności w fazie projektowania przy definiowaniu produktu końcowego, który zostanie sprzedany, wybierając technologie sprzyjające ochronie prywatności i dodając do produktu końcowego środki bezpieczeństwa, takie jak decentralizacja bazy danych;
- klienci (potencjalni administratorzy danych) powinni stosować zasady ochrony prywatności w fazie projektowania za każdym razem, kiedy zamawiają konkretny system biometryczny lub definiują cechy techniczne systemu. W tym przypadku producenci i integratorzy powinni oferować pewną elastyczność w ramach swojego

produktu, aby zachować zgodność z zasadami proporcjonalności, celowości, minimalizacji danych oraz bezpieczeństwa.

Zasady te zostały już z powodzeniem wdrożone w niektórych urządzeniach biometrycznych: niektórzy producenci wyposażyli konkretny czytnik biometryczny w funkcje szyfrowania oraz wyłączniki zabezpieczające przed wyciąganiem i manipulowaniem, aby zapobiec nieuprawnionemu dostępowi do danych biometrycznych.

Grupa robocza zaleca, aby systemy biometryczne były projektowane zgodnie z formalnymi „cyklami rozwoju", co obejmuje następujące etapy:

1. określenie wymogów na podstawie analizy ryzyka lub specjalnej oceny wpływu na prywatność;
2. opis i uzasadnienie sposobu, w jaki dany projekt spełnia wymogi;
3. walidacja za pomocą testów funkcjonalnych i testów bezpieczeństwa;
4. weryfikacja zgodności końcowego projektu z ramami regulacyjnymi.

Grupa robocza zachęca do opracowania definicji systemów certyfikacji, które mogłyby zapewnić wdrażanie ochrony prywatności w fazie projektowania oraz poprawę znajdujących się w posiadaniu administratorów danych informacji na temat ryzyka dotyczącego ochrony danych związanego z systemami biometrycznymi.

5.3. Ramy oceny wpływu na prywatność

5.3.1. Zasady ogólne

Ocena wpływu na prywatność jest procesem, w ramach którego dany podmiot przeprowadza ocenę ryzyka związanego z przetwarzaniem danych osobowych oraz określa dodatkowe środki służące ograniczeniu tego ryzyka. Przykładowo, w przypadku technologii radiowej (RFID) grupa robocza ustaliła, że podmiot, który definiuje aplikację ponosi odpowiedzialność za przeprowadzenie oceny wpływu na prywatność. Podmiotem tym może być administrator danych lub dostawca, który projektuje aplikację RFID.

Ze względu na szczególne czynniki ryzyka związane ze stosowaniem danych biometrycznych grupa robocza zaleca, aby podmiot definiujący cel i środki stosowane w danym urządzeniu, przeprowadzał oceny wpływu na prywatność jako integralny element fazy projektowania systemów, w których stosuje się ten rodzaj danych. Podmiotem tym może być producent, integrator lub klient końcowy.

W ocenie wpływu na prywatność należy wziąć pod uwagę:

- charakter gromadzonych informacji;
- cel gromadzonych informacji;
- dokładność systemu, zakładając, że istotne dla danej osoby decyzje mogą wynikać ze zgodności/z niezgodności wzorca biometrycznego;
- podstawę prawną i zgodność z prawem; czy jest wymagana zgoda?
- dostęp do urządzenia oraz wewnętrzną i zewnętrzną wymianę informacji prowadzoną przez administratora danych, która będzie miała wpływ na techniki bezpieczeństwa oraz procedury ochrony danych osobowych przed nieuprawnionym dostępem;
- podjęte już środki, które w mniejszym stopniu naruszają prywatność. Czy istnieje alternatywna procedura do urządzenia biometrycznego (na przykład żądanie okazania dowodu tożsamości)?
- podjęte decyzje dotyczące czasu zatrzymywania i usuwania danych. Jaki jest odpowiedni okres czasu? Czy wszystkie dane są gromadzone przez

taki sam okres czasu? Czy istnieje mechanizm automatycznego podejmowania decyzji oraz odpowiedni proces awaryjny?
- prawa osób, których dane dotyczą.

Oceny wpływu na prywatność nie powinny skupiać się wyłącznie na identyfikacji ryzyka, powinny również zapewniać odpowiednie środki ochrony danych oraz określać, w jaki sposób administrator danych wypracował odpowiednie rozwiązania służące ograniczeniu ryzyka dotyczącego ochrony danych określonego w poprzedniej części.

Jeżeli ocenę wpływu na prywatność przeprowadził producent lub integrator, wdrożenie systemu biometrycznego może wymagać również przeprowadzenia dodatkowej oceny uwzględniającej specyficzne cechy administratora danych. Przykładowo, jeżeli system biometryczny jest zintegrowany z systemem informacyjnym klienta, klient ten powinien przeprowadzić dodatkową ocenę wpływu na prywatność, w ramach której przeanalizuje własne środki i procedury bezpieczeństwa informatycznego.

5.3.2. Specyfika danych biometrycznych

Dane biometryczne wymagają szczególnej uwagi, ponieważ jednoznacznie identyfikują osobę fizyczną za pomocą jej niepowtarzalnych cech behawioralnych lub psychologicznych.

Z tego powodu ocena wpływu na prywatność powinna mieć na celu ocenę możliwości uniknięcia trzech wymienionych niżej czynników ryzyka lub ich znacznego ograniczenia przez analizowany w ramach tej oceny system.

Pierwszym czynnikiem ryzyka jest oszustwo dotyczące tożsamości, w szczególności w przypadku identyfikacji i uwierzytelniania. Urządzenie biometryczne nie powinno dać się wprowadzić w błąd podczas próby podszycia się i powinno gwarantować, że osoba podejmująca próbę skojarzenia danych jest rzeczywiście osobą zarejestrowaną w systemie. Wydaje się, że zagrożenie to ma mniejsze znaczenie w przypadku danych biometrycznych, których nie można gromadzić bez wiedzy osoby, której dane dotyczą, takich jak układ żył[17]. Jest to jednak poważny problem w przypadku urządzeń rozpoznających odciski palców lub twarze. Odciski palców pozostawia się wszędzie, po prostu dotykając dowolnego przedmiotu. Twarz można również sfotografować bez wiedzy zainteresowanej osoby.

Drugim czynnikiem ryzyka jest zmiana celu przed samego administratora danych lub przez osobę trzecią, w tym przez organy ścigania. To powszechne zagrożenie dotyczące danych osobowych nabiera kluczowego znaczenia w przypadku wykorzystywania danych biometrycznych. Producenci powinni podjąć wszelkie środki bezpieczeństwa, aby uniknąć jakichkolwiek przypadków nieodpowiedniego wykorzystywania danych oraz upewnić się, że wszelkie dane, które nie są już potrzebne do celów przetwarzania, są natychmiast usuwane.

Podobnie jak w przypadku innych danych, administrator danych nie może przetwarzać ani rejestrować przetwarzanych lub przechowywanych zgodnie z prawem danych biometrycznych lub źródeł identyfikatorów biometrycznych w żadnym nowym lub innym celu, chyba że istnieje nowa uzasadniona podstawa dla takiego nowego przetwarzania tych danych.

[17] Nawet jeśli trudno jest przewidzieć, jakie ataki w odniesieniu do technologii dotyczącej układu żył będą możliwe w nadchodzących latach, jeżeli technologia ta stanie się bardziej powszechna.

Trzecim czynnikiem ryzyka jest naruszenie ochrony danych, które w kontekście danych biometrycznych wymaga podjęcia specjalnych działań w zależności od tego, jakiego rodzaju danych ochronę naruszono. W przypadku stosowania systemu, który tworzy dane biometryczne w oparciu o algorytm przekształcający wzorzec biometryczny na określony kod, a dane biometryczne lub algorytm skradziono lub naruszono, wówczas należy je wymienić. Jeżeli naruszenie ochrony danych wiąże się z utratą bezpośrednio zidentyfikowanych danych biometrycznych, które są bardzo zbliżone do źródła danych biometrycznych, takich jak fotografie twarzy czy odciski palców, wówczas należy szczegółowo powiadomić zainteresowaną osobę, aby mogła obronić się w przypadku ewentualnego przyszłego zdarzenia, kiedy takie naruszone dane biometryczne mogą być ponownie wykorzystane przeciwko tej osobie jako dowód.

5.4. Środki techniczne i organizacyjne

Z uwagi na charakter danych biometrycznych, ich przetwarzanie wymaga szczególnych środków technicznych i organizacyjnych oraz środków ostrożności zapobiegających niekorzystnym skutkom dla osoby, której dane dotyczą, w przypadku naruszenia danych, w szczególności ze względu na ryzyko niezgodnego z prawem postępowania prowadzącego do niedozwolonego „odtworzenia" identyfikatora biometrycznego na podstawie wzorca referencyjnego, powiązania danych z różnymi bazami danych, ich dalszego „wykorzystywania" bez wiedzy osoby, której dane dotyczą, w celach niezgodnych z pierwotnymi celami lub możliwość wykorzystania niektórych danych biometrycznych w celu ujawnienia informacji na temat rasy lub stanu zdrowia osób, których dane dotyczą.

5.4.1. Środki techniczne

- *Stosowanie wzorców biometrycznych*

W miarę możliwości dane biometryczne powinny być przechowywane jako wzorce biometryczne.

Wzorce należy wyodrębniać w sposób właściwy dla danego systemu biometrycznego; nie powinny być one wykorzystywane przez innych administratorów danych podobnych systemów, aby zagwarantować, że daną osobę można zidentyfikować tylko w systemach biometrycznych posiadających podstawę prawną do takiego działania.

- *Przechowywanie na urządzeniu osobistym a przechowywanie scentralizowane*

W każdym przypadku, w którym dozwolone jest przetwarzanie danych biometrycznych, należy unikać scentralizowanego przechowywania osobowych informacji biometrycznych.

W szczególności w odniesieniu do weryfikacji grupa robocza uważa, że wskazane jest, aby systemy biometryczne działały w oparciu o odczyty danych biometrycznych przechowywanych jako zaszyfrowane wzorce na nośnikach znajdujących się w wyłącznym posiadaniu zainteresowanych osób, których dane dotyczą (np. na kartach elektronicznych lub podobnych urządzeniach). Ich identyfikatory biometryczne można porównać ze wzorcem lub wzorcami przechowywanymi na karcie lub urządzeniu za pomocą standardowych procedur porównywania, które wdrożono bezpośrednio na danej karcie lub urządzeniu, co powinno pozwolić uniknąć, co do zasady i w miarę możliwości, tworzenia baz danych zawierających informacje biometryczne. Co więcej, obecnie w przypadku utraty lub zagubienia karty lub urządzenia istnieje ograniczone ryzyko niewłaściwego wykorzystania zawartych na nich informacji biometrycznych. Aby ograniczyć ryzyko kradzieży tożsamości, na takich urządzeniach należy przechowywać tylko ograniczone dane identyfikacyjne osoby, której dane dotyczą.

W szczególnych celach i wobec obiektywnych potrzeb można jednak uznać dopuszczalność istnienia scentralizowanej bazy danych zawierającej informacje lub wzorce biometryczne. Wykorzystywany system biometryczny oraz wybrane środki bezpieczeństwa powinny ograniczać wymienione czynniki ryzyka i zapewniać brak możliwości ponownego wykorzystania przedmiotowych danych do dalszych celów lub co najmniej możliwość wykrycia takiego działania. Aby zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, modyfikowaniu lub usuwaniu danych biometrycznych, należy stosować mechanizmy oparte na technologiach kryptograficznych.

Jeżeli dane biometryczne są przechowywane na urządzeniu, nad którym osoba, której dane dotyczą, ma fizyczną kontrolę, należy zastosować specjalny kod szyfrujący do urządzeń odczytujących jako skuteczne zabezpieczenie chroniące te dane przed nieuprawnionym dostępem. Ponadto takie zdecentralizowane systemy zapewniają lepszą ochronę danych biometrycznych w fazie projektowania, ponieważ osoba, której dane dotyczą, zachowuje fizyczną kontrolę nad swoimi danymi biometrycznymi i nie ma jednego punktu, który można przyjąć za cel lub wykorzystać.

Grupa robocza podkreśla również, że pojęcie scentralizowanej bazy danych obejmuje szereg realizacji technicznych, od przechowywania na czytniku po bazę danych w obrębie sieci.

- *Odnawialność i odwoływalność*

Ponieważ nie można zmienić źródła danych biometrycznych, systemy biometryczne, których celem jest ustalenie elementów potwierdzających tożsamość, muszą być zaprojektowane w taki sposób, aby proces rejestracji oraz przetwarzanie danych biometrycznych umożliwiały wyodrębnienie wielu niezależnych wzorców biometrycznych z jednego źródła, aby można było je zastąpić w przypadku naruszenia ochrony danych lub rozwoju technologii.

Systemy biometryczne powinny być zaprojektowane w sposób umożliwiający odwołanie elementów potwierdzających tożsamość w celu ich odnowienia lub trwałego usunięcia, np. w przypadku cofnięcia zgody[18].

- *Postać zaszyfrowana*

Jeżeli chodzi o kwestię bezpieczeństwa, należy przyjąć odpowiednie środki zabezpieczające dane przechowywane i przetwarzane w systemie biometrycznym: informacje biometryczne muszą być zawsze przechowywane w postaci zaszyfrowanej. Należy określić główne ramy zarządzania w celu zapewnienia dostępu do kluczy deszyfrujących tylko wtedy, gdy jest to niezbędne.

Z uwagi na powszechne korzystanie z publicznych i prywatnych baz danych zawierających informacje biometryczne oraz coraz większą interoperacyjność różnych systemów wykorzystujących biometrię, należy preferować wykorzystywanie konkretnych technologii

[18] Przykładowo technologia TURBINE, która ma na celu ochronę wzorca biometrycznego dzięki kryptograficznemu przekształceniu informacji daktyloskopijnych w nieodwracalny klucz, który umożliwia dopasowanie poprzez porównanie bitowe. Przekształcone dane biometryczne uważa się za nieodwracalne w stosunku do próbek danych biometrycznych i oryginalnych wzorców biometrycznych. Ponadto, aby zwiększyć zaufanie użytkownika, klucz ten będzie również odwoływalny, tj. można wygenerować nowy, niezależny klucz, aby ponownie wyemitować identyfikatory biometryczne. Zob. również: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf.

lub formatów danych, które uniemożliwiają łączenie baz danych biometrycznych oraz niekontrolowane ujawnianie danych.

- *Ochrona przed podszywaniem się*

Aby utrzymać wiarygodność systemu biometrycznego i zapobiec oszustwom dotyczącym tożsamości, producent musi wdrożyć systemy, których celem jest stwierdzenie, czy dane biometryczne są zarówno prawdziwe, jak i nadal związane z osobą fizyczną. W odniesieniu do rozpoznawania twarzy decydujące znaczenie może mieć dopilnowanie, aby dana twarz była prawdziwą twarzą, a nie, na przykład, fotografią umieszczoną na głowie oszusta.

- *Szyfrowanie i deszyfrowanie danych biometrycznych*

Szyfrowanie danych biometrycznych jest techniką, w której jako element algorytmu szyfrowania i deszyfrowania wykorzystuje się cechy biometryczne. W tym przypadku fragment danych biometrycznych jest wykorzystywany zasadniczo jako klucz w celu zaszyfrowania identyfikatora potrzebnego dla danej usługi.

System ten ma wiele zalet[19]. Dzięki niemu nie przechowuje się identyfikatora ani danych biometrycznych, a jedynie wynik identyfikatora zaszyfrowanego w danych biometrycznych. Ponadto dane osobowe są odwołalne, ponieważ istnieje możliwość utworzenia innego identyfikatora, który również można zabezpieczyć za pomocą szyfrowania danych biometrycznych. System ten jest również bardziej bezpieczny i łatwiejszy w użytkowaniu dla zainteresowanej osoby: rozwiązuje problem zapamiętywania długich i złożonych haseł.

Problem dotyczący kryptografii, który należy rozwiązać, nie jest jednak łatwy, ponieważ szyfrowanie i deszyfrowanie nie pozwalają na żadne zmiany klucza, podczas gdy identyfikator biometryczny daje różne wzorce, co może powodować zmiany w wyodrębnionym kluczu. Dlatego system musi być w stanie obliczyć ten sam klucz na podstawie nieco innych danych biometrycznych bez zwiększania wskaźnika błędnej akceptacji.

Grupa robocza podziela opinię, że technologia szyfrowania danych biometrycznych stanowi obszar o dużym potencjale dla badań i uzyskała wystarczający stopień rozwoju do szerszego uwzględnienia w polityce publicznej, opracowania prototypu oraz rozważenia pod katem zastosowań.

- *Automatyczne mechanizmy usuwania danych*

Aby zapobiec przechowywaniu informacji biometrycznych dłużej niż jest to konieczne do celów, w których je zgromadzono lub następnie przetworzono, należy wdrożyć odpowiednie mechanizmy automatycznego usuwania danych, również jeżeli okres zatrzymywania może zostać zgodnie z prawem wydłużony, zapewniając szybkie usunięcie danych osobowych, które stają niepotrzebne dla działania systemu biometrycznego.

W przypadku stosowania zintegrowanego przechowywania na czytniku, producenci mogą również wdrożyć przechowywanie wzorców biometrycznych w pamięci ulotnej, która gwarantuje usunięcie danych po odłączeniu czytnika. W razie sprzedaży lub odinstalowania czytnika nie pozostają więc na nim żadne bazy danych biometrycznych. Można również stosować wyłączniki zabezpieczające przed wyciąganiem, automatycznie usuwające dane w przypadku próby kradzieży czytnika.

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

- *Duże bazy danych biometrycznych oraz bazy danych stanowiące „słabe ogniwo”*

Niektóre państwa korzystają z dużych baz danych biometrycznych przede wszystkim w dwóch celach: aby pomagać w prowadzeniu dochodzeń oraz aby zabezpieczyć dostarczanie dokumentów tożsamości (paszportów, dowodów tożsamości, praw jazdy). W bazach danych wykorzystywanych na potrzeby dochodzeń na ogół gromadzi się informacje na temat przestępców i osób podejrzanych i takie bazy danych muszą umożliwiać identyfikację danej osoby za pomocą danych biometrycznych. Natomiast bazy danych wykorzystywane w celu zwalczania oszustw dotyczących tożsamości zawierają dane biometryczne całej populacji i powinny być wykorzystywane wyłącznie do uwierzytelnienia osoby (na przykład, jeżeli dana osoba utraciła swoje dokumenty lub zniszczyła układ scalony stanowiący zabezpieczenie paszportu, w którym są przechowywane dane biometryczne).

W przypadku wykorzystywania bazy danych na potrzeby walki z oszustwem dotyczącym tożsamości grupa robocza uważa, że należy wdrożyć środki techniczne w celu uniknięcia jakiekolwiek zmiany celu. Po pierwsze zasada minimalizacji danych wymaga, aby gromadzone były wyłącznie dane niezbędne do uwierzytelnienia danej osoby. Przykładowo uważa się, że porównanie linii papilarnych dwóch palców jest wystarczająco dokładne, aby uwierzytelnić daną osobę.

Ponadto administratorzy danych mogą wykorzystywać bazy danych stanowiące „słabe ogniwo” w przypadku, gdy z daną osobą nie jest powiązany pojedynczy składnik danych biometrycznych, ale raczej grupa w ramach zbioru danych biometrycznych. Projekt baz danych powinien gwarantować uwierzytelnienie osoby z bardzo dużym prawdopodobieństwem (na przykład 99,9 %, co wystarczy, aby zniechęcić oszustów) oraz zapewnić brak możliwości wykorzystania bazy danych do identyfikacji (ponieważ jeden zbiór danych biometrycznych odpowiada dużej liczbie osób).

Grupa robocza wspiera stosowanie takich systemów w przypadku, gdy duże bazy danych biometrycznych są wykorzystywane do walki z oszustwem dotyczącym tożsamości.

Przykład: środki techniczne dla systemów uwierzytelniania
Źródło danych biometrycznych jest niepowtarzalne i potencjalnie przez całe życie powiązane z osobą, której dane dotyczą. Jeżeli jest wykorzystywane jako podstawa dla systemu uwierzytelniania, należy pamiętać o tym, że nie może być ono zmieniane, podczas gdy w przypadku powszechnych technologii uwierzytelniania, które zwykle wymagają „znajomości lub posiadania” elementu uwierzytelniającego (na przykład identyfikatora użytkownika, hasła), zmiana tego elementu jest zawsze możliwa. Dlatego w systemach wykorzystujących uwierzytelnianie biometryczne należy wdrożyć specjalne zabezpieczenia chroniące związek między identyfikatorem biometrycznym a innymi danymi potwierdzającymi tożsamość:
- dane z wzorców nie powinny być przechowywane centralnie, ponieważ bezpieczeństwo przechowywania danych biometrycznych ma kluczowe znaczenie w kontekście ogólnego bezpieczeństwa systemu biometrycznego. Należy preferować przechowywanie rozproszone (na przykład na karcie elektronicznej). W takim przypadku zarówno źródło danych, jak i wzorzec są przenoszone przez osobę, której dane dotyczą;
- należy zapewnić ochronę przechowywania i transmisji danych biometrycznych przed przechwyceniem, niedozwolonym ujawnieniem i modyfikacją, za pomocą odpowiednich technologii kryptograficznych;

- niektóre rodzaje danych biometrycznych nie są tajne (na przykład twarz) i nie mogą zostać zabezpieczone, zablokowane ani zmienione w następstwie naruszenia ochrony danych, ich ujawnienia lub w przypadkach wykorzystania niezgodnie z przeznaczeniem. W konsekwencji uwierzytelnianie powinno odbywać się w połączeniu z innymi elementami uwierzytelniającymi, które można zabezpieczyć lub zmienić.

5.4.2. Środki organizacyjne

Aby zagwarantować ochronę danych, należy zaplanować i wdrożyć środki organizacyjne. Przykładowo administrator danych musi ustanowić przejrzystą procedurę określającą, kto może mieć dostęp do informacji zawartych w systemie, czy dostęp jest częściowy czy pełny i z jakich powodów. Wszystkie działania muszą być kontrolowane.

Grupa robocza zauważa, że możliwy jest outsourcing zewnętrznym dostawcom usług, również w przypadku wniosków wizowych (art. 13 i 43 rozporządzenia (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiającego Wspólnotowy Kodeks Wizowy), i staje się on coraz bardziej popularny ze względu na częstsze korzystanie z tzw. *cloud storage* (przechowywanie danych w chmurze).

W tym przypadku administrator danych musi określić szczegółową politykę kontrolowania swoich wykonawców, na przykład poprzez niezapowiedziane kontrole, oraz wymagać gwarancji dotyczących pracowników, procedury dotyczącej praw jednostki itp.

Sporządzono w Brukseli dnia 27 kwietnia 2012 r.

W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM