POLSKIE
TOWARZYSTWO
KRYMINALISTYCZNE

Magdalena Tomaszewska-Michalak

Implementacja norm prawa unijnego w zakresie zabezpieczeń biometrycznych do polskiego porządku prawnego. Perspektywa historyczna

Tekst opracowany na podstawie pracy magisterskiej

Warszawa 2020

Recenzja
prof. dr hab. Piotr Girdwoyń

Redakcja techniczna
Mieczysław Goc
Kacper Choromański

Korekta przypisów
Anna Kaniewska

Skład komputerowy, projekt graficzny
Mieczysław Goc
Kacper Choromański

ISBN: 978-83-926115-1-6

Wydawca
Polskie Towarzystwo Kryminalistyczne
ul. Zgoda 11 lok. 300
00-018 Warszawa
www.kryminalistyka.pl

Monografia jest publikowana na warunkach licencji
Creative Commons Attribution Non Commercial 4.0 International. (CC BY-NC 4.0)

Spis treści

1. Wstęp ... 3
2. Rys historyczny ... 5
2.1. Berillionage, odciski palców ... 5
2.2. Badanie tęczówki ... 6
2.3. Geometria kształtu twarzy ... 6
2.4. Identyfikacja na podstawie głosu ... 7
2.5. Identyfikacja na podstawie podpisu ... 7
3. Techniki biometryczne ... 8
3.1. Weryfikacja a identyfikacja ... 8
3.2. Poszczególne metody ... 9
3.2.1. Badanie linii papilarnych ... 9
3.2.2. Badanie geometrii dłoni ... 11
3.2.3. Analiza siatki naczyń krwionośnych ... 12
3.2.4. Badanie geometrii twarzy ... 13
3.2.5. Badanie tęczówki oka ... 15
3.2.6. Badanie podpisu ... 16
3.2.7. Badanie parametrów głosu ... 17
3.2.8. Inne metody ... 18
4. Ustawodawstwo w zakresie zabezpieczeń biometrycznych ... 19
4.1. Prawo Unii Europejskiej ... 19
4.1.1. Konkretne wykorzystanie biometrii w Unii Europejskiej ... 30
4.1.2. EURODAC ... 30
4.1.3. SIS II ... 35
4.1.4. VIS ... 37
4.2. Ustawodawstwo polskie ... 41
4.2.1. Wdrażanie SIS II, VIS oraz EURODAC ... 46
5. Podsumowanie ... 50
Bibliografia ... 58

1. Wstęp

Termin biometria jest połączeniem dwóch słów wywodzących się z języka greckiego. *Bios* oznacza życie, natomiast *metron* odpowiada polskiemu słowu *mierzyć.* Biometria jest nauką, która wykorzystując zasady statystyki matematycznej, opisuje zmienność cech populacji organizmów żywych. Wyniki pomiarów biometrycznych wykorzystywane są w wielu różnych dziedzinach życia, jak np. w medycynie, genetyce, hodowli czy antropologii. Biometria jest również techniką wykorzystywaną w celu dokonywania pomiarów istot żywych[1]. W tym kontekście, obecnie biometria stała się popularna jako metoda rozpoznawania osób na podstawie ich cech fizycznych. W licznych opracowaniach można spotkać podział biometrii na fizyczno - biologiczną oraz behawioralną. Kryterium tego podziału jest rodzaj cech, które wykorzystuje się do identyfikacji lub weryfikacji jednostki. W pierwszym przypadku są to właściwości biologiczno- fizyczne danej osoby (możemy tu wyróżnić identyfikację lub weryfikację, np. na podstawie linii papilarnych, geometrii dłoni, geometrii ucha, geometrii twarzy, badania siatkówki oka), w drugim pewne cechy, które możemy wyczytać z zachowania interesującego nas podmiotu (do tej kategorii należy chociażby badanie chodu konkretnej osoby czy też badanie dynamiki i sposobu naciskania klawiatury podczas pisania na komputerze). Chociaż współczesna biometria zawdzięcza swój rozwój nowoczesnym osiągnięciom w dziedzinie techniki komputerowej, to idea, na której opiera się identyfikacja osoby na podstawie jej cech, sięga czasów starożytnych. Jedną z najstarszych metod, za pomocą której rozpoznawano daną osobę było ustalanie jej tożsamości na podstawie wizerunku. Metoda ta opierała się na porównaniu konkretnego obrazu z obrazem znajdującym się w pamięci osoby dokonującej identyfikacji. W małych społecznościach, dokonywanie tego typu sprawdzania tożsamości było z pewnością wystarczające do odróżnienia członka własnej wspólnoty od obcej jednostki. Problem jednakże pojawił się w momencie, gdy liczba osób we wspólnocie zaczęła wzrastać, a podróżowanie stało się dużo prostsze. Ludzka pamięć stała się w takich okolicznościach zawodna i powstała potrzeba znalezienia innych sposobów, za pomocą których można zidentyfikować jednostki. Już w starożytności możemy zauważyć potrzebę poszukiwania metod użytecznych do identyfikacji człowieka, innych niż opartych na ludzkiej pamięci. I tak z literatury możemy się dowiedzieć, że odciski palców były używane jako

[1] K. Krassowski, I. Sołtyszewski, *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252.

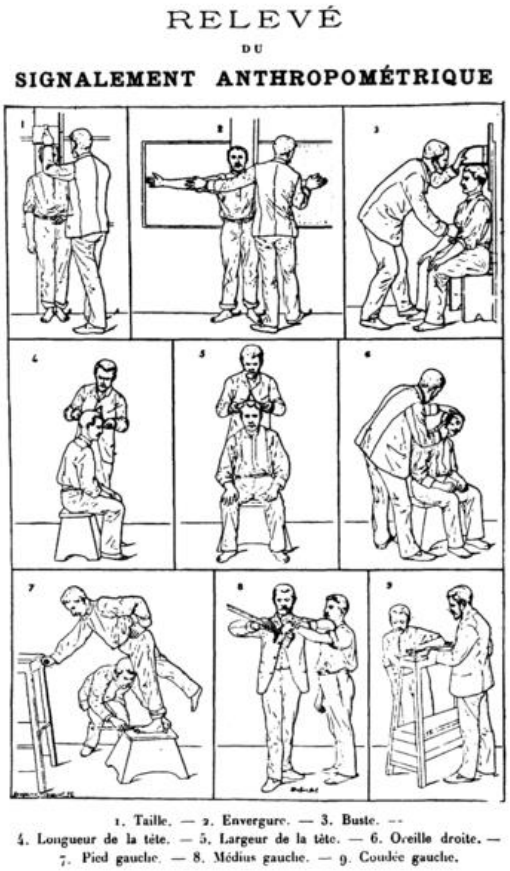
identyfikator danej osoby np. w Chinach[2]. Były to jednakże przypadki odosobnione i tak naprawdę dopiero w XIX wiecznej Europie możemy mówić o szybkim rozwoju metod wykorzystujących odbitki linii papilarnych w celu identyfikacji tożsamości danej osoby.

[2] T. Szczepański *Daktyloskopia na przestrzeni wieków*, „Problemy Kryminalistyki" 2019, nr 303.

2. Rys historyczny

2.1. Berillionage, odciski palców

Właściwie pierwszą próbą stworzenia katalogu pozwalającego na identyfikacje osoby nie jest ta podjęta w dziedzinie odcisków palców, ale zainteresowanie się problematyką identyfikacji przez Francuza Alphonse'a Berilliona. Bertillion opracował system identyfikacji zwany antropometrią. „Bertillionage" (bo tak została nazwana metoda wprowadzona w XIX wieku we Francji) polegał na bardzo precyzyjnym pomiarze długości poszczególnych kości człowieka. Bertillion zauważył bowiem, że pewne części ludzkiego ciała pozostają względnie niezmienne podczas całego dorosłego życia człowieka. Precyzyjnie mierząc, a następnie zapisując uzyskane pomiary doprowadził do stworzenia kartoteki, która przez wiele lat pomagała francuskiej policji w identyfikacji osób, które w przeszłości popełniły już jakieś przestępstwo. System Bertillona, aczkolwiek bardzo pomocny w ówczesnych czasach, wymagał jednak od osoby katalogującej ogromnej precyzji, zaangażowania i czasu. Dlatego też, gdy w 1892 roku, Sir Francis Galton opracował system klasyfikacji odcisków palców, a w cztery lata później, Sir Edward Henry udoskonalił pracę F. Galtona, oparta na antropometrii metoda A. Bertilliona, została wyparta przez łatwiejszą w użyciu i mniej czasochłonną weryfikację tożsamości za pomocą badania linii papilarnych. Identyfikacja oraz weryfikacja za pomocą badania linii papilarnych jest wykorzystywana do dziś, a czytniki linii papilarnych w urządzeniach elektronicznych są obecnie jednym z najczęściej spotykanych zabezpieczeń biometrycznych.



Ryc. 1. Ilustracja obrazująca sposób mierzenia człowieka przy zastosowaniu Bertillionage'u (źródło: ilustracja pochodz z książki A.Bertillion „Idetification antrophopétrique")

2.2. Badanie tęczówki

Rozwój innych metod identyfikacji człowieka zaczął się około 40 lat później. W 1936 roku Frank Burch stwierdził, że można wykorzystać badanie tęczówki oka w celu identyfikacji osoby. Pomysł Burcha zyskał jednak uznanie dopiero w latach 80 – tych XX wieku, kiedy to dwaj okuliści: Leonard Flom i Aran Safir postawili tezę stwierdzającą, że tęczówka oka jest jak odciski palców – inna u każdego człowieka. Wychodząc z tego założenia Flom i Safir zwrócili się w 1989 roku do wykładającego wówczas na harwardzkim Uniwersytecie, Johna Daugmana, aby ten opracował algorytm niezbędny do przeprowadzenia identyfikacji tęczówki oka. W 1994r. Daugman opatentował algorytm, który od tego czasu stał się podstawą do tworzenia wszelkiego rodzaju urządzeń posługujących się badaniem tęczówki oka w celu identyfikacji[3]. W 2011 roku wygasł patent na rozpoznawanie tęczówki za pomocą algorytmu Johna Daugmana, co otworzyło możliwość rozwoju w dziedzinie porównywania biometrycznego na podstawie tęczówki oka[4].

2.3. Geometria kształtu twarzy

W zakresie identyfikacji na podstawie geometrii kształtu twarzy wspomnieć należy nazwisko Woodrowa W. Bledsoe'a, który w latach 60' XX wieku opracował technikę zwaną „pół automatyczną maszyną do rozpoznawania ludzkiej twarzy". Technika polegała na fotografowaniu poszczególnych części twarzy (jak nos, uszy, usta czy oczy), które później umieszczało się w przeznaczonej do tego bazie danych. Następnie wprowadzano do systemu zdjęcie nieznanej osoby, a ten wydobywał fotografię najbardziej zbliżoną do wizerunku porównawczego (podstawą działania urządzenia stworzonego przez Bledsoe'a było porównywanie odległości pomiędzy sfotografowanymi częściami twarzy)[5]. W latach 70' podejmowane były kroki w celu większego zautomatyzowania systemów służących do identyfikacji w tej dziedzinie, jednakże dopiero pod koniec lat 80 - tych udało się stworzyć w pełni zautomatyzowany system rozpoznawania ludzkiej twarzy. W 1988 Kirby i Sirovich opracowali wzór matematyczny, na którym opierały się współczesne urządzenia służące do identyfikacji na podstawie kształtu twarzy[6].

---

[4] https://www.biometricupdate.com/201206/explainer-iris-recognition (dostęp 11.11.2020).
[5] M. Ballantyne, R. Boyer, L. Hines, *Woody Bledsoe: His life and legacy*, „AI Magazine" 1996, t. 17, nr 1.
[6] M. Kirby, L. Sirovich, *Low-dimensional procedure for the characterisation of human faces*, „Journal of the Optical Society of America" 1987, t. 4 (3).

2.4. Identyfikacja na podstawie głosu

Warto również przyjrzeć się, jak przedstawiała się historia identyfikacji na postawie głosu. Jej początków upatrywać można w metodzie opracowanej przez Lawrence Kersta. Wykorzystał on urządzenie (tzw. spektrograf dźwiękowy), za pomocą którego możliwe było przedstawienie głosu osoby mówiącej w formie graficznego obrazu (tzw. voiceprint). Pozwalało to na zestawienie ze sobą dwóch próbek głosu (dowodowej i porównawczej), a w konsekwencji określenie czy nagrane słowa zostały wypowiedziane przez tę samą osobę[7]. Jednakże pierwszym krokiem do stworzenia urządzeń biometrycznych w tej dziedzinie było stworzenie 1960 roku modelu akustycznego bazującego na wykorzystaniu promieni Roentgena w celu analizy podmiotów wydających poszczególne dźwięki. Model ten został stworzony przez szwedzkiego naukowca Gunnara Fanta, którego rezultaty badań w tej dziedzinie pozwoliły na zrozumienie biologicznych komponentów mowy, która to wiedza jest niezbędna do identyfikacji osoby mówiącej[8].

2.5. Identyfikacja na podstawie podpisu

Od najdawniejszych czasów możemy się spotkać z próbą identyfikacji człowieka na podstawie składanego przez niego podpisu. Jednakże urządzenia biometryczne, których zadaniem jest identyfikacja osoby na podstawie podpisu, pojawiły się dopiero w połowie lat sześćdziesiątych XX wieku. Skonstruowane w 1965 przez północnoamerykańskie lotnictwo urządzenie zapoczątkowało rozwój biometrii w tej dziedzinie[9]. W 1977 firma Veripen Inc. dostała patent dotyczący urządzenia identyfikacji personalnej, które wykorzystywało analizę dynamicznego nacisku pióra[10]. Obecnie biometryczne uwierzytelnianie podpisu nie sprowadza się jedynie do porównywania wyglądu wzoru podpisu z tym zakodowanym w urządzeniu weryfikującym. Współczesne urządzenia badają również dynamikę nakreślenia podpisu, na którą składa się: szybkość i kolejność pisania, siła nacisku pióra na tablet, a również kąt nachylenia pióra podczas pisania.

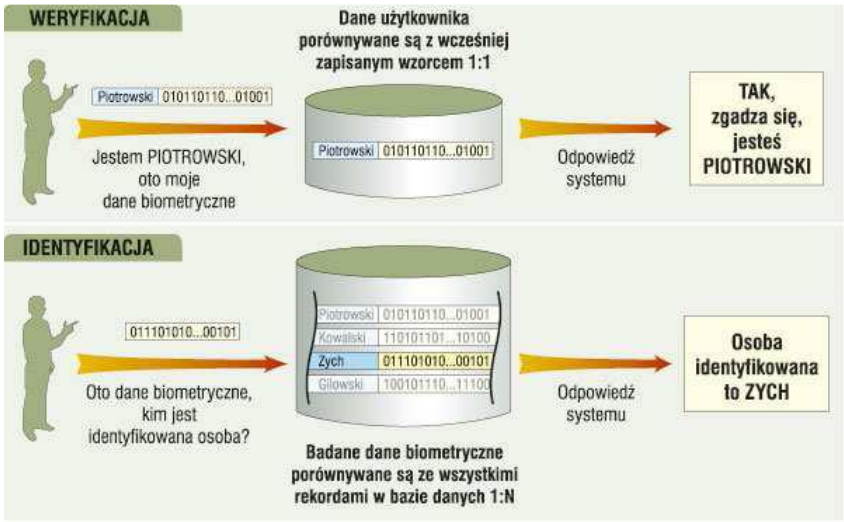
---

[7] C. Shaver, J. Acken, *A Brief Review of Speaker Recognition Technology*, Electrical and Computer Engineering Faculty Publications and Presentations, 2016.
[8] Ibidem.
[9] https://www.biometricupdate.com/201802/history-of-biometrics-2 (dostęp 11.11.2020).
[10] Ibidem.

3. Techniki biometryczne

3.1. Weryfikacja a identyfikacja

Przed przejściem do omawiania poszczególnych metod biometrycznych trzeba zwrócić uwagę na dwa pojęcia nieodłącznie związane z używaniem systemów biometrycznych. Są to: *weryfikacja* i *identyfikacja*.



Ryc. 2. Identyfikacja a weryfikacja (źródło: A. Dzwonek, T. Kling, *„Biometria w dokumentach podróży”*, Człowiek i dokumenty nr 10, Warszawa 2008 r.)

Identyfikacja polega na ustaleniu przez urządzenie biometryczne tożsamości sprawdzanej osoby. Urządzenie biometryczne zbiera informacje za pomocą sensorów, a następnie system komputerowy porównuje je z wzorcami, które znajdują się w bazie danych. Identyfikacja jest najczęściej stosowana przez policję i wojsko[11].

Weryfikacja sprowadza się do porównania danej cechy biometrycznej z jej wzorcem, który został już wcześniej umieszczony w bazie danych. W ten sposób system weryfikuje tożsamość sprawdzanej osoby[12]. Tego typu urządzenia używane są np. przez prywatne firmy pragnące zweryfikować tożsamość swoich pracowników. Spotykamy się z nimi również częściej w urządzeniach elektronicznych, takich jak np. smartphone z wbudowanym czytnikiem linii papilarnych.

[11] K. Krassowski, I. Sołtyszewski, op. cit., s. 39.
[12] Ibidem.

3.2. Poszczególne metody

W celu identyfikacji lub weryfikacji możemy zastosować następujące metody biometryczne:

1) badanie odcisku palca
2) badanie geometrii dłoni
3) analiza siatki naczyń krwionośnych
4) badanie geometrii twarzy
5) badanie tęczówki oka
6) badanie podpisu
7) badanie parametrów głosu
8) inne metody: badanie geometrii stopy, badanie geometrii ucha, badanie sposobu poruszania się, badanie DNA

3.2.1. Badanie linii papilarnych

Jak już było wspomniane w części dotyczącej historii, odbitki linii papilarnych są już od wieków używane w celu weryfikacji tożsamości danej osoby. Powodem popularności tej metody było i jest prawdopodobnie to, co możemy określić jako reguła 3N, a mianowicie, że odbitki linii papilarnych są niezmienne, niepowtarzalne i nieusuwalne.

Niezmienność oznacza, że od momentu ukształtowania się wzorów linii papilarnych, które następuje między szóstym, a siedemnastym tygodniem życia płodowego, stworzony w tym okresie układ bruzd na skórze pozostaje taki sam przez całe życie człowieka (jest to prawidłowość obserwowana nie tylko dla dłoni, ale także dla stóp, a także nawet ust).

Niepowtarzalność oznacza, że pomimo możliwości powtórzenia się minucji (czyli charakterystycznych cech linii papilarnych) u poszczególnych osób, to jednak układ linii papilarnych różni się nawet u bliźniąt jednojajowych.

Nieusuwalność natomiast oznacza, że trwałe usunięcie linii papilarnych jest prawie niemożliwe (istnieją jednakże bardzo rzadkie choroby genetyczne, które mogą powodować brak linii papilarnych).

Bazując na zasadzie 3N identyfikacja lub weryfikacja tożsamości osoby poprzez badanie odbitek linii papilarnych ewoluowała od porównywania minucji przez człowieka za czasów F. Galtona[13], do stworzenia systemów komputerowych dokonujących automatycznego

[13] F. Galton, *Finger Prints*, McMillan, London 1982.

porównania dostarczonych próbek z wzorcem lub wzorcami (w zależności od tego, czy mamy do czynienia z identyfikacją czy weryfikacją) znajdującymi się w bazie danych.

Urządzenia biometryczne w tej dziedzinie mogą charakteryzować się różną metodą działania. Poniżej omówione zostanie cztery typy sensorów wykorzystywanych w celu rejestrowania linii papilarnych. Będą to sensory optyczne, sensory pojemnościowe, sensory termiczne, sensory ultradźwiękowe.

Sensory optyczne działają na takiej samej zasadzie, na jakiej działa komputerowy skaner. Głównym źródłem działania jest tu źródło światła, które wykorzystywane jest do wykonania zdjęcia linii papilarnych palca przyłożonego do urządzenia. Urządzenie takie bazuje na zjawisku absorpcji i odbicia polegającym na tym, że stykając się z powierzchnią, grzbiety linii papilarnych absorbują światło, natomiast doliny linii papilarnych odbijają je. Tak wykonane zdjęcie może być następnie użyte przez system komputerowy jako materiał porównawczy względem wzorca/wzorców znajdujących się w bazie danych[14]. Należy zwrócić uwagę, że sensory optyczne posiadają wiele wad, ze względu na które często zastępuje się je urządzeniami, których działanie opiera się na innych zasadach. Przede wszystkim metody optyczne nie pozwalają na stwierdzenie czy palec przykładany do takiego urządzenia jest prawdziwy. Można więc oszukać sensor poprzez przyłożenie do niego spreparowanego odcisku palca.

Sensory pojemnościowe posiadają matrycę, która zbudowana jest z kondensatorów. Urządzenia te dokonują pomiaru z uwzględnieniem różnic pomiędzy grzbietami i dolinami linii papilarnych, jakie występują podczas nacisku na matrycę. Na tej podstawie urządzenie tworzy obraz linii papilarnych, który wykorzystywany jest do utworzenia unikalnego wzorca[15].

Sensory termiczne sczytują linie papilarne poprzez pomiar temperatury palca przesuwanego prostopadle do matrycy. Do utworzenia obrazu sensor wykorzystuje różnicę temperatur pomiędzy grzbietami, a powietrzem złapanym w doliny linii papilarnych. Jako że czujniki termiczne wykorzystują do swego działania temperaturę, dużo trudniej jest oszukać takie urządzenie poprzez np. przyłożenie do matrycy sztucznie skonstruowanego palca.

Sensory ultradźwiękowe wysyłają w kierunku badanego odcisku, fale dźwiękowe o różnej częstotliwości, rejestrują powstałe echo, a następne analizują je w celu odtworzenia trójwymiarowej struktury odcisku[16].

---

[14] G. Marcialis, F. Roli, *Fingerprint verification by fusion of optical and capacitive sensors*, „Pattern Recognition Letters" 2004, t. 25.

[15] Ibidem.

[16] X. Jiang, Y. Lu, H.Y. Tang *et al.*, *Monolithic ultrasound fingerprint sensor*, „Microsystems and Nanoengineering" 2017, t. 3.

Bez względu na sposób działania urządzenia biometryczne zajmujące się identyfikacją lub weryfikacją tożsamości na podstawie linii papilarnych są obecnie bardzo popularnym zabezpieczeniem spotykanym w sprzętach elektronicznych, takich jak smartphony. Są one również montowane w drzwiach wejściowych w firmach, w celu weryfikacji tożsamości osób wchodzących.

Ryc. 3. Przykłady urządzeń wykorzystujących zabezpieczenia oparte na wzorze linii papilarnych (źródło: (https://www.mytrendyphone.pl/, https://myapple.pl/)

3.2.2. Badanie geometrii dłoni

Urządzenia biometryczne skonstruowane w celu badania geometrii dłoni mierzą i zapisują informacje o wymiarach dłoni, takich jak: mierzona w kilku punktach długość i szerokość palców oraz geometryczne właściwości śródręcza. Tradycyjnie urządzenie takie składało się z kamery, która wykonywała zdjęcie dłoni oraz przetwarzała wyżej wymienione właściwości fizyczne. W czasie wykonywania zdjęcia, dłoń leżała na specjalnym panelu, a pomiędzy palcami ułożone były kołki. Gdy system przeanalizował już uzyskane informacje mógł dokonać porównania zdjęcia z wzorcem znajdującym się w bazie danych[17].

[17] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, *Biometric identification through hand geometry measurements*, „IEEE Transactions on Pattern Analysis and Machine Intelligence" 2000, t. 22(10).

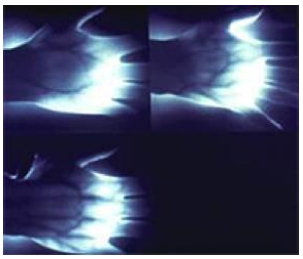
Ryc. 4. Obraz dłoni wykonany za pomocą czytnika dłoni (źródło:http://www.biometriclabs.pl/index.php?option=com_content&task=view&id=48&Itemid=105)

Ryc. 5. Cechy geometryczne dłoni (źródło:http://www.biometriclabs.pl/index.php?option=com_content&task=view&id=48&Itemid=105)

Ponieważ kształt dłoni nie jest niepowtarzalny, jak to było w przypadku odcisków palców, badanie geometrii dłoni częściej wykorzystywane jest do weryfikacji tożsamości niż do identyfikacji osoby.

3.2.3. Analiza siatki naczyń krwionośnych

Dziedzina biometrii zajmująca się analizą siatki naczyń krwionośnych polega na badaniu ułożenia naczyń krwionośnych na dłoniach człowieka. Metoda ta bazuje na założeniu, że układ oraz grubość żył różnią się u poszczególnych ludzi. Promienie podczerwieni, emitowane przez specjalne diody elektroluminescencyjne przenikają przez skórę dłoni i powodują wyodrębnienie się unikalnej siatki naczyń krwionośnych.



Ryc. 6. Zdjęcie siatki naczyń krwionośnych dłoni (źródło: http://www.biometrics.gov/Docments/vascularpatternrec.pdf)

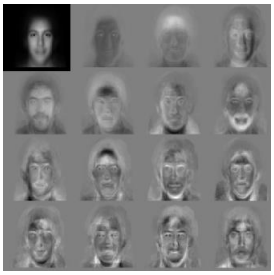
Następnie system porównuje otrzymany wzór z oryginałem, zamieszczonym wcześniej w bazie danych i dokonuje weryfikacji tożsamości osoby egzaminowanej. Zaletą takich urządzeń dla użytkowników jest to, że wystarczy zbliżyć dłoń do urządzenia bez potrzeby dotykania go[18].

3.2.4. Badanie geometrii twarzy

Badanie geometrii twarzy polega na porównywaniu przez system komputerowy informacji wyczytanych przez system ze specjalnie zrobionego zdjęcia twarzy danej osoby, z informacjami już wcześniej znajdującymi się w systemie (na informacje te składa się m.in. odległość pomiędzy poszczególnymi częściami twarzy, jak np. pomiędzy oczami, nosem i ustami). Aby przeprowadzić analizę ludzkiej twarzy należy posłużyć się jednym z wielu opracowanych algorytmów. Trzy przykłady wykorzystywanych algorytmów przedstawione zostaną poniżej. Będą to: *Analiza Głównych Składowych* (PCA od ang. Principal Components Analysis), *Analiza Liniowa Wyznaczników* (LDA od ang. Linear Discriminant Analysis) oraz *Analiza Siatki Graficznej Twarzy* (EBGM od ang. Elastic Bunch Graph Matching).
Analiza głównych składowych polega na zastosowaniu tzw. eigenfaces (właściwych twarzy). Warunkiem zastosowania tej metody jest to, że rozmiar obrazu porównywanego oraz wzorca znajdującego się w bazie danych urządzenia, jest taki sam. Gdy warunek ten jest spełniony algorytm jest używany do zredukowania rozmiaru obrazu porównywanego jedynie do charakterystycznych cech twarzy niezbędnych do dokonania komparacji (w tym właśnie wyraża się koncepcja „właściwych twarzy"). Tak zapisany obraz jest następnie porównywany z wzorcem/wzorcami (w zależności czy celem badania było dokonanie identyfikacji czy weryfikacji) znajdującymi się w pamięci systemu[19].

---

[18] K. Shaheed, H. Liu, G. Yang, I. Qureshi, J. Gou, Y. Yin, *A systematic review of finger vein recognition techniques*, „Information" 2018, nr 9.
[19] M. Turk, A. Pentland, *Eigenfaces for recognition*, „Journal of Cognitive Neuroscience" 1991, t. 3.



Ryc. 7. Przykład uzyskania eigenfaces stosując metodę PCA (źródło: http://www.biometrics.gov/Documents/facerec.pdf)

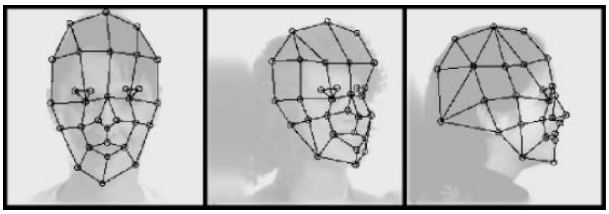
Liniowa analiza dyskryminacji jest metodą opierającą się na statystyce, stosowaną w celu odseparowania od siebie różnych obiektów i zdarzeń. W rezultacie zastosowania tej metody można stworzyć liniową klasyfikację badanych obiektów ze względu na ich podobieństwo względem siebie. W przypadku badania geometrii twarzy zastosowanie tej techniki powoduje stworzenie przez system komputerowy grup podobieństwa twarzy, które pomagają w procesie identyfikacji lub weryfikacji[20].

Ryc. 8. Przykład zastosowania liniowej analizy dyskryminacji (źródło: http://www.biometrics.gov/Documents/facerec.pdf)

Analiza Siatki Graficznej Twarzy jest metodą polegającą na wyszukiwaniu przez system, punktów charakterystycznych twarzy, a następnie łączeniu ich w celu stworzenia specyficznej siatki graficznej twarzy. Gdy siatka taka jest już utworzona, system wyszukuje w bazie danych wzorca, którego siatka graficzna jest identyczna z siatką graficzną obrazu porównywanego. Oczywiście, ta procedura ma miejsce w tylko przypadku identyfikacji, gdyż gdy mamy do czynienia z weryfikacją system porównuje otrzymaną siatkę graficzną z konkretnym wzorcem znajdującym się w pamięci urządzenia[21].

[20] S. Satonkar Suhas, B. Kurhe Ajay, B. Prakash Khanale, *Face recognition using principal component analysis and linear discriminant analysis on holistic approach in facial images database*, „Journal of Engineering" 2012, t. 2(12).

[21] L. Wiskott, N. Krüger, N. Kuiger, C. von der Malsburg, *Face recognition by elastic bunch graph matching*, „IEEE Transactions on Pattern Analysis and Machine Intelligence" 1997, t. 19, nr 7.



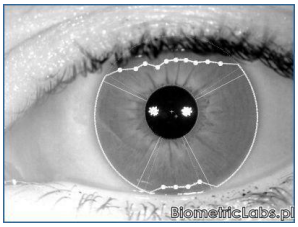
Ryc. 9. Siatka graficzna twarzy (źródło:http://www.biometrics.gov/Documents/facerec.pdfhttp://www.biometrics.gov/Documents/facerec.pdf)

Należy zauważyć, że obecnie bardzo często wykorzystywane są metody pozwalające na przeprowadzenie biometrycznego rozpoznawania twarzy 3D[22].

Urządzenia, które badają geometrię twarzy, mogą służyć zarówno do identyfikacji osoby, jak i do weryfikacji jej tożsamości. Zabezpieczenia wykorzystujące opisywaną cechę biometryczną, możemy obecnie znaleźć w paszportach czy też dowodach osobistych.

3.2.5. Badanie tęczówki oka

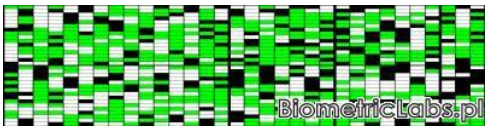
Tęczówka jest kolorowym elementem oka, który odpowiedzialny jest za regulowanie dopływu światła do soczewki. Po ostatecznym wykształceniu się w młodości, tęczówka nie zmienia się aż do śmierci osoby. Ta cecha oka jest tak unikalna, że tęczówka prawego oka człowieka różni się od tęczówki oka lewego. Do wygaśnięcia patentu w 2011r. urządzenia zajmujące się badaniem tej cechy biometrycznej bazowały na czterech matematycznych równaniach opracowanych w 1994 roku przez Brytyjczyka Johna Daugmana. Aby pomiar tęczówki był udany, urządzenie najpierw lokalizuje oko, a następnie wykonuje zdjęcie tęczówki.



Ryc. 10. Lokalizacja tęczówki przez urządzenie biometryczne (źródło:http://www.biometriclabs.pl/index.php?option=com_content&task=view&id=47&Itemid=104)

W tęczówce znajduje się około 200 cech charakterystycznych, które po dokonaniu zdjęcia, są rozpoznawane przez system, a następnie kodowane za pomocą specjalnego szyfru.

[22] Por. np. Y. Lei, M. Bennamoun, M. Hayat, Y. Guo, *An efficient 3D face recognition approach using local geometrical signatures*, „Pattern Recognition" 2004, t. 47(2).



Ryc. 11. Przykładowy kod tęczówki (źródło: http://www.biometriclabs.pl/index.php?option=com_content&task=view&id=47&Itemid=104)

Tak otrzymany kod porównywany jest z wzorcem/wzorcami znajdującymi się w systemie w celu dokonania weryfikacji bądź identyfikacji[23]. Niewątpliwą zaletą tej metody jest jej szybkość i dość mała inwazyjność. Jak wszystkie metody badające cechy niepowtarzalne w populacji, tak i ta, nadaje się zarówno do identyfikacji jak i weryfikacji.

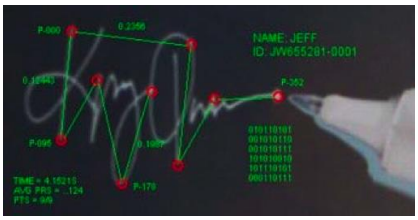
3.2.6. Badanie podpisu

Badane podpisu należy do grupy biometrii behawioralnej. Oznacza to, że przedmiotem badania nie jest cecha wrodzona człowieka (jak to było w przypadku wszystkich wyżej opisanych metod) lecz pewna cecha wyuczona, w tym przypadku podpis danej osoby. Podpis, który następnie ma podlegać weryfikacji, jest składany na urządzeniu zwanym tabletem, za pomocą specjalnego pióra.

Ryc. 12. Tablet graficzny (źródło: http://www.nobleco.org/Surveyor/files/images/tablet.jpg)

Urządzenie rejestruje dynamiczne cechy podpisu, takie jak: prędkość składania odpisu, kąt nachylenia pióra oraz nacisk pióra na tablet podczas pisania. Niektóre urządzenia porównują również cechy statyczne podpisu, takie jak ogólny wygląd liter czy ich wysokość.

[23] J. Daugman, *How iris recognition works*, „IEEE Transactions on Circuits and Systems for Video Technology" 2004, t. 14, nr 1.

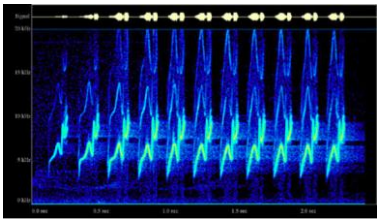


Ryc. 13. Punkty charakterystyczne odnalezione przez system we wzorze podpisu (źródło: http://www.biometrics.gov/Documents/dynamicsig.pdf)

Ostatnim krokiem jest porównanie przez system popisu złożonego na tablecie z podpisem znajdującym się w pamięci urządzenia [24].

3.2.7. Badanie parametrów głosu

Badanie parametrów głosu jest również jednym z przykładów biometrii behawioralnej. Urządzenia służące do rozpoznania mówiącego badają około dwudziestu cech głosu, takich jak wysokość tonu, dynamika głosu, kształt fali czy sposób wymowy. Występują dwa rodzaje urządzeń służące do rozpoznania mówiącego: te, które wykorzystują do tego celu tzw. tekst zależny oraz te bazujące na tzw. tekście niezależnym. Pierwsze z nich wymagają od osoby egzaminowanej podania określonego słowa, hasła lub ciągu cyfr. Zadaniem drugiego jest rozpoznanie mówiącego na podstawie próbki jego głosu. W tym przypadku nie ma wymogu, aby osoba egzaminowana wypowiedziała konkretne słowa. Pobrana próbka głosu, zapisywana jest przez urządzenie za pomocą wykresu przedstawiającego parametry głosu[25].



Ryc. 14. Wykres przedstawiający parametry głosu (źródło: http://www.biometrics.gov/Documents/speakerrec.pdf)

[24] A. Czajka, A. Pacut, *Biometria podpisu odręcznego*, w: P. Zając, S. Kwaśniowski (red.), *Automatyczna identyfikacja w systemach logistycznych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.
[25] T. Majekodunmi, F. Idachaba, *A review of the fingerprint, speaker recognition, face recognition and iris recognition based biometric identification technologies*, „Proceedings of the World Congress on Engineering" 2011, t. II, WCE 2011, July 6–8, 2011, London, U.K., tekst dostępny: http://eprints.covenantuniversity.edu.ng/3946/1/WCE2011_pp1681-1687.pdf (dostęp 11.11.2020).

3.2.8. Inne metody

Metody biometryczne opisane w tej części są stosowane rzadziej w porównaniu z wyszczególnionymi powyżej. Wynika to albo z trudności w stworzeniu odpowiedniego urządzenia do badania danej cechy biometrycznej albo w niepraktyczności użycia danej cechy w celu dokonania weryfikacji lub identyfikacji tożsamości osoby. Do tego typu metod zaliczyć można np. badanie odcisku stopy czy ucha.

Oddzielnym problemem jest wykorzystywanie badania DNA w celu weryfikacji tożsamości lub identyfikacji danej osoby. Wielu naukowców uważa, że jest to przyszłość w dziedzinie badań biometrycznych, ponieważ wzór w jaki układa się spirala DNA jest niepowtarzalny. Problem z wykorzystaniem DNA do weryfikacji lub identyfikacji polega jednak na tym, że metoda, jaką trzeba by zastosować, aby pobrać materiał porównawczy, różni się od metod stosowanych w przypadku technik wykorzystujących inne cechy biometryczne. Na obecnym etapie, nie ma możliwości zastosowania, przy badaniu DNA, urządzenia optycznego bądź podczerwieni. Wymagana jest namacalna próbka w postaci pobrania tkanki od osoby egzaminowanej (źródłem pobranej tkanki może być np. krew). Jak na razie nie ma urządzenia, które pozwalałoby na szybką identyfikację lub weryfikację na podstawie porównywania próbek DNA dlatego też metoda ta nie znajduje zastosowania poza medycyną sądową. Warto jednak zauważyć, że w Stanach Zjednoczonych w 2017 roku wdrożono koncepcję Rapid DNA[26], która pozwala na dużo szybsze niż do tej pory (w ciągu dwóch godzin) porównanie próbki pobranej od osoby z profilami zamieszczonymi w bazie danych[27].

[26] The Rapid DNA Act of 2017 (Public Law 115-50).
[27] https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna (dostęp 11.11.2020).

4. Ustawodawstwo w zakresie zabezpieczeń biometrycznych

Wraz z rozwojem technologicznym, który doprowadził do rozkwitu w dziedzinie konstrukcji urządzeń biometrycznych, zaistniała potrzeba wprowadzenia regulacji prawnych niezbędnych do uporządkowania korzystania z tychże urządzeń przy jednoczesnym poszanowaniu praw jednostki. Jako że początkowo porównywanie cech biometrycznych przez maszyny nie było jeszcze rozpowszechnione, zadanie utworzenia odpowiedniej legislacji stanowiło duże wyzwanie. Brak praktycznych doświadczeń sprawił, że w pierwszych powstających regulacjach prawnych, ustawodawca nie zwrócił uwagi na wszystkie problemy, które później pojawiały się w praktyce podczas stosowania systemów biometrycznych w celu identyfikacji osoby bądź weryfikacji jej tożsamości. Pierwszego maja 2004 roku Polska stała się członkiem Unii Europejskiej przyjmując na siebie zobowiązanie do wdrażania do polskiego porządku prawnego norm ustanowionych na szczeblu wspólnotowym. Powyższa zasada ma zastosowanie również w stosunku do legislacji unijnej regulującej zastosowanie technologii bazującej na badaniu cech biometrycznych.

4.1. Prawo Unii Europejskiej

Pierwszym unijnym wiążącym aktem prawnym wprowadzającym wykorzystanie technologii w dziedzinie zabezpieczeń biometrycznych dla celów wspólnotowych było Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie[28]. Jednakże już wiosną 2004 roku, Parlament Europejski, zaniepokojony możliwością wprowadzenia do ustawodawstwa unijnego nowoczesnych zabezpieczeń biometrycznych, zwrócił się do Komisji Europejskiej o dokonanie oceny i skutków wdrożenia legislacji nakazującej użycie systemów biometrycznych w dokumentach. W odpowiedzi na apel Parlamentu Komisja wydała opublikowany w 2005 roku raport: „*Biometria na granicach: ocena wpływu na społeczeństwo*”[29]. Raport Komisji przedstawiał prawdopodobne konsekwencje, jakie może mieć zastosowanie biometrii w życiu codziennym obywateli Unii. Komisja sugerała, aby przed wprowadzeniem urządzeń wykorzystujących cechy biometryczne

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

[29] *Biometrics at the Frontiers: Assessing the Impact on Society – EUR 21585.*

w celu identyfikacji osoby lub weryfikacji jej tożsamości, przeprowadzić analizę ich przydatności bazując na tzw. siedmiu filarach wiedzy o danych biometrycznych, które stanowią: uniwersalność, unikalność, niezmienność, możliwość pobrania, wydajność, akceptowalność oraz odporność na oszukanie.

Uniwersalność oznacza, że aby wykorzystać daną cechę w celu identyfikacji, musi ona powszechnie występować w populacji. Takimi cechami są np. linie papilarne na palcach czy DNA.

Unikalność oznacza, że wykorzystywane cechy muszą odznaczać się indywidualnością, tak więc nie mogą powtarzać się w populacji (np. wzór linii papilarnych u jednej osoby zawsze różni się od wzoru u innej osoby).

Niezmienność oznacza, że aby dana cecha stanowiła wiarygodny materiał identyfikacyjny, musi odznaczać się względną niezmiennością w ciągu całego życia osoby (np. gdy wzory linii papilarnych zostaną ostatecznie uformowane podczas życia płodowego dziecka, pozostają one już zawsze w takim kształcie).

Możliwość pobrania stanowi, że pobranie materiału wzorcowego oraz porównawczego w celu weryfikacji lub identyfikacji powinno być łatwe oraz odbywać się w krótkim czasie (kryteria te spełnia na przykład skanowanie tęczówki oka).

Wydajność oznacza, że zanim urządzenie wykorzystujące technologię biometryczną zostanie wdrożone, należy zbadać i zdawać sobie sprawę ze stopnia dokładności identyfikacji dokonywanego przy takim pomiarze.

Akceptowalność – Komisja podkreśliła, że wprowadzając systemy biometryczne należy pamiętać jak ważnym czynnikiem jest zaaprobowanie ich przez społeczeństwo. W przeciwnym razie tego typu metody identyfikacji nie odniosą sukcesu oczekiwanego przez ich twórców.

Odporność na oszukanie – Komisja zauważyła również, że przesłanką do wdrażania nowych technologii, opartych na porównywaniu cech biometrycznych, jest to, że nowe urządzenia będą mniej podatne na próby oszukania ich niż aktualnie istniejące systemy[30].

Analizując wdrażanie systemów biometrycznych, Komisja wzięła pod uwagę konsekwencje, jakie istnienie nowych technologii mało mieć dla obywateli Wspólnoty. Wyróżniła przy tym pięć podstawowych rodzajów konsekwencji: na płaszczyźnie społecznej, ekonomicznej, prawnej, technicznej oraz medycznej.

Biorąc pod uwagę aspekt społeczny, Komisja podkreśliła, że aby systemy biometryczne były powszechnie akceptowalne, społeczeństwo musi być informowane o celach wprowadzania

[30] K. Krassowski, I. Sołtyszewski, op. cit., s. 42.

danej technologii oraz konsekwencjach, jakie się z tym wiążą. Potrzeba informacji wynika bowiem stąd, iż wprowadzenie takiego systemu skutkuje zmianą dotychczasowej pozycji obywatela w stosunku do państwa. W zamian za wprowadzanie technologii mającej zapewnić większe bezpieczeństwo, obywatele zmuszeni są zgodzić się na pomniejszenie swojej sfery prywatności i anonimowości[31].

W aspekcie ekonomicznym, Komisja przekonywała, że ponieważ identyfikacja za pomocą urządzeń posługujących się technologią biometryczną jest bezpieczniejsza i skuteczniejsza od aktualnie występujących procedur, może ona być z powodzeniem stosowana podczas transakcji gospodarczych. Patrząc również z ekonomicznego punktu widzenia, trzeba zwrócić uwagę, że wprowadzenie nowych technologii miało wiązać się z koniecznością poniesienia pewnych kosztów. Koszty nie ograniczały się jedynie do sumy jaką trzeba wyłożyć dla prawidłowego funkcjonowania technologii biometrycznej, ale również wiązały się z wprowadzeniem procedur awaryjnych, a także procedur służących do prawidłowego zbierania oraz przechowywania danych w systemie[32].

W ramach aspektu prawnego raport skupił się na dwóch zagadnieniach. Pierwsze z nich to opracowanie takich procedur pobierania i porównywania cech biometrycznych, które byłyby w zgodzie z prawami człowieka, a zwłaszcza z prawem do poszanowania godności ludzkiej. Drugim problemem, który Komisja zauważyła, było wprowadzenie legislacji zapewniającej ochronę danych osobowych (zresztą problem ochrony danych osobowych podczas użycia technologii opartej na systemach biometrycznych, będzie wracał jako argument stosowany w celu skrytykowania pojawiających się w tej dziedzinie aktów prawnych wydawanych przez prawodawcę Unijnego)[33].

Aspekt technologiczny przejawiał się przede wszystkim w zwróceniu uwagi na potrzebę ciągłego prowadzenia badań nad rozwojem technologii biometrycznej, gdyż w czasie powstania raportu nie wszystkie z istniejących technik zostały sprawdzone w dostatecznym zakresie. Komisja zwrciła również uwagę, że w celu zapewnienia większej skuteczności funkcjonowania zabezpieczeń biometrycznych, dobrym pomysłem jest łączenie kilku systemów biometrycznych w dokumentach (może się to np. przejawiać we wprowadzeniu zabezpieczeń w postaci zakodowania na specjalnym chipie wzoru linii papilarnych oraz w postaci umieszczenia w dokumencie zdjęcia wykonanego techniką biometryczną)[34].

---

[31] *Biometrics at the Frontiers*…, op. cit., s. 7.
[32] Ibidem, s. 8.
[33] Ibidem, s. 6, 8–9.
[34] Ibidem, s. 9.

W czasie, kiedy raport powstawał, przeciwnicy wprowadzania technologii opartej na biometrii zgłaszali obawy co do bezpieczeństwa użycia tego typu urządzeń ze względów zdrowotnych. Komisja postanowiła zająć się również i tym problemem. W raporcie czytamy, że nowa technologia może mieć dwojaki wpływ na zdrowie osób egzaminowanych: bezpośredni i pośredni. Bezpośredni wiąże się z tym, że gdy podczas używania urządzenia osoba egzaminowana musi go dotknąć (np. w przypadku sensora sczytującego wzór linii papilarnych) pojawia się ryzyko zakażenia przez bakterie pozostawione wcześniej na urządzeniu przez inną osobę. Analizując ten problem, sama Komisja zauważyła, że ryzyko, aczkolwiek istniejące, jest jednak niewielkie, a można je dodatkowo zminimalizować poprzez częste czyszczenie sensora. Ponadto pojawiły się głosy, że używanie skanerów przy metodach skanowania tęczówki i siatkówki może mieć szkodliwy wpływ na oczy osoby poddanej badaniu. Jak do tej pory przekonanie takie nie znalazło żadnego potwierdzenia w rzeczywistości. Wpływ pośredni polega natomiast na możliwości „wyczytania" z analizy niektórych cech biometrycznych kondycji zdrowotnej osoby egzaminowanej. W tym miejscu pojawia się oczywiście problem wykorzystania przez osobę zajmującą się pomiarami, uzyskanych informacji[35]. W opinii autorki jest to jednak kwestia wprowadzenia odpowiednich regulacji prawnych, które konkretnie określą cel do jakiego użyta może zostać pobrana próbka danej cechy.

We wnioskach Komisja stwierdziła, że wprowadzanie systemów biometrycznych może znacząco ułatwić życie obywatelom oraz funkcjonariuszom pracującym na granicach Unii. Aby jednak tak się stało, musi zostać wprowadzona odpowiednia regulacja prawna stwarzająca ramy do funkcjonowania technologii biometrycznej w ramach Wspólnoty oraz rozwiązująca problemy przedstawione w raporcie, jak również te, które mogą pojawić się w przyszłości podczas praktycznego zastosowania urządzeń biometrycznych.

Pierwszym wiążącym aktem prawnym Unii regulującym użycie technologii biometrycznych jest wspomniane wyżej Rozporządzenie Rady Wspólnot Europejskich nr 2252/2004 z grudnia 2004 roku. Jak w każdym akcie wspólnotowym posiadającym wiążącą moc prawną, tak i tutaj pierwszą część stanowią motywy i cele, którymi legislator kierował się wprowadzając dane przepisy do porządku prawnego Unii Europejskiej. Z tej części rozporządzenia wyczytać możemy, że paszport obywatela Unii powinien zawierać nie tylko zabezpieczenia chroniące przed sfałszowaniem (jak znaki wodne czy barwne włókna widoczne w świetle ultrafioletowym), ale również identyfikatory biometryczne, które zapewnić mają „związek pomiędzy dokumentem, a jego prawowitym posiadaczem". Rozporządzenie wprowadza dwa

[35] Ibidem, s. 10.

rodzaje identyfikatorów biometrycznych, które mają znaleźć się w paszportach oraz dokumentach podróży. Pierwszy z nich, to zamieszczony na specjalnym nośniku pamięci, obraz twarzy właściciela dokumentu. Drugi to załączone odciski palców w interoperacyjnych formatach (interoperacyjność jest terminem technicznym używanym przez legislatora unijnego, odnoszącym się do możliwości jakie posiadają systemy technologii informacyjnej IT w dziedzinie wymiany danych[36]). Mimo że do opisywanego Rozporządzenia Rady dodano załącznik określający minimalne normy dotyczące zabezpieczeń paszportów i dokumentów podróży wydawanych przez Państwa Członkowskie, norm technicznych dotyczących zastosowania identyfikatorów biometrycznych należało szukać w Załącznikach do decyzji Komisji z dnia 28 lutego 2005 roku oraz z dnia 28 czerwca 2006 roku ustanawiających specyfikacje techniczne dla norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie[37]. Zgodnie z tymi załącznikami identyfikatory biometryczne musiały spełniać normy Międzynarodowej Organizacji Normalizacyjnej (ISO – International Organization for Standarization) oraz zalecenia Międzynarodowej Organizacji Lotnictwa Cywilnego (ICAO – International Civil Aviation Organization). Powyższe normy miały być stosowane m.in. w odniesieniu do nośnika informacji, na którym miały być przechowywane identyfikatory biometryczne, struktury danych zapisanych na mikroprocesorze czy specyfikacjach dotyczących odcisków palców oraz zdjęcia twarzy zmieszczonych na nośniku informacji. W stosunku do obrazu twarzy załączniki nakazywały, aby zdjęcie właściciela dokumentu podróży zostało wykonane en face. Pojawiły się również zalecenia co do formatu pliku, w jakim obraz ma zostać zapisany oraz co do pojemności, jaką miał zajmować. W przypadku obrazu linii papilarnych załączniki określały, że na mikroprocesorze miały zostać zapisane odciski palców wskazujących obu rąk. W przypadku trudności w pobraniu wzoru linii papilarnych z palców wskazujących, należało pobrać je z palców środkowych, serdecznych lub kciuków. Również i w tym przypadku, załączniki precyzyjnie określały format, jakość oraz pojemność, jaką zajmować miał zapisany obraz. Rozporządzenie Rady nr 2252/2004 określił dla obu identyfikatorów biometrycznych, różne terminy wprowadzenia ich do paszportów i dokumentów podróży. Na wprowadzenie

[36] Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final.

[37] Decyzja Komisji z 28.02.2005 roku ustanawiająca specyfikacje techniczne dla norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, C(2005)409; Decyzja Komisji z 28.06.2006 roku, ustanawiająca specyfikacje techniczne dla norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie.

biometrycznego obrazu twarzy Państwa Członkowskie miały 18 miesięcy od dnia, w którym zaczęło obowiązywać rozporządzenie, co oznacza, że od połowy roku 2006 wprowadzanie obrazu twarzy zgodnego z normami rozporządzenia stało się wymogiem, które Państwa Członkowskie musiały uwzględniać wydając swoim obywatelom paszporty oraz inne dokumenty podróży. Jako że prawodawca unijny zdawał sobie sprawę, że wprowadzenie technologii zawierającej odciski palców może stanowić większe wyzwanie, dał Członkom Wspólnoty więcej czasu na wdrożenie nowoczesnej technologii. Państwa miały na to czas do połowy 2009r.

Jeden z artykułów w Rozporządzeniu ściśle precyzuje w jakim celu może być wykorzystane odczytywanie cech biometrycznych znajdujących się w dokumentach podróży. Te cele to: sprawdzenie autentyczności dokumentu oraz sprawdzenie tożsamości posiadacza paszportu lub innego dokumentu podróży.

Lakoniczność Rozporządzenia Rady spowodowała jednak dużą krytykę tego aktu, zwłaszcza, że na jego podstawie Państwa Członkowskie zmuszone były wdrożyć technologie biometryczną do krajowych porządków prawnych. Wątpliwości, co do regulacji z 2004 roku zostały przedstawione między innymi w opinii Grupy Roboczej nr 3/2005 w sprawie wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie[38]. Grupa Robocza podkreśliła, że akty normatywne regulujące wykorzystanie technologii biometrycznej w dokumentach podróży wymagały ich przeanalizowania zwracając szczególną uwagę na stopień ochrony danych w postaci identyfikatorów biometrycznych. Już na etapie tworzenia opinii na temat wdrażania systemów biometrycznych, Grupa Robocza zauważyła, że „szybki dostęp w zakresie technologii biometrycznych i ich coraz szersze zastosowanie obserwowane w ostatnich latach wymagają bliższego zbadania w kontekście ochrony danych. Powszechne i niekontrolowane wykorzystanie biometryki rodzi niepokój co do ochrony fundamentalnych praw i wolności obywatelskich. Są to dane o szczególnym charakterze, jako że odnoszą się bezpośrednio do behawioralnych i fizjologicznych cech danej osoby i pozwalają na jej absolutnie jednoznaczną identyfikację”[39]. W związku z tym w opinii wskazane zostały kwestie, które mogły rodzić problemy podczas stosowania rozporządzenia w praktyce. Pierwszym

[38] Opinia Grupy Roboczej nr 3/2005 w sprawie wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie.
[39] Ibidem.

problemem, jaki pojawił się w opinii, jest odwoływanie się rozporządzenia do wyżej wspomnianych norm Międzynarodowej Organizacji Normalizacyjnej ISO. Jedną z takich norm jest zastosowanie bezkontaktowych mikroprocesorów RFID – chip do zapisywania identyfikatorów biometrycznych (standard ISO nr 14443). Jako że dane z takiego chipu sczytywane są w sposób automatyczny, rodzi to ryzyko łatwego przechwycenia zawartych na mikroprocesorze informacji. Grupa Robocza postulowała więc wprowadzenie zabezpieczeń, aby uniknąć opisanej powyżej sytuacji. W tym celu odwołała się do standardu ISO nr 15408, mówiącego o utworzeniu profilu zabezpieczeń mającego doprowadzić do utrudnienia wycieku danych biometrycznych zapisanych na chipie RFID. Grupa analizowała również przepisy dotyczące poszczególnych identyfikatorów biometrycznych, które zgodnie z planem legislatora unijnego, miały znaleźć się w paszportach i innych dokumentach podróży. W opinii zwrócona została uwaga, że samo zastosowanie zgodnej z normami ICAO tzw. kontroli BAC (Basic Access Control – Podstawowa Kontrola Dostępu) nie wystarczy do zabezpieczenia obrazu twarzy zapisanego na mikroprocesorze. System BAC ma zapewnić, że dane zabezpieczone za jego pomocą będą zaszyfrowane w ten sposób, że można je będzie odczytać tylko w momencie kontaktu mikroprocesora z czytnikiem. Krytyka wynikała jednak stąd, że algorytm, jaki wykorzystuje BAC do szyfrowania danych, nie jest określany jako poufny, a co za tym idzie może zostać kiedyś udostępniony opinii publicznej. Jeśli chodzi o odciski palców, mają być one zabezpieczane poprzez zastosowanie rozszerzonej kontroli dostępu zwanej Extended Access Control. Problemem związanym z tym systemem nie było to, że nie chronił on danych w wystarczającym stopniu, lecz to, że jego zastosowanie, pod rządami wdrażanego prawodawstwa, nie było obowiązkowe. Trudności jakie mogłyby wynikać z wprowadzaniem tego typu zabezpieczeń były również takie, że odczytanie identyfikatorów biometrycznych chronionych takim szyfrem mogłoby nie być możliwe w państwach trzecich, gdzie czytniki nie zawierałyby funkcji umożliwiającej odszyfrowanie znajdujących się na chipie obrazów linii papilarnych.

W akcie prawnym z 2004 roku, wiele problemów budziło również wprowadzanie odstępstw od pobierania odcisków palców. Spowodowało to, że niezgodnie z celem jakim było wydanie rozporządzenia, ustawodawstwa państw różniły się między sobą w tym względzie. Aby zaradzić tej kwestii, po ponad dwóch latach obowiązywania Rozporządzenia nr 2252/2004, legislator wspólnotowy postanowił wprowadzić zmiany do prawa wprowadzonego przez Radę w 2004 roku. W październiku 2007 roku Komisja przedstawiła wniosek: Rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i

dokumentach podróży wydawanych przez Państwa Członkowskie[40]. We wniosku tym zaproponowane zostały odstępstwa od pobierania odcisków palców od dzieci poniżej 6 roku życia, gdyż jakość pobieranych odbitek linii papilarnych bardzo często była zbyt niska, aby nadawała się do celów weryfikacyjnych. Komisja zauważyła jednak, że brak możliwości weryfikacji tożsamości dziecka przy pomocy identyfikatorów biometrycznych nie może prowadzić do, co było częstą praktyką w Państwach Członkowskich, niewydawania indywidualnych paszportów dla dzieci i wpisywania ich danych w dokument podróżnych rodziców. Według Komisji mogło to spowodować zwiększenie ryzyka handlu dziećmi. Dlatego też, aby nie dopuścić do szerzenia się na terenie Unii tego typu przestępczości, Wniosek Rozporządzenia z 2007 roku wprowadzał zasadę „jedna osoba – jeden paszport", która nakłada na każdego obywatela Unii, niezależnie od wieku (a więc także na dzieci poniżej 6 roku życia) obowiązek posiadania paszportu w celu przekroczenia granicy zewnętrznej Wspólnoty.

W trakcie realizacji w Państwach Członkowskich projektów pilotażowych wprowadzających identyfikatory biometryczne w postaci zamieszczenia na mikroprocesorze wzoru linii papilarnych, okazało się, że istnieje pewien niewielki procent ludzi, od których pobranie odcisku palca jest fizycznie niemożliwe (wynikało to głównie ze względów medycznych: wspomnianych w początkowej części pracy chorób czy braku palców niezbędnych do pobrania identyfikatora). Spowodowało to wprowadzenie propozycji drugiego odstępstwa od obowiązkowego pobierania odcisków palców. W stosunku do tej kategorii osób, Państwo Członkowskie musiało wprowadzić tak zwane procedury awaryjne, które zapewniały traktowanie ich na równi z osobami posiadającymi identyfikatory biometryczne w dokumentach podróży. Wniosek Rozporządzenia został jednak skrytykowany przez Europejskiego Inspektora Ochrony Danych Osobowych (EIOD), który w swej opinii z 26 marca 2008 roku wyraził wątpliwości co do niektórych propozycji wysuniętych przez Komisję[41]. Przede wszystkim EIOD zauważył, że Komisja nie zajęła się w wystarczającym stopniu problemem odstępstw od pobierania identyfikatorów biometrycznych. W swojej opinii EIOD zaznaczył, że nie zostały przeprowadzone wyczerpujące badania, które pomogłyby stwierdzić, że przyjęcie 6 lat jako granicy wieku, od której dokonuje się pomiarów, jest odpowiednia. Europejski Inspektor Ochrony Danych Osobowych apelował więc, aby zanim

[40] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, COM(2007) 619, wersja ostateczna.

[41] Opinia Europejskiego Inspektora Ochrony Danych dotycząca rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie, Dz. Urz. z 2008 r., C. 200.

zostaną dokonane dogłębne analizy dotyczące jakości pobieranych odbitek linii papilarnych, zastosować granicę wieku występującą już w aktach prawnych również wykorzystujących tego typu technologię (jak np. przy programie EURODAC, gdzie powiedziane jest, że odciski palców pobiera się od dzieci, które ukończyły 14 lat). Ponadto EIOD naświetlił problem pobierania identyfikatorów biometrycznych od osób starszych. Opinia podkreślała, że badania przeprowadzone w tej dziedzinie wskazały, że z wiekiem z powodu różnych czynników (na przykład chorób) coraz trudniejsze staje się pobieranie próbek odbitek linii papilarnych, które według rozporządzenia, powinny być zamieszczone w paszportach lub innych dokumentach podróży. Dlatego też EIOD zaproponował nie tylko dolną, ale i górną granicę wieku, po której przekroczeniu, osoba miałaby zostać zwolniona z obowiązku posiadania takiego identyfikatora w dokumencie. Granica ta, zaczerpnięta podobnie jak w odniesieniu do dzieci, z innych regulacji stosujących zabezpieczenia biometryczne w dokumentach, mogłaby wynosić 79 lat (jak to ma miejsce w przypadku programu US – VISIT). Europejski Inspektor Ochrony Danych Osobowych w swej opinii, odniósł się również do wprowadzonej przez wniosek rozporządzenia zasady „jedna osoba – jeden paszport". EIOD uznał, że jako iż w paszportach dzieci do określonego wieku, identyfikatory biometryczne i tak nie zostaną wprowadzone, wymóg odrębnego paszportu dla dziecka spowoduje tylko niepotrzebne zwiększenie kosztów podróży. Dlatego też EIOD zauważył, że dziecko powinno posiadać swój własny paszport od momentu, gdy jego dane biometryczne mogą zostać zakodowane w dokumencie podróży (musi zostać więc prowadzona rozporządzeniem granica wieku: albo ta zaproponowana przez Komisję we wniosku albo ta przyjęta pod wpływem opinii Europejskiego Inspektora Ochrony Danych Osobowych). EIOD poruszył również problem przechowywania danych biometrycznych, które powinno odpowiadać wymogom nałożonym przez legislatora unijnego w dziedzinie ochrony danych osobowych. Dwa podstawowe wspólnotowe akty prawne miały w tym czasie zastosowanie: Dyrektywa 95/46/EC Parlamentu Europejskiego i Rady z 14 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[42][43]oraz Rozporządzenie 45/2001/EC Parlamentu Europejskiego i Rady z 18 grudnia 2000 roku o ochronie osób fizycznych w związku z

[42] Dyrektywa 95/46/EC Parlamentu Europejskiego i Rady z 14 października 2004 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz. Urz. z 1995 r., L 281.

[43] Należy zauważyć, że obecnie ochrona danych osobowych, w tym danych biometrycznych, odbywa się na podstawie Rozporządzenia Parlamentu Europejskiego i Rady(UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. z 2016, L119 (tzw. RODO).

przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie danych[44]. Pierwszy z wymienionych aktów prawnych został wskazany zarówno w rozporządzeniu Rady nr 2252/2004 jak i we wniosku rozporządzenia Komisji zmieniającego rozporządzenie Rady, jako podstawa, na której opierać miała się między innymi ochrona danych biometrycznych zawartych w dokumencie podróży. EIOD zwrócił jednak uwagę, że rozporządzenie Rady oraz wniosek Komisji zezwalały w pewnym stopniu na działania mogące zagrozić bezpieczeństwu zapisanych identyfikatorów biometrycznych. Przywołane akty prawne pozwalały bowiem na zakładanie przez państwo członkowskie centralnej bazy danych, w której gromadzone byłyby dane biometryczne znajdujące się w dokumentach podróży obywateli danego państwa. Według Europejskiego Inspektora Ochrony Danych Osobowych taka praktyka była niedopuszczalna, gdyż umożliwiała wykorzystanie danych również do innych celów niż przewidywane w rozporządzeniu i we wniosku. EIOD zaproponował więc wprowadzenie do rozporządzenia przepisu, który wymusiłby przechowywanie danych biometrycznych w sposób zdecentralizowany, tzn. na bezprzewodowym mikroprocesorze w paszporcie.

EIOD zwrócił także uwagę, że ani rozporządzenie Rady z 2004 roku ani zmiany tego rozporządzenia proponowane przez Komisję, nie poruszały problemu tzw. odsetka błędnych odrzuceń na granicy (FRR czyli the false rejection rate). Jest to pewien procent osób, u których, podczas kontroli granicznej, porównanie identyfikatorów biometrycznych oraz próbek pobranej cechy biometrycznej dało wynik negatywny. Jako że urządzenia biometryczne nie dają stuprocentowej pewności co do swej skuteczności, istnieje pewne prawdopodobieństwo, że urządzenie dokonujące weryfikacji tożsamości dokona błędnego odrzucenia. EIOD domagał się więc wprowadzenia regulacji, które określiłyby procedurę, jaką należało zastosować w przypadku, gdy straż graniczna uznałaby, że ma do czynienia z błędnym odrzuceniem. EIOD proponował również, aby wprowadzić do rozporządzenia normy mówiące nie tylko o wysokości odsetka błędnych odrzuceń, ale także o wysokości odsetka nieudanych wpisów (FER – failure to enroll rate). Pod wpływem opinii Europejskiego Inspektora Ochrony Danych Osobowych, Parlament Europejski wystosował poprawki do wniosku rozporządzenia sporządzonego przez Komisję[45]. Piętnastego grudnia 2008 roku, przedstawione zostało

[44] Rozporządzenie 45/2001/EC Parlamentu Europejskiego i Rady z 18 grudnia 2000 roku o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie danych, Dz. Urz. z 2001 r., L 8.

[45] Projekt Rezolucji legislacyjnej Parlamentu Europejskiego w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach [podróży wydawanych przez państwa członkowskie, PE 405.718v02 – 00 A6 – 0500/2008].

sprawozdanie, w którym zawarte zostały proponowane zmiany. Parlament wziął pod uwagę sugestie EIOD co do podwyższenia granicy wieku, od której wydawane miały dzieciom dokumenty podróży z identyfikatorami biometrycznymi (Parlament co prawa opowiedział się za granicą wynoszącą 12 lat, a nie tak jak proponował EIOD 14 lat, jest to jednakże znaczna różnica biorąc pod uwagę pierwotną wersję rozporządzenia przedstawioną przez Komisję). Ciekawą propozycją wysuniętą przez Parlament było wydanie tzw. paszportu na 12 miesięcy w przypadku, gdy pobranie odcisków palców było „chwilowo niemożliwe". Niestety Parlament nie doprecyzował, co miał na myśli wprowadzając tego typu niedookreślone pojęcia, pozostawiając tym samym tę kwestię do rozstrzygnięcia w przyszłości państwom członkowskim (możemy się tylko domyślać, że chodziło o takie problemy jak oparzenia powodujące czasowy zanik linii papilarnych). Parlament wnioskował również o wprowadzenie normy, która gwarantowałaby, że zostaną przeprowadzone badania mierzące m.in. średni odsetek fałszywych odrzuceń w państwach członkowskich. Ponadto, aby uniknąć ryzyka wycieku danych, Parlament starał się przeforsować, aby tylko specjalnie wykwalifikowane osoby w danym państwie były upoważnione do pobierania danych biometrycznych. Z powyższych poprawek wynikało, że przynajmniej w pewnej części Parlament odniósł się do krytycznych uwag wystosowanych pod adresem wniosku Komisji przez Europejskiego Inspektora Ochrony Danych Osobowych.

Ostatecznie w 2009 r. pojawiło się Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 444/2009 z dnia 28 maja 2009 r. zmieniające rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i w dokumentach podróży wydawanych przez państwa członkowskie[46]. Biorąc pod uwagę krytykę rozporządzenia z 2004 roku, prawodawca unijny prowadził ujednolicone odstępstwa od konieczności pobierania wzorców linii papilarnych do celów paszportowych. Zwolnione z tego obowiązku zostały dzieci do 12 roku życia, a także osoby od których pobieranie odbitek palców jest fizycznie niemożliwe. Prawodawca wspólnotowy dopuścił także możliwość wydawania paszportów tymczasowych (na 12 miesięcy) osobom, od których czasowo nie można pobrać linii papilarnych w celu stworzenia wzorca biometrycznego. Dodatkowo wzięte zostały pod uwagę sugestie EIOD dotyczące konieczności wprowadzenia przepisów dotyczących rejestrowania wzorców przez wykwalifikowany personel w zgodzie ze standardami gwarantującymi poszanowanie godności osoby.

[46] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 444/2009 z dnia 28 maja 2009 r. zmieniające rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i w dokumentach podróży wydawanych przez państwa członkowskie, Dz. Urz. z 2009, L 142.

Nowe rozporządzenie nie odniosło się jednak do problemu infrastruktury przechowywania wzorców linii papilarnych pozostawiając to do indywidualnego rozstrzygnięcia państwom członkowskim.

4.1.1. Konkretne wykorzystanie biometrii w Unii Europejskiej

Pomimo wątpliwości, jakie pojawiały się w początkowej fazie wykorzystywania technologii biometrycznej, legislator unijny postanowił konsekwentnie wprowadzać nowoczesne metody zabezpieczeń do tworzonych przez siebie systemów pomagających w zwiększeniu poziomu bezpieczeństwa na granicach Unii. Komisja, w celu podkreślenia wagi jaką przywiązuje do wdrażania technologii biometrycznej, wydała 24 listopada 2005 roku Komunikat skierowany do Rady oraz Parlamentu Europejskiego w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych[47]. Komunikat zwracał uwagę na trzy konkretne, istniejące już w ramach Wspólnoty, systemy: EURODAC, SIS II oraz VIS. Według Komisji wprowadzenie technologii biometrycznej do wyżej wymienionych systemów doprowadzić miało zarówno do usprawnienia kontroli na granicach, jak i do zwiększenia bezpieczeństwa wewnętrznego Unii. Wprowadzone zmiany miały więc pomóc w realizacji celów jakie stawia sobie Unia w tym zakresie, a mianowicie z jednej strony, rozwijanie zasady swobodnego przepływu osób, a z drugiej walki z terroryzmem oraz innymi poważnymi przestępstwami. Warto przyjrzeć się więc systemom wspomnianym w komunikacie wystosowanym przez Komisję.

4.1.2. EURODAC

EURODAC jest systemem będącym częścią wspólnej polityki azylowej prowadzonej przez Unię Europejską. Początki tej polityki sięgają Konwencji Dublińskiej uchwalonej w 1990 roku, która wprowadzić miała zasady, jakimi kierować się będą Państwa Członkowskie udzielając azylu obywatelom państw trzecich. W oparciu o powyższą Konwencję (tzw. Dublin I) w 2003 roku, wdrożone zostało Rozporządzenie nr 343/2003/EC ustanawiające kryteria i mechanizmy

[47] Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final.

określenia Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl wniesionego w jednym z Państw Członkowskich przez obywatela Państwa Trzeciego (zwane Dublin II)[48]. Jak można to wyczytać z nazwy rozporządzenia, znajdowały się w nim regulacje, które szczegółowo wskazywały, w jakiej sytuacji dane państwo jest właściwe do rozpatrzenia wniosku o azyl. Ogólną zasadą, która pojawiła się już w Konwencji Dublin I było to, aby odpowiedzialność spadała na organy administracyjne członka wspólnoty, do którego wniosek został złożony po raz pierwszy.

Już w 1990 roku, ministrowie obradujący w Dublinie zdawali sobie sprawę, że wspólna polityka azylowa wymaga wprowadzenia systemu, dzięki któremu państwa mogłyby w łatwy sposób wymieniać informacje na temat danych osób ubiegających się o azyl. W przeciwnym razie powstałaby sytuacja, w której obywatele państw trzecich nie otrzymawszy zgody na pozostanie w jednym z Państw członkowskich, ubiegaliby się o azyl w innym. Taka praktyka byłaby szkodliwa dla istnienia spójnej polityki azylowej Unii. Dlatego też w 1991 roku, ministrowie zgodzili się na utworzenie w państwach Schengen systemu EURODAC, którego zadaniem miałoby być wypełnianie postanowień zawartych w Konwencji Dublin I (a później także Dublin II). Możliwości techniczne uniemożliwiły jednakże natychmiastowe wdrożenie EURODAC. Pierwszy akt prawny regulujący ten system powstał dopiero w grudniu 2000 roku. Rozporządzenie Rady (WE) nr 2725/2000 dotyczące ustanowienia systemu EURODAC do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej[49] powoływało do życia system, który miał być pomocny w przyznawaniu azylu. Jest to baza danych, w której gromadzone są odciski palców osób ubiegających się o azyl. Państwo Członkowskie, do którego zostaje złożony wniosek o azyl, pobiera od wnioskodawcy odciski dziesięciu palców, a następnie przesyła je w celu porównania, do centralnej bazy danych EURODAC ustanowionej przy Komisji Europejskiej. Przesłane dane zostają zarejestrowane w bazie, a następnie system dokonuje porównania otrzymanej próbki z obrazami linii papilarnych znajdującymi się już w pamięci systemu. W przypadku, gdy okaże się, że rezultat badania jest pozytywny, centralny system EURODAC przesyła informację o trafieniu do Państwa Członkowskiego, które przyjęło do rozpatrzenia wniosek o azyl. Kraj taki odsyła wtedy osobę ubiegającą się o azyl do Państwa, w którym po raz pierwszy złożyła ona wniosek. W ten sposób

[48] Rozporządzenie nr 343/2003/EC ustanawiające kryteria i mechanizmy określenia Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl wniesionego w jednym z Państw Członkowskich przez obywatela Państwa Trzeciego (zwane Dublin II), Dz. Urz. z 2003 r., L. 50.

[49] Rozporządzenie Rady (WE) nr 2725/2000 dotyczące ustanowienia systemu EURODAC do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, Dz. Urz. z 2002 r., L. 62.

udaje się uniknąć sytuacji, w której jeden z członków Unii podważałby wcześniej podjętą decyzję innego członka.

Rozporządzenie wyraźnie określało, że odbitki palców mogą być pobierane tylko od osób, które ukończyły 14 lat i tylko w sposób, który nie naruszałby praw zapisanych w Europejskiej Konwencji Praw Człowieka (chodzi tu głównie o poszanowanie prawa do prywatności oraz poszanowanie godności ludzkiej)[50]. Ponadto rozporządzenie wprowadzało pewne reguły, które miały zapewnić, że wykorzystywanie danych w postaci identyfikatorów biometrycznych, odbywać się będzie zgodnie z obowiązującymi w Unii aktami normatywnymi, które skupiają uwagę na ochronie danych osobowych. I tak w legislacji ustanawiającej system EURODAC wyraźnie zaznaczone było, że identyfikatory biometryczne nie mogą zostać wykorzystane do celów innych niż przewidziane w rozporządzeniu. Co za tym idzie, Rada domagała się, aby dostęp do danych znajdujących się w centralnej bazie, posiadały jedynie osoby upoważnione. Ponadto, co równie ważne, z rozporządzenia wynikało jasno, kiedy dane biometryczne miały zostać usunięte z systemu. Prawodawca Unijny przyjął, że przechowywanie odcisków palców nie może trwać dłużej niż dziesięć lat. Istniały jednakże sytuacje, w których identyfikatory biometryczne powinny były być usunięte z EURODAC wcześniej. Działo się tak w momencie, gdy osoba ubiegająca się o azyl otrzymała obywatelstwo jednego z państw członkowskich lub gdy opuściła terytorium Unii Europejskiej.

Dodatkową ochroną danych miało być wprowadzenie przepisu nakładającego na Państwo Członkowskie, do którego wpłynął wniosek o azyl, odpowiedzialność za bezpieczeństwo pobieranych przez nie identyfikatorów biometrycznych. W przypadku wykorzystania danych w sposób niezgodny z przepisami rozporządzenia, osoba lub Państwo Członkowskie, które poniosło szkodę w wyniku takiego działania, miało prawo domagania się odszkodowania.

System EURODAC mógł być również wykorzystywany w celu sprawdzenia czy osoba przebywająca nielegalnie na terenie jednego z Państw Członkowskich, złożyła wniosek o azyl w innym Państwie. Procedura porównywania wyglądała identycznie jak ta przedstawiona wyżej. Sytuacja ta różniła się jednak tym, że po sprawdzeniu czy dane odciski palców figurują w systemie EURODAC, nie były one zapamiętane w centralnej bazie danych.

Analizując historyczne ustawodawstwo Unijne regulujące działanie systemu EURODAC, trzeba przyznać, że Rada skupiła się nie tylko na wdrożeniu nowoczesnej technologii biometrycznej w celu usprawnienia prowadzenia spójnej polityki azylowej w granicach Unii, ale starała się również, aby wprowadzone rozwiązania nie naruszały postanowień dotyczących

[50] Konwencja Rady Europy o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r.

kwestii przetwarzania danych osobowych i ich przepływu ustanowionych na mocy ówczesnych aktów wspólnotowych takich jak Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Kilka lat funkcjonowania systemu EURODAC doprowadziło do wypracowania propozycji w sprawie nowego rozporządzenia dotyczącego systemu EURODAC. Był to wniosek rozporządzenia Parlamentu Europejskiego i Rady z dnia 3 grudnia 2008 r. dotyczący ustanowienia systemu EURODAC do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr […/…] [ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela kraju trzeciego lub bezpaństwowca[51]. Nowe rozporządzenie miało wprowadzać zmiany będące odpowiedzią na zarzuty postawione prze Komisję w sprawozdaniu z oceny systemu dublińskiego[52], w którym część poświęcona była funkcjonowaniu systemu EURODAC w latach 2003 – 2005. Ze sprawozdania można między innymi wyczytać, że niektóre państwa członkowskie spóźniały się z przesyłaniem odcisków palców do systemu centralnego, co często powodowało trudności w późniejszym ustaleniu, w którym kraju wniosek o azyl został złożony po raz pierwszy. Ponadto wymiana obrazów identyfikatorów biometrycznych nie była tak sprawna jak życzył sobie tego prawodawca Unijny wprowadzając wyżej wymieniony system. Dlatego też we wniosek rozporządzenia proponowano pewne rozwiązania, których konieczność wprowadzenia wymusiło zastosowanie systemu EURODAC w praktyce. Nowe prawodawstwo wprowadzać miało konkretne terminy, w których państwo przyjmujące wniosek miało przesłać obraz linii papilarnych do bazy centralnej. System centralny był zobligowany do porównania w ciągu 24 godzin otrzymanych odcisków palców z tymi, które znajdują się w jego bazie. Doprowadzić to miało do szybszego i sprawniejszego przepływu danych na temat osób ubiegających się o azyl. Poza tym, do przesyłania danych miały zostać zastosowane dostępne ówcześnie nowoczesne technologie cyfrowe, które zastąpić miały te używane dotychczas. Oprócz usprawnienia systemu, miało to jeszcze tę zaletę, że cyfrowy przekaz danych miał być bezpieczniejszy z punktu widzenia ochrony danych osobowych.

[51] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 3 grudnia 2008 r. powołującego system EURODAC do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr […/…] [ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela kraju trzeciego lub bezpaństwowca], COM(2008) 825, wersja ostateczna.

[52] Sprawozdanie Komisji do Parlamentu Europejskiego i Rady z oceny systemu dublińskiego (COM(2007)299, wersja ostateczna) {SEC(2007) 742}.

Wyżej wymieniony wniosek rozporządzenia został przeanalizowany przez Europejskiego Inspektora Ochrony Danych Osobowych, który 18 lutego 2009 roku wydał opinię[53] dotyczącą wprowadzenia proponowanego aktu. Opinia bardzo pochlebnie wypowiada się na temat wniosku rozporządzenia Parlamentu Europejskiego i Rady. EIOD zauważył, że wiele aspektów proponowanych przez niego w innych opiniach dotyczących wykorzystana danych osobowych (w tym identyfikatorów biometrycznych) w systemach utworzonych w celu harmonizowania wspólnej polityki granicznej, zostało wziętych pod uwagę w powyższym wniosku. Ostatecznie w życie weszły dwa rozporządzenia, na mocy których funkcjonuje obecnie system EURODAC: Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca[54] oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona)[55].

---

[53] Opinion of the European Data Protection Supervisor on the proposal for the regulation of the European Parliament and the Council concerning the establishment of EURODAC for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (COM(2008)825).

[54] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca, Dz. Urz. z 2013 r., L 180.

[55] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona), Dz. Urz. z 2013 r., L. 180.

4.1.3. SIS II

System Informacyjny Schengen II (SIS II) jest elementem polityki Unii, która prowadzić ma do poprawienia bezpieczeństwa na terenie państw należących do strefy Schengen, ustanowionej w pierwotnym kształcie, w 1985 roku. W 1990 roku, na mocy konwencji wykonawczej do układu z Schengen[56], porozumiewające się strony zadecydowały o utworzeniu Systemu Informacyjnego Schengen pierwszej generacji (SIS I – Schengen Information System I). Istnienie SIS I opierało się na stworzeniu komputerowej bazy danych, w której państwa zamieszczały informacje na temat poszukiwanych osób i przedmiotów. Ponadto, sięgając do SIS I, można było się dowiedzieć, czy dana osoba nie jest niejawnie nadzorowana lub czy nie dotyczy jej zakaz wstępu na terytorium Wspólnoty. Stworzenie systemu miało pomóc Państwom Członkowskim w sprawnej wymianie informacji, co miało przyczynić się do zwiększenia poczucia bezpieczeństwa obywateli Unii, jak również stanowiło jeden z elementów stopniowego znoszenia kontroli granicznych pomiędzy państwami, które podpisały układ z Schengen. Jako przesłanki uzasadniające zastąpienie Systemu Informacyjnego Schengen pierwszej Generacji Systemem Informacyjnym Schengen drugiej generacji, zarówno Rozporządzenie Rady nr 2424/2001 w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II)[57] jak i decyzja Rady o tym samym tytule[58] podają brak dostosowania SIS I do warunków, w których Unia Europejska uległa powiększeniu o nowych członków oraz konieczność rozwoju systemu wprowadzając do niego nowoczesne rozwiązania technologiczne. Niewątpliwą nowością, którą odnajdujemy w SIS II jest wprowadzanie do systemu identyfikatorów biometrycznych. Rozporządzenie Parlamentu Europejskiego i Rady nr 1987/2006[59] stanowi, że cechami biometrycznymi mającymi podlegać sprawdzeniu przez system będą odciski palców oraz obraz twarzy obywateli państw trzecich. Rozporządzenie wskazuje również, że zarówno odciski palców jak i fotografie biometryczne wykorzystywane są jedynie po to, aby dokonać weryfikacji tożsamości osoby, której personalia zostały już ustalone na podstawie innych danych zawartych w systemie (jak miejsce i data urodzenia,

[56] Konwencja wykonawcza do Układu z Schengen z dnia 14 czerwca 1985 r. w sprawie stopniowego znoszenia kontroli na wspólnych granicach z 1990 r.
[57] Rozporządzenie Rady (WE) nr 2424/2001 z dnia 6 grudnia 2001 roku w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji, Dz. Urz. z 2001 r., L 328.
[58] Decyzja Rady z dnia 6 grudnia 2001 roku w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. z 2001 r., L 328.
[59] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1985/2006 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. z 2006 r., L 381.

obywatelstwo itp.). Zarazem rozporządzenie z 2006 roku i jak decyzja Rady wydana rok później[60] wprowadziły zastrzeżenie, że w przypadku, gdy stanie się to technicznie możliwe, identyfikatory biometryczne miały być podstawą weryfikacji tożsamości, a nie tylko środkiem pomocniczym.

System Informacyjny Schengen składa się z systemu centralnego (składającego się z kolei z funkcji wsparcia technicznego „CS – SIS" oraz jednolitego interfejsu krajowego „NI – SIS"), systemu krajowego „N. SIS II" oraz infrastruktury łączności pomiędzy CI – SIS a NI – SIS. W ramach systemów krajowych funkcjonują bazy danych, do których Państwo Członkowskie wprowadza identyfikatory biometryczne pobrane od obywatela państwa trzeciego. Następnie, otrzymany obraz przesyłany jest do centralnej bazy danych SIS II znajdującej się w Salzburgu, w Austrii, gdzie weryfikowane jest czy dana osoba nie figuruje już w systemie jako osoba poszukiwana, niejawnie nadzorowana czy też mająca zakaz wstępu na terytorium Unii.

Jako że ustawodawca unijny przywiązuje znaczą wagę do ochrony danych osobowych, również i przy okazji wdrażania legislacji dotyczącej funkcjonowania Systemu Informacyjnego Schengen II, problem ten został uregulowany dość obszernie. Już na etapie wprowadzania danych do systemów krajowych, rozporządzenie z 2006 roku wskazywało konkretnie, w jakich sytuacjach identyfikatory biometryczne mogą być umieszczane w bazie danych (uwaga autorki skupia się na identyfikatorach biometrycznych, rozporządzenie jednakże nie czyni rozróżnienia pomiędzy danymi biometrycznymi, a pozostałymi danymi wpisywanymi do systemu). Ponadto wpisy mogły być przechowywane jedynie przez trzy lata. W szczególnych przypadkach mogły one być przechowywane dłużej. Został również ustalony katalog podmiotów, które miały dostęp do centralnej bazy danych SIS II (jest to na przykład policja czy straż graniczna). Dodatkowym zabezpieczeniem w tej dziedzinie było to, że System Informacji Schengen zaprojektowany został jako system hit/no hit co oznacza, że w celu uzyskania precyzyjnych informacji tłumaczących, dlaczego dane sprawdzanej osoby znajdują się w centralnej bazie danych, należało złożyć wniosek do podmiotów obsługujących program SIRENE (Supplementary Information Request at National Entries – wniosek o informacje uzupełniające na wejściach krajowych) o uzupełnienie informacji otrzymanych z SIS II. SIRENE jest bowiem narzędziem wykonawczym dla SIS II[61] zabezpieczającym przez zbyt łatwym przepływem wrażliwych danych osobowych.

---

[60] Decyzja Rady 2007/533 z dnia 12 czerwca 2007 roku w sprawie utworzenia, funkcjonowania i używania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. z 2007 r., L. 205.

[61] Decyzja Komisji z dnia 4 marca 2008 roku w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla Systemu Informacyjnego Schengen drugiej generacji (SIS II), notyfikowana jako dokument nr C(2008) 774, Dz. Urz. z 2008 r., L 123.

W swojej opinii z 19 października 2006 roku[62] Europejski Inspektor Ochrony Danych Osobowych poświęcił sporo uwagi rozwiązaniom biometrycznych wprowadzonym do systemu SIS II. EIOD postulował, aby do prawodawstwa dotyczącego Systemu Informacji Schengen wprowadzić regulację precyzyjnie określającą procedurę wpisywania do systemu, przez uprawnione podmioty w państwie, danych biometrycznych. Zbyt ogólne zasady powodują bowiem, że państwa mają dużą swobodę w tym zakresie, co w konsekwencji mogło prowadzić do różnic w ustawodawstwach krajowych. EIOD uważał procedurę wpisywania za kluczowy element prawidłowego funkcjonowania systemu SIS, dlatego też kładł nacisk na wypracowanie wspólnych norm w tej dziedzinie.

Ponadto EIOD podkreślił, że dane biometryczne nie dają stuprocentowej pewności wiarygodności i nie można na nich polegać bez zastrzeżeń. Jak możemy przeczytać w opinii „(…) Dane biometryczne „żyją" i ewoluują z czasem; próbki przechowywane w bazie danych stanowią jedynie zapis chwilowego stanu dynamicznego elementu. Ich aktualność nie jest absolutna i musi być kontrolowana. Dokładność danych biometrycznych musi być zawsze rozpatrywana z perspektywy innych elementów, gdyż nigdy nie jest ona wartością absolutną."[63].

Zgodnie z komunikatem prasowym Komisji Europejskiej, system SIS II ruszył 9 kwietnia 2013r.[64]. Dodatkowym atutem SIS II jest możliwość korzystania z niego nie tylko przez Państwa Członkowskie, ale również przez państwa stowarzyszone, takie jak Norwegia czy Szwajcaria.

4.1.4. VIS

Podstawa prawna do funkcjonowania Wizowego Systemu Informacyjnego (VIS – Visa Information System) znalazła się w Decyzji Rady z dnia 8 czerwca 2004 roku w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS).[65] Rada zwróciła uwagę, że wspólna

---

[62] Opinia Europejskiego Inspektora Ochrony Danych Osobowych z października 2006 r., Dz. Urz. z 2006 r., C 91/38:

- w sprawie wniosku dotyczącego decyzji Rady w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II),
- w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie utworzenia, eksploatacji i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II),
- w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie dostępu służb odpowiedzialnych w Państwach Członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji.

[63] Ibidem.

[64] https://ec.europa.eu/commission/presscorner/detail/pl/IP_13_309 (dostęp 11.11.2020).

[65] Decyzja Rady (WE) nr 512/2004 z dnia 8 czerwca 2004 roku w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz. Urz. z 2004 r., L 213.

polityka wizowa jest elementem porozumienia z Schengen mającego na celu, z jednej strony ułatwienie swobodnego przepływu osób na terenie Wspólnoty, a z drugiej podniesienie bezpieczeństwa poprzez prowadzenie spójnej polityki na granicach Unii. Prawodawstwo w tej dziedzinie ma także w znacznym stopniu zmniejszyć ryzyko występowania zjawiska handlu wizami, jak również ułatwić uprawnionym podmiotom zweryfikowanie, czy osoba przebywająca na obszarze Schengen posiada wymaganą do tego wizę. Jednakże, aby poznać funkcjonowanie VIS należało w tym czasie sięgnąć do Wniosku rozporządzenia Parlamentu Europejskiego i Rady z dnia 31 maja 2006 roku, zmieniającego Wspólne Instrukcje Konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczącego wiz w związku z wprowadzeniem technologii biometrycznych, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków wizowych (wniosek przedstawiony przez Komisję)[66]. We wniosku dotyczącym Wspólnych Instrukcji Konsularnych (WIK) można było przeczytać, że identyfikatorami biometrycznymi, które miały zostać pobrane od osób składających wniosek o wizę, były odciski palców oraz fotografia twarzy obywatela państwa trzeciego. Podobnie jak to miało miejsce przy okazji rozporządzenia Rady z 2004 roku, tak i tutaj pobranie próbki cech biometrycznych, a następnie wprowadzenie jej do systemu, odbywać się miało zgodnie z normami zaleconymi w dokumencie nr 9303 Międzynarodowej Organizacji Lotnictwa Cywilnego. Ponadto identyfikatory biometryczne miały być przechowywane w Systemie Informacji Wizowej, a nie jak to było wcześniej planowane na bezdotykowym układzie scalonym, który miał być dołączony do każdej nalepki wizowej. Zmiana ta wynikała z trudności technicznych, jakie mogłyby powstać przy próbie wprowadzenia takiego rozwiązania. WIK przewidywał również dwie kategorie osób stanowiących wyjątki od obowiązkowego pobierania odcisków palców. Są to: dzieci poniżej szóstego roku życia oraz osoby, od których pobranie odcisków palców jest fizycznie niemożliwe. W stosunku do tych osób zastosowanie znajduje procedura awaryjna, która wyraża się w dołączeniu dopisku: „nie dotyczy" w odpowiedniej rubryce systemu VIS

Warto przyjrzeć się jeszcze jednej kwestii zawartej we wniosku rozporządzenia dotyczącego Wspólnych Instrukcji Konsularnych, która miała znaczenie ze względu na ochronę danych biometrycznych przechowywanych w systemie VIS. WIK wychodząc naprzeciw trudnościom, jakie mogło mieć państwo z przyjmowaniem i rejestrowaniem wniosków wizowych,

[66] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 31 maja 2006 roku, 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 (wniosek przedstawiony przez Komisję), COM/2006/0269 końcowy – COD 2006/0088.

proponowało zezwolić na wprowadzenie dwóch typów rozwiązań. Pierwsze z nich to ustanowienie jednego, wspólnego miejsca przyjmowania wniosków wizowych dla kilku państw. Drugie to możliwość zlecenia firmie zewnętrznej wykonywania pewnych usług w ramach funkcjonowania systemu VIS. Zwłaszcza to drugie rozwiązanie zostało przyjęte z niepokojem przez instytucje Unijne zajmujące się nadzorem nad przestrzeganiem legislacji dotyczącej ochrony danych osobowych. Zarówno Europejski Inspektor Ochrony Danych Osobowych w swej opinii wydanej 27 października 2006 roku dotyczącej wniosku 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[67], jak i opinia Grupy Roboczej do spraw Ochrony Danych z dnia 1 marca 2007 roku[68], zauważyły, że choć korzystanie z usług podmiotów zewnętrznych uregulowane było we wniosku rozporządzenia w sposób bardzo dokładny, przepisy te budziły jednak wątpliwość co do bezpieczeństwa danych biometrycznych (oraz oczywiście innych danych osobowych) znajdujących się w systemie. Oba podmioty zauważyły, że zweryfikowanie wiarygodności oraz stopnia zaufania do pracowników zewnętrznego usługodawcy może okazać się bardzo trudne. Poza tym EIOD słusznie podkreślił, że zmienna sytuacja polityczna może oddziaływać na podmiot zewnętrzny, co w konsekwencji może doprowadzić do trudności w wypełnianiu przez niego zobowiązań dotyczących bezpiecznego przetwarzania danych osobowych, w tym identyfikatorów biometrycznych. W jednej ze swoich wcześniejszych opinii EIOD podkreślił, że „Biometria (…) zmienia w sposób nieodwracalny stosunek pomiędzy ciałem a tożsamością: cechy ciała ludzkiego stają się przedmiotem odczytu maszynowego i mogą być dalej wykorzystywane. Nawet jeśli cechy biometryczne nie są rozpoznawalne dla ludzkiego oka, to można je zawsze odczytać i wykorzystać przy zastosowaniu odpowiednich narządzi, bez względu na miejsce przebywania danej osoby”[69]. EIOD zauważył więc, że ze względu na wrażliwość tych danych,

---

[67] Opinia Europejskiego Inspektora Danych Osobowych z 27 października 2006 r. dotycząca wniosku 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, Dz. Urz. z 2006 r., C 321.

[68] 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.

[69] Opinia Europejskiego Inspektora Ochrony Danych Osobowych z dnia 23 marca 2005 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz

dopuszczanie do nich podmiotu zewnętrznego powinno stanowić ostateczne rozwiązanie, a kiedy nie da się już tego uniknąć należy stworzyć warunki, aby przetwarzanie danych przez usługodawcę zewnętrznego odbywało się w miejscu, w którym zapewniona jest ochrona dyplomatyczna. Takowa możliwa jest zgodnie z prawem międzynarodowym na podstawie Konwencji Wiedeńskiej z 18 kwietnia 1961 r. o stosunkach dyplomatycznych, która stanowi: „Pomieszczenia misji są nietykalne. Funkcjonariusze państwa przyjmującego nie mogą do nich wkraczać, chyba że uzyskają zgodę szefa misji (…). Pomieszczania misji, ich urządzenia i inne przedmioty, które się w nich znajdują, oraz środki transportu misji nie podlegają rewizji, rekwizycji, zajęciu lub egzekucji”[70] .

EIOD, podobnie jak to miało miejsce w opinii z 2005 dotyczącej wniosku rozporządzenia zmieniającego rozporządzenie Rady nr 2252/2004, odniósł się do odstępstw od obowiązku pobierania odcisków palców, jakie zostały wprowadzone we Wspólnych Instrukcjach Konsularnych. Jak i wcześniej, tak i tutaj Europejski Inspektor Ochrony Danych Osobowych krytykował wprowadzenie regulacji, która pozwala na pobieranie obrazu linii papilarnych od małych dzieci. EIOD zauważył, że granica wprowadzona w ramach systemu EURODAC (czyli pobieranie odcisków palców od osób, które ukończyły 14 lat) jest rozwiązaniem, które powinno zostać wdrożone również w innych systemach wykorzystujących technologię opartą na identyfikatorach biometrycznych. W podobny sposób EIOD wypowiedział się na temat wykonywania biometrycznego obrazu twarzy dzieciom. W swej opinii Inspektor wyraził wątpliwości co do przydatności zamieszczania zdjęć dzieci w celu identyfikacji czy weryfikacji. Ponieważ rysy twarzy dziecka się zmieniają, fotografia zamieszczona w VIS - ie powinna służyć jedynie jako element uzupełniający w procesie weryfikacji tożsamości osoby.

W stosunku do drugiej kategorii osób zwolnionych od wymogu posiadania zapisanego w VIS identyfikatora biometrycznego w postaci obrazu linii papilarnych (fizyczna niemożność pobrania), EIOD podkreślił, że niemożność pobrania próbki cechy biometrycznej, nie może prowadzić do częstszej odmowy wydawania wizy takim podmiotom.

Aktem prawnym Unii regulującym funkcjonowanie systemu VIS obecnie jest rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 roku w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami

wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych, Dz. Urz. z 2005 r., C 181.

[70] Konwencja wiedeńska z dnia 18 kwietnia 1961 r. o stosunkach dyplomatycznych, art. 21.

członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS)[71]. Zgodnie z postanowieniami rozporządzenia system VIS składa się, podobnie jak SIS z centralnego systemu informacyjnego (jest to centralna baza danych zlokalizowana w Strasburgu), z interfejsu krajowego (baza danych Państwa Członkowskiego, do której wprowadza się dane osoby ubiegającej się o wizę) oraz z infrastruktury, która umożliwia wymianę danych pomiędzy bazą centralną, a systemami krajowymi. Podczas rejestracji wniosku wizowego w Państwie Członkowskim, upoważnieni pracownicy wprowadzają do krajowego systemu VIS dane osoby ubiegającej się o wizę. Wśród nich znajdują się pobrane wcześniej identyfikatory biometryczne w postaci obrazu twarzy oraz dziesięciu odcisków palców wnioskodawcy.

Ciekawą regulacją pojawiającą się w rozporządzeniu jest wskazanie, że to państwo członkowskie jest odpowiedzialne za dane wpisywane i przechowywane w krajowym systemie VIS, nawet jeśli państwo to korzysta z usług podmiotu zewnętrznego. Ponadto rozporządzenie, powołując się na decyzję Rady nr 633/2008 z dnia 23 czerwca 2008 roku w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania[72], zezwala w wyżej określonych celach na dostęp Europolu do danych osobowych znajdujących się w systemie VIS (w tym także do identyfikatorów biometrycznych).

4.2. Ustawodawstwo polskie

Ustawodawstwo polskie w dziedzinie wykorzystana zabezpieczeń biometrycznych nie miało zbyt długiej historii przed wstąpieniem do Unii Europejskiej. W zasadzie wszelkie uregulowania prawne powstały z powodu obowiązku wdrażania do porządków krajowych aktów normatywnych wydawanych na szczeblu wspólnotowym. W przypadku wprowadzania paszportów biometrycznych polskie ustawodawstwo bazowało na wspomnianym wyżej Rozporządzeniu Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych

[71] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 roku w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz. Urz. z 2008 r., L. 218 ze zm.

[72] Decyzja Rady nr 633/2008 z dnia 23 czerwca 2008 roku w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz. Urz. z 2008 r., L 218 ze zm.

biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie. Na podstawie rozporządzenia na Polskę został nałożony obowiązek wprowadzania do książeczki paszportowej zapisanego cyfrowo obrazu twarzy. Według aktu unijnego dokumenty z takim zabezpieczeniem miały być wydawane najpóźniej od 28 sierpnia 2006 roku. Wymóg wprowadzenia drugiego identyfikatora biometrycznego, mianowicie zakodowanych na mikroprocesorze odcisków palców, miał zostać spełniony najpóźniej do czerwca 2009 roku. Aby dostosować prawo polskie do standardów ustalonych przez Wspólnotę, krajowy legislator uchwalił 13 lipca 2006 roku Ustawę o dokumentach paszportowych[73]. Jednakże, przed wejściem w życie ustawy, Urząd do Spraw Repatriacji i Cudzoziemców, działający w ramach Ministerstwa Spraw Wewnętrznych i Administracji opublikował Program dostosowania systemu paszportowego oraz dokumentów podróży wydawanych cudzoziemcom przez władze polskie do wymogów prawa unijnego[74]. Program ten określał cele i korzyści, jakie płyną z wprowadzenia nowoczesnych dokumentów podróży. Głównym celem był wspomniany już wyżej obowiązek wdrażania prawa unijnego, jaki Polska przyjęła na siebie stając się 1 maja 2004 roku członkiem Unii Europejskiej. Drugi równie ważny stanowiła większa ochrona, jaką daje zastosowanie mikroprocesora z zakodowanymi danymi biometrycznymi przed różnego rodzaju próbami fałszowania dokumentów. Program określił również wymagania, zarówno techniczne, jak i prawne, jakie miały zostać spełnione, aby wdrażanie nowego wzoru paszportu przebiegało nie tylko sprawnie, ale i zgodne z normami ustanowionymi do ochrony danych osobowych. Zmiany, które miały zostać wprowadzone w ramach nowego ustawodawstwa powinny były, według Programu MSWiA, pojawić się w kilku etapach, w trzech aspektach: prawnym, organizacyjnym oraz technicznym. W przypadku zmian prawnych i organizacyjnych bardzo duży nacisk położony został na bezpośrednią lub pośrednią ochronę danych biometrycznych (jako że główną zmianą w nowych paszportach miało być wprowadzenie tych właśnie danych, Program skupiał się w dużej mierze na ich ochronie). Aby zrealizować ten cel należało wprowadzić specjalne jednostki podlegające MSWiA uprawnione do pobierania identyfikatorów biometrycznych od osób wnioskujących o wydanie paszportu. Poza tym, jako że informacje zapisane na mikroprocesorze, są bardzo ściśle związane z osobą, od której zostały pobrane, konieczne było wprowadzenie wymogu osobistego odbioru książeczki paszportowej. W przypadku nieodebrania dokumentu, bądź wydania wadliwego paszportu, Program zakładał zainicjowanie procedury niszczenia dokumentów w taki sposób,

[73] Ustawa o dokumentach paszportowych z dnia 13 lipca 2006 r., Dz. U. z 2006 r. Nr 143, poz. 1027 ze zm.
[74] Program dostosowania systemu paszportowego oraz dokumentów podróży wydawanych cudzoziemcom przez władze polskie do wymogów prawa unijnego, dostępny na stronie: www.mswia.gov.pl.

aby nie zaistniało zagrożenie wycieku informacji. Ponadto, ochrona danych wyrażać się miała w utworzeniu specjalnej ewidencji, w której umieszczane miały być informacje zawarte w dokumencie podróży. Dostęp do tak stworzonej bazy danych miałyby mieć - w ściśle określonym celu - jedynie podmioty do tego uprawnione[75]. W zakresie zmian technologicznych Program zakładał wprowadzenie nowego wzoru książeczek paszportowych, który dostosowany miał być do wymagań stawianych przez Unię Europejską[76].

Jak to już zostało wyżej wspomniane, wdrożenie Programu Ministerstwo Spraw Wewnętrznych i Administracji podzieliło na trzy etapy. Zgodnie z planem w ramach realizacji pierwszej fazy w 2005 roku zainicjowany został Pilotażowy System Wydawania Paszportów z danymi biometrycznymi (PSWP). Pilotaż polegał na dołączaniu do paszportów dyplomatycznych chipów, na których zakodowane zostały identyfikatory biometryczne. Drugi etap przypadać miał na rok 2006 i skupiał się w dużej mierze na wprowadzaniu do książeczki paszportowej biometrycznego obrazu twarzy jej posiadacza. Trzeci natomiast przypadał na lata 2007 - 2009 i przygotowywał Polskę do wdrożenia drugiej, wymaganej przez ustawodawcę unijnego, cechy biometrycznej[77].

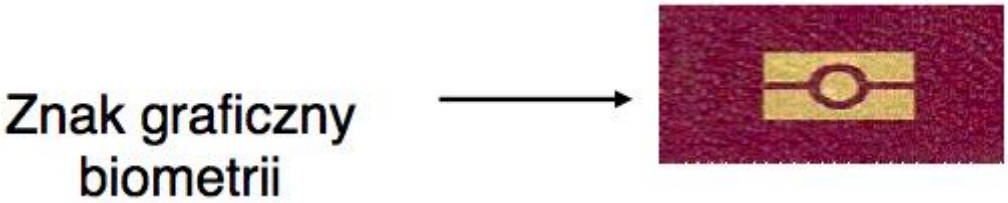
W myśl realizacji opartego na wymogach unijnych Programu MSWiA, ustawodawca polski wprowadził w życie wyżej wspomnianą ustawę o dokumentach paszportowych. Znajduje się w niej między innymi katalog danych, które mają znaleźć się w książeczce paszportowej. Wśród nich wyróżniają się dwa intersujące z perspektywy niniejszego opracowania elementy, nieistniejące we wcześniejszych regulacjach. Są to właśnie identyfikatory biometryczne. Ustawa wyróżnia cztery rodzaje paszportów, które mogą być wydawane na terytorium Polski. Są to: paszporty, paszporty tymczasowe, paszporty dyplomatyczne oraz paszporty służbowe Ministerstwa Spraw Zagranicznych. Obowiązek zamieszczenia identyfikatorów biometrycznych nie dotyczy jedynie paszportów tymczasowych, które to dokumenty podróży wydaje się między innymi osobom, od których czasowo nie można pobrać linii papilarnych. Ponadto polska regulacja przejęła zasadę „jedna osoba – jeden paszport", co w konsekwencji oznacza, że dzieci muszą posiadać własne paszporty i nie mogą być wpisywane w dokumenty rodziców.

[75] Ibidem.
[76] Ibidem.
[77] Ibidem.

Aspekt techniczny

Paszporty zaopatrzone w identyfikatory biometryczne posiadają specjalne, świadczące o tym oznaczenia. Można je zaobserwować na obecnie wydawanych polskich dokumentach podróży.

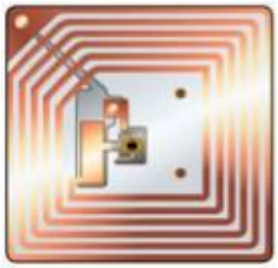
Ryc. 15. Paszport biometryczny (źródło: http://www.paszporty.mswia.gov.pl)



Ryc. 16. Znak graficzny biometrii (źródło: A. Dzwonek, T. Kling, „Biometria w dokumentach podróży", Człowiek i dokumenty, nr 10, Warszawa 2008)

Pobrane dane biometryczne zapisywane są na mikroprocesorze, który zamieszczany jest w tylnej stronie okładki dokumentu. Podczas zbliżania dokumentu z chipem do czytnika, odbiera on sygnał RFID (Radio Frequency Identyfication). Sygnał ten powoduje, że mikroprocesor wysyła drogą radiową zapisane na nim dane biometryczne do czytnika[78]. W taki sposób odbywa się kontrola dokumentów biometrycznych na granicy. Zgodnie z normami ICAO, dane znajdujące się na mikroprocesorze zabezpieczone powinny być zabezpieczone za pomocą co najmniej systemu Basic Access Control[79].

[78] A. Dzwonek, T. Kling, *Biometria w dokumentach podróży*, „Człowiek i Dokumenty" 2008, nr 10.
[79] http://www.mswia.gov.pl/index.php?dzial=298&id=3998 (dostęp 18.04.2009).



Ryc. 17. Mikroprocesor umieszczany w paszporcie (źródło: A. Dzwonek, T. Kling, „Biometria w dokumentach podróży", Człowiek i dokumenty, nr 10, Warszawa 2008)

Do połowy 2009 roku, jedyną cechą biometryczną, jaka zapisywana była na bezkontaktowym mikroprocesorze, był biometryczny obraz twarzy właściciela paszportu. Ministerstwo Spraw Wewnętrznych i Administracji wprowadziło zasady określające, gdzie i w jaki sposób fotografia miała zostać wykonana. Ustawodawca nie zdecydował się scentralizować placówek wykonujących zdjęcia zamieszczane następnie w dokumentach podróży. Zasadą jest, że fotografie robione są w prywatnych zakładach fotograficznych i dostarczane przez wnioskującego organom administracyjnym właściwym do wydawania paszportów. Zdjęcie musi mieć określone wymiary (szerokość 35mm, wysokość 45mm) oraz spełniać kryteria jakości wskazane w instrukcji ministerialnej[80].

Drugi identyfikator biometryczny, który według unijnych wytycznych miał znaleźć się w polskim paszporcie, również wymagał od organów odpowiedzialnych za wydawanie dokumentów podróży, kierowania się wskazówkami zawartymi w instrukcjach specjalnie do tego celu wydanych. Ponieważ Polska wdrażała procedury pobierania odbitek linii papilarnych w ostatnim dopuszczalnym przez Unię Europejską terminie, prawodawca krajowy mógł posiłkować się w tym względzie zasadami wypracowanymi już przez inne państwa członkowskie. I tak Niemcy wprowadziły instrukcję dla urzędników zajmujących się pobieraniem odcisków palców. Jak to już zostało ustalone na szczeblu unijnym, na mikroprocesorze zapisane miały być obrazy linii papilarnych obydwu palców wskazujących. Osoba, która wnioskowała o wydanie paszportu, musiała przyłożyć palce do urządzenia, a następnie wykonywane było zdjęcie. Procedurę powtarzało się trzy razy. Następnie system porównywał ze sobą zrobione zdjęcia i zapisywał tylko to, którego jakość była najlepsza. Pozostałe dwa zdjęcia usuwane były z systemu. Kolejnym etapem było przesłanie otrzymanego obrazu do podmiotu, który zajmuje się wykonywaniem dokumentów zabezpieczonych mikroprocesorem. W ramach ochrony danych osobowych w postaci identyfikatorów biometrycznych ustawodawca niemiecki zdecydował, że obrazy linii papilarnych usuwane

[80] https://www.gov.pl/web/gov/zdjecie-do-dowodu-lub-paszportu (dostęp 11.11.2020).

będą z bazy danych podmiotu produkującego paszporty w momencie wydania dokumentu wnioskodawcy[81]. W przypadku, gdy z jakichś przyczyn niemożliwe było pobranie odcisków palców z obu rąk (na przykład z powodu trwałego obrażenia ręki) należało wykonać zdjęcie linii papilarnych jednej ręki. Zasadą było, że na mikroprocesorze powinny, o ile to możliwe, znaleźć się dwa odciski palców[82]. Ponadto w instrukcji znajdowało się zastrzeżenie, że nie pobiera się odcisków palców od dzieci poniżej szóstego roku życia[83] [84]. Co ciekawe, ustawodawca niemiecki zwrócił również uwagę na możliwość wystąpienia sytuacji, w której wnioskodawca nie zgadza się na pobranie od niego obrazu linii papilarnych. W takim przypadku nie było możliwości wydania osobie paszportu elektronicznego, a jedyną możliwością było otrzymanie paszportu tymczasowego (aby jednakże został wydany paszport tymczasowy, musiały również być spełnione przesłanki określone w niemieckiej ustawie dotyczącej wydawania dokumentów podróży)[85].

Polsce zasady dotyczące pobierania identyfikatora biometrycznego w postaci odcisków palców znajdują się w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 2010r. w sprawie dokumentów paszportowych[86]. Rozporządzenie wskazuje zarówno sposób pobierania odcisków palców wskazujących, jak i wymienia procedury awaryjne, które muszą zostać zastosowane w przypadku braku możliwości stworzenia wzorca z tychże palców.

4.2.1. Wdrażanie SIS II, VIS oraz EURODAC

Jak już to było zaznaczone w poprzednich rozdziałach, Polska uczestniczyłała we wdrażaniu technologii biometrycznej nie tylko w formie zabezpieczeń znajdujących się w paszportach, ale także występujących w postaci systemów, które pomagają w usprawnieniu procesu swobodnego przemieszczania się po terenie Wspólnoty oraz w prowadzeniu jasnej i spójnej

---

81 http://www.warschau.diplo.de/Vertretung/warschau/pl/04/Informationen__Polen/bioPass__PL,property=Daten.pdf (dostęp 28.03.2009).

82 Ibidem.

83 Ibidem.

84 Ta zasada została następnie zmieniona w celu dostosowania się do nowej granicy wiekowej wskazanej w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 444/2009.

85 http://www.warschau.diplo.de/Vertretung/warschau/pl/04/Informationen__Polen/bioPass__PL,property=Daten.pdf (dostęp 28.03.2009).

86 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 2010 r. w sprawie dokumentów paszportowych, Dz. U. z 2010 r. Nr 151, poz. 1026 ze zm.

polityki azylowej (chodzi tu oczywiście o System Informacji Schengen SIS II, System Informacji Wizowej VIS oraz system EURODAC). Aby jednak sprostać wymaganiom legislatora unijnego, konieczne stało się wprowadzenie do porządku krajowego unormowań, które stwarzałyby jasne zasady funkcjonowania wspomnianych wyżej systemów. Dwa zadania, które były priorytetowe to: stworzenie odpowiedniej sieci informatycznej, która pozwoliłaby na sprawne funkcjonowanie systemów oraz wyznaczenie organów krajowych odpowiedzialnych za działanie wdrażanych rozwiązań zgodne z unijnymi normami odnoszącymi się do ochrony danych osobowych. Aby więc wypełnić należycie swoje zadania związane z przynależnością Polski do strefy Schengen, Ministerstwo Spraw Wewnętrznych i Administracji zaczęło wydawać, począwszy od roku 2004 dokumenty, w których zawarty był plan funkcjonowania rozwiązań unijnych na terenie naszego kraju (w zależności od zakresu regulacji tytuły planów różniły się między sobą: pierwszy chronologicznie plan powstały w 2004 roku nazwany został *Programem dla uczestnictwa Rzeczypospolitej Polskiej w realizacji tytułu IV konwencji wykonawczej Schengen*[87]*;* z kolei plan z 2006 roku był *Programem dostosowania organów administracji państwowej do współpracy z Systemem Informacyjnym Schengen II i Systemem Informacji Wizowej VIS*[88]).

Jeśli chodzi o aspekt techniczny SIS, to zgodnie z prawodawstwem unijnym miał się on składać z systemu centralnego, systemu krajowego oraz infrastruktury łączności pomiędzy systemem centralnym i krajowym (analogiczną budowę ma system VIS)[89]. Aby jednak zrozumieć funkcjonowanie Systemu Informacji Schengen oraz Systemu Informacji Wizowej w Polsce należy wspomnieć jeszcze o istnieniu Krajowego Systemu Informatycznego KSI, którego celem jest zbieranie i przetwarzanie danych, które następnie mogą być wykorzystywane przez uprawnione do tego podmioty w celu realizacji ich zadań. Ponieważ kategorie danych, jak również zakres organów upoważnionych do korzystania z informacji zapisanych w Systemie Informacji Schengen drugiej generacji oraz w Systemie Informacji Wizowej pokrywa się z tymi wymienionymi w regulacji dotyczącej Krajowego Systemu Informatycznego (organy te to m.in. Komendant Główny Policji, Komendant Główny Straży Granicznej, organy celne, Minister Sprawiedliwości), bazą do wdrożenia systemów VIS i SIS stały się właśnie informacje

[87] Program dla uczestnictwa Rzeczypospolitej Polskiej w realizacji tytułu IV konwencji wykonawczej Schengen, MSWiA, Warszawa, październik 2004 r., dostępny na stronie: www.mswia.gov.pl.

[88] Informacja o Programie dostosowania organów administracji państwowej do współpracy z Systemem Informacyjnym Schengen II i Systemem Informacji Wizowej VIS znajduje się na archiwalnej stronie: https://archiwum.premier.gov.pl/wydarzenia/decyzje-rzadu/program-dostosowania-organow-administracji-panstwowej-do-wspolpracy-z.html (dostęp 11.11.2020).

[89] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM%3Al14544 (dostęp 11.11.2020); https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM%3Al14517 (dostęp 11.11.2020).

zapisane w KSI. Miał on stać się łącznikiem pomiędzy Narodowym Interfejsem SIS II oraz Narodowym Interfejsem VIS, a Centralnym Systemem SIS i VIS [90]. Z wdrażaniem do porządku krajowego wyżej wymienionych systemów, które pomóc miały w budowaniu wzajemnej współpracy pomiędzy państwami członkowskimi Unii, wiązał się nieodłącznie problem ochrony danych osobowych, jakie miały znaleźć się w bazach systemów. Ustawa z dnia 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej[91] określała okoliczności, w których dane osoby (w tym oczywiście dane biometryczne) miały zostać zapisane w krajowych bazach systemów SIS i VIS, które następnie, w ramach współpracy pomiędzy państwami członkowskimi, miały zostać udostępnione w centralnych bazach SIS i VIS (kategorie te wypracowane na szczeblu unijnym, zostały implementowane do polskiego porządku prawnego). Znając cel, do jakiego zostały powołane powyższe systemy, nie nastręcza problemu zrozumienie idei wprowadzenia przepisu pozwalającego na wykorzystywanie danych nawet bez wiedzy i woli osób, których zebrane informacje dotyczą[92]. Aby jednak zapobiec nadużyciom, które mogły się pojawić w związku z powyższą regulacją, ustawa z 2007 roku określiła, że organem odpowiedzialnym za kontrolę nad prawidłowym zbieraniem, przetwarzaniem, przechowywaniem oraz udostępnianiem danych sprawuje Generalny Inspektor Ochrony Danych Osobowych[93][94]. W tym celu Generalny Inspektor miał ustawowo zapewniony bezpośredni dostęp do bazy danych Krajowego Systemu Informatycznego. Jednocześnie polska ustawa o SIS i VIS nakładała na wszystkie podmioty, które według regulacji mają dostęp do wrażliwych danych, obowiązek takiego korzystania z dostępnych systemów, który zgodny będzie ze standardami będącej ówcześnie w mocy Ustawy o ochronie danych osobowych (która odpowiadała w swoim brzmieniu występującym w tej materii przepisom unijnych). W przypadku, gdy osoba działała wbrew przepisom regulacji dotyczącej ochrony danych, popełnia przestępstwo, za które groziła odpowiedzialność karna[95]. Warto również wspomnieć o funkcjonowaniu w Polsce systemu EURODAC. Jak wiadomo, na mocy rozporządzenia Rady (WE) nr 2725/2000 dotyczącego ustanowienia systemu EURODAC do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, Unia Europejska wprowadziła obowiązek pobierania odcisków palców od

[90] Ustawa z dnia 17 czerwca 2004 r. o zmianie ustawy o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz niektórych innych ustaw, Dz. U. z 2004 r. Nr 179, poz. 1842 ze zm.
[91] Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, Dz. U. z 2007 r. Nr 165, poz. 1170.
[92] Ibidem.
[93] Ibidem.
[94] Obecnie GIODO zastąpił Urząd Ochrony Danych Osobowych, na którego czele stoi prezes UODO.
[95] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.; obecnie zastąpiło ją przez RODO.

cudzoziemców, którzy wnioskują o nadanie im statusu uchodźcy w jednym z Państw Członkowskich Wspólnoty[96]. W Polsce system EURODAC zaczął funkcjonować 1 maja 2004. Obrazy linii papilarnych pobierane są w Krajowej jednostce NAP EURODAC (National Access Point), a następnie przekazywane drogą elektroniczną do centralnej bazy systemu[97].

Aby uniknąć problemu budowania nowej infrastruktury technicznej specjalnie powołanej do działania polskiej sekcji EURODAC, ustawodawca krajowy zadecydował, że odciski palców cudzoziemców zapisywane będą w istniejącej już bazie AFIS. AFIS jest to Automatyczny System Identyfikacji Daktyloskopijnej (z ang. Automated Fingerprint Identyfication System)[98], którego głównym zadaniem jest porównywanie wprowadzanych odcisków palców z odbitkami linii papilarnych znalezionymi na miejscu zdarzenia o charakterze przestępczym. Ma to na celu szybkie i sprawne wykrywanie sprawców przestępstw. W przypadku systemu EURODAC działanie AFIS – u jest podobne jednakże celem, który przyświeca wprowadzaniu odcisków palców do systemu jest sprawdzenie czy odbitki linii papilarnych cudzoziemca nie zostały już wcześniej zapisane w NAP EURODAC innego kraju, a co za tym idzie, czy osoba już uprzednio nie ubiegała się o status uchodźcy na terenie innego Państwa Członkowskiego Unii Europejskiej. Ze sprawozdania Komisji do Parlamentu Europejskiego i Rady z oceny systemu dublińskiego opublikowanego w 2007 roku[99] wynikało, że system EURODAC spełnia swoje funkcje na terenie państw członkowskich. Dla Polski, początkowa współpraca w ramach systemu EURODAC spowodowała znaczny wzrost w liczbie powtórnie rozpatrywanych wniosków o udzielenie cudzoziemcowi statusu uchodźcy (ze sprawozdania wynika, że był to około 20 procentowy wzrost)[100]. Tendencja ta tłumaczona była w samym sprawozdaniu tym, że państwa, w których wzrosła liczba przekazanych wniosków (gdyż nie dotyczyło to tylko Polski) są geograficznie usytuowane przy granicach Unii Europejskiej i stanowią na ogół

---

[96] Obecnie EURODAC funkcjonuje na mocy przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu „Eurodac" do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniającego rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz. Urz. z 2013 r., L 180.

[97] https://clkp.policja.pl/clk/clkp/struktura/zaklad-daktyloskopii/65736,Zespol-Miedzynarodowej-Wymiany-Danych.html (dostęp 11.11.2020).

[98] B. Krzemińska, *System AFIS w polskiej Policji – wczoraj, dzisiaj, jutro,* „Problemy Kryminalistyki" 2018, nr 300.

[99] Sprawozdanie Komisji do Parlamentu Europejskiego i Rady z oceny systemu dublińskiego {SEK(2007)742}, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0299:PL:NOT (dostęp 11.11.2020).

[100] Ibidem.

pierwszy etap podróży podczas wkroczania do strefy Schengen[101]. Identyfikacja za pomocą cechy biometrycznej, w postaci obrazu linii papilarnych pozwala na sprawniejszą kontrolę niż to było w przypadku porównywania fotografii, a tym samym na większe prawdopodobieństwo uniknięcia sytuacji, w której cudzoziemiec ubiega się o nadanie statusu uchodźcy w jednym z państw członkowskich po uprzedniej negatywnej opinii innego członka Wspólnoty.

5. Podsumowanie

Pomimo początkowych wątpliwości co do skuteczności wykorzystania identyfikatorów biometrycznych oraz ich wiarygodności jako danych mogących zostać z powodzeniem użytych w celu weryfikacji tożsamości lub identyfikacji osoby, legislator unijny zdecydował się na wdrożenie nowoczesnych technologii oraz wykorzystanie cech biometrycznych jako jednego z rodzajów zabezpieczeń używanych w paszportach oraz innych dokumentach podróży. Zdecydował się on także na stworzenie baz danych, w których przechowywane są takie identyfikatory w celu rozwoju spójnej polityki azylowej i wizowej. Prawodawca wspólnotowy zdawał sobie sprawę z zagrożeń, jakie niesie za sobą takie roziwązanie. Jak można zaobserwować w pierwszej części rozdziału dotyczącej legislacji Unii Europejskiej, problemy pojawiały się najczęściej w dwóch aspektach. Pierwszy, to brak zaufania do technologii opartej na wykorzystaniu cech biometrycznych. Drugi to problem ochrony tak wrażliwych danych, jakimi są przetworzone cyfrowo identyfikatory biometryczne. Podstawowa kwestia wywołująca wątpliwości wynikała z tego, że gdy powstawały pierwsze rozporządzenia odwołujące się do stosowania technologii biometrycznej, w obrębie Unii nie było państwa, które miałoby jakiekolwiek doświadczenia w tym zakresie. Brak praktycznej wiedzy spowodował wśród obywateli Wspólnoty nieufność w stosunku do proponowanych uregulowań. Obecnie zarówno urządzenia służące do pobierania cech biometrycznych, jak i samo wykorzystanie danych w procesie weryfikacji tożsamości lub identyfikacji osoby budzi dużo mniejszy opór społeczny. Wynika to z tego, że prawodawstwo w tej dziedzinie funkcjonuje w ramach Unii już wiele lat, a przeprowadzone badania technologiczne pozwalają na ciągłe ulepszanie funkcjonowania zabezpieczeń i systemów. Jest to również rezultatem wykorzystywania tylko takich cech biometrycznych, których pobieranie obywatele Państw Członkowskich akceptują ze względu na ich małą inwazyjność (gromadzenie innych

[101] Ibidem.

identyfikatorów biometrycznych poza obrazem twarzy oraz odciskami palców nie zostało, jak do tej pory, uregulowane w aktach prawnych wydawanych przez Unię).

Mimo iż celem jaki przyświecał prawodawcy wspólnotowemu podczas wprowadzania zabezpieczeń biometrycznych do dokumentów podróży było zwiększenie bezpieczeństwa na terenie Unii Europejskiej, nie wszystkie państwa członkowskie zostały objęte działaniem legislacji w tej materii. Uzasadnienie do rozporządzenia 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie statuuje, że Zjednoczone Królestwo zostało wykluczone zostało z brania udziału w przyjmowaniu regulacji dotyczących paszportów biometrycznych[102]. Na tym tle powstał konflikt pomiędzy Zjednoczonym Królestwem, a Radą, którego rozwiązanie przyniosło dopiero orzeczenie Europejskiego Trybunału Sprawiedliwości[103]. Zjednoczone Królestwo stanęło na stanowisku, że ponieważ celem wdrażania nowoczesnej technologii do paszportów jest lepsze ich zabezpieczenie przed sfałszowaniem, a niektóre regulacje wydawane na podstawie konwencji wykonawczej Schengen mogą być przyjmowane przez Państwa Członkowskie pozostające poza strefą Schengen, również i w tym przypadku, Zjednoczone Królestwo powinno zostać objęte postanowieniami rozporządzenia[104]. Z argumentacji użytej przez Radę wywnioskować można natomiast, że Rozporządzenie 2252/2004 stanowiło rozwinięcie dorobku Schengen, w którym to Zjednoczone Królestwo nie uczestniczyło, a co za tym idzie, nie mogło ono być włączone w regulacje wynikające bezpośrednio z funkcjonowania strefy Schengen[105]. Ostatecznie Europejski Trybunał Sprawiedliwości opowiedział się po stronie Rady[106]. Nie podważając orzeczenia ETS-u (gdyż trzeba zaznaczyć, że przedmiot sporu miał głębsze podłoże niż same paszporty biometryczne; chodziło mianowicie o stosowanie regulacji, których podstawą tworzenia jest konwencja wykonawcza Schengen w państwach członkowskich Unii, które dobrowolnie zrezygnowały z funkcjonowania w ramach strefy Schengen) należy stwierdzić, że taka sentencja nie stała w zgodzie z celami, jakie przyświecały tworzeniu omawianych regulacji, którymi było jak najpowszechniejsze użycie paszportów biometrycznych w obrębie państw Wspólnoty. Spełnienie norm nałożonych przez Międzynarodową Organizację

[102] Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, Dz. Urz. z 2009 r., L 142.
[103] Wyrok Trybunału (Wielka Izba) z dnia 18.12.2007 roku w sprawie C-137/05 mającej za przedmiot skargę o stwierdzenie nieważności rozporządzenia nr 2252/2004 na podstawie art. 230 WE.
[104] Ibidem.
[105] Ibidem.
[106] Ibidem.

Lotnictwa Cywilnego ICAO pozwalało nie tylko na zmniejszenie ryzyka sfałszowania paszportu, ale także na sprawniejsze przeprowadzanie kontroli granicznej pomiędzy obywatelami Unii a Stanami Zjednoczonymi, gdzie po zamachu terrorystycznym mającym miejsce 11 września 2001 roku, pobieranie odcisków palców od osób wkraczających na terytorium USA stało się obowiązkowe. Dlatego też inicjowanie wprowadzania identyfikatorów biometrycznych do paszportów było skupione jedynie na wywieraniu nacisku na państwa należące do strefy Schengen, aby te implementowały regulacje opracowane na szczeblu unijnym, ale również na zachęcaniu i wspomaganiu wdrażania nowoczesnej technologii w państwach członkowskich spoza tej strefy.

Ochrona pobierania, przechowywania, przepływu i przetwarzania danych w postaci identyfikatorów biometrycznych, to drugi, ze wspomnianych wyżej problemów, z jakim musiał się uporać prawodawca wspólnotowy wdrażając nowoczesne rozwiązania do systemu prawnego Unii. Jako że jednym z wyznaczników cech biometrycznych jest ich unikalność, wypracowanie sposobu, w jaki ma się odbywać cały proces „używania" tychże danych (od momentu ich pobrania, poprzez przetwarzanie i przesyłanie, aż do porównywania) stał się istotnym czynnikiem we wdrażanej w tej dziedzinie legislacji. Ponadto odczytywanie danych znajdujących się w dokumencie od początku odbywało się zgodnie ze standardami ICAO. Wprowadzane przez prawodawcę unijnego rozwiązania, budziły bardzo często niepokój Europejskiego Inspektora Ochrony Danych Osobowych. W swoich opiniach wskazywał on, że niektóre normy regulujące korzystanie z identyfikatorów biometrycznych (lub bardzo często brak koniecznych regulacji) mogły nie odpowiadać standardom wypracowanym przez Unię w zakresie ochrony danych osobowych osób fizycznych. Z czasem prawodawca wspólnotowy zaczął udoskonalać regulację dotyczącą wdrażania identyfikatorów biometrycznych w duchu wskazówek, jakie EIOD udzielał w wydawanych przez siebie opiniach. Wspomniana przy okazji omawiania EURODACU opinia Europejskiego Inspektora Ochrony Danych Osobowych z lutego 2009 roku, o zmianach, które miały zostać wprowadzone w ramach systemu EURODAC, była pierwszą tak pochlebną oceną wystawioną przez EIOD legislacji wykorzystującej do swego działania identyfikatory biometryczne. Prawodawcy wspólnotowemu udało się więc doprowadzić do stworzenia w miarę spójnej i akceptowanej przez EIOD legislacji dążącej do usprawnienia działań Unii w zakresie polityki granicznej. To, co mogło budzić pewien niepokój w kontekście ochrony prywatności osób, których cechy biometryczne wprowadzane są do wspólnotowych baz danych, to istnienie centralnych systemów, do których trafiają identyfikatory biometryczne przetworzone cyfrowo przez krajowe jednostki. Jest to więc olbrzymie źródło informacji, które gdyby trafiło w niepowołane

ręce, mogłoby mieć bardzo negatywne skutki. Dlatego też Europejski Inspektor Danych Osobowych położył tak duży nacisk na określenie podmiotów, które mają dostęp do tych danych oraz celów, w jakich te podmioty mogą odczytywać informacje znajdujące się w systemie.

Obecnie po wielokrotnych zmianach prawodawstwa unijnego wykorzystującego technologię biometryczną oraz dzięki prowadzeniu RODO regulacje wspólnotowe w zakresie biometrii są w większości spójne i wyczerpująco normują kwestie, które rodziły trudności podczas praktycznego stosowania identyfikatorów biometrycznych. Należy jednakże pamiętać, że to po stronie państw członkowskich leży wprowadzanie w życie norm regulujących wykorzystywanie biometrii dla celów podniesienia bezpieczeństwa na terenie Unii Europejskiej.

Jak to już było wspomniane w rozdziale dotyczącym funkcjonowania technologii biometrycznej na terenie Polski, identyfikatory biometryczne musiały zostać wprowadzone do rodzimego prawodawstwa ze względu na wymogi stawiane w tym względzie przez Unię Europejską, której Polska stała się członkiem 1 maja 2004 roku. Rzeczypospolita zobowiązała się wtedy do przyjęcia całego *acquis communautaire*, w tym również legislacji dotyczącej polityki migracyjnej i azylowej prowadzonej w ramach istnienia strefy Schengen. Do momentu przyjęcia powyższych aktów prawnych, wykorzystywanie cech biometrycznych w celu identyfikacji osoby lub weryfikacji jej tożsamości nie było w Polsce popularne. Jedynym przykładem wykorzystywania unikalności identyfikatorów biometrycznych było funkcjonowanie na terenie naszego kraju wspomnianego wyżej systemu AFIS (Automated Fingerprint Identyfication System). W celu wykrywania sprawców przestępstw (a również do innych celów takich jak np. identyfikacja zwłok nieznanej osoby) system ten wykorzystuje cechę, jaką jest indywidualny dla każdego człowieka układ wzorów linii papilarnych znajdujących się na opuszkach palców dłoni. System porównuje wprowadzone do niego odciski palców z tymi, które już wcześniej ostały zamieszczone w bazie danych.

Jednakże większość inicjatyw, podejmowanych przez członków strefy Schengen była wymuszona regulacjami wdrażanymi przez prawodawcę wspólnotowego. Największe trudności w Polsce występowały w stosunku do wprowadzania regulacji dotyczących zamieszczania identyfikatorów biometrycznych w dokumentach podróży. Dostosowując polskie prawo do wymogów unijnych, ustawodawca krajowy w 2006 roku powołał do życia ustawę o dokumentach paszportowych. Ważnym elementem powyższej regulacji było wprowadzenie do książeczki paszportowej zdjęcia biometrycznego oraz mikroprocesora, na

którym zakodowany miał być odcisk palca właściciela dokumentu[107]. Pierwsza cecha, jaką jest biometryczny obraz twarzy, została wdrożona zgodnie z przyjętym w ustawie terminem (był to sierpień 2006 roku). Wprowadzenie tej cechy biometrycznej do paszportów nie nastręczyło większych problemów ustawodawcy krajowemu. Problem pojawił się jednakże przy w początkowej fazie wdrażania drugiej cechy biometrycznej do paszportu – linii papilarnych. Największym problemem był brak regulacji wykonawczych, które uzupełniałyby ustawę o dokumentach paszportowych, a także brak instrukcji co do sposobu pobierania odcisków palców od osób wnioskujących o wydanie paszportu. Powyższe kwestie zostały jednakże rozwiązane i obecnie, po wielu latach funkcjonowania identyfikatorów biometrycznych w paszportach, nie stanowią one już problemu.

Wstępując do Unii Europejskiej w 2004 roku, Polska zobowiązała się również do wdrożenia Systemu Informacyjnego Schengen drugiej generacji SIS II, Systemu Informacji Wizowej VIS oraz Systemu służącego do porównywania odcisków palców azylantów oraz nielegalnych imigrantów EURODAC. Należy pochwalić ustawodawcę krajowego za podjęte w tej dziedzinie kroki. Najważniejszym z nich było opracowywanie Master planów, które miały pomóc w prawidłowym funkcjonowaniu systemów VIS, SIS oraz SIS II na teranie naszego kraju. W planach tych wskazane zostały konkretne działania, które musiały zostać podjęte, aby sprostać wymaganiom unijnym w tej materii. Dobrym sposobem na osiągnięcie zamierzonych celów okazało się podzielenie ich na trzy kategorie: cele organizacyjne, prawne i techniczne. Dzięki temu możliwe stało się rozdzielenie zadań pomiędzy różne ekipy, które od tej pory zajmowały się tylko przydzielonymi im funkcjami. Aby poradzić sobie z problemem budowy krajowych baz danych systemów VIS oraz SIS (przekształconego następnie w SIS II), polski ustawodawca zdecydował się na wykorzystanie istniejącego już systemu, w którym gromadzone są informacje konieczne do prawidłowego działania Systemu Informacji Schengen oraz Systemu Informacji Wizowej. Systemem tym jest Krajowy System Informatyczny, który zaadoptowany został głównie na potrzeby funkcjonowania systemu SIS (a obecnie SIS II). Oparcie się na już istniejącej bazie pozwoliło na uniknięcie problemu budowania infrastruktury informatycznej od zupełnych podstaw. Jeśli chodzi o aspekt prawny, to od 2007 roku obowiązuje w Polsce ustawa o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej. Precyzyjnie określa ona sytuacje, w które dane mają się znaleźć w krajowych bazach SIS i VIS. Kategorie te zostały przekopiowane z przepisów ustanowionych na szczeblu wspólnotowym.

[107] Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych, Dz. U. z 2006 r. Nr 143, poz. 1027 ze zm.

Jeśli chodzi o system EURODAC to ustawodawca polski zadecydował, że krajowa jednostka NAP EURODAC bazować będzie na infrastrukturze informatycznej stworzonej do funkcjonowania systemu AFIS. Pamiętać należy, że wszystkie trzy systemy (VIS, SIS oraz EURODAC) zostały stworzone i są udoskonalane w celu osiągnięcia wysokiego poziomu bezpieczeństwa oraz harmonijnej współpracy pomiędzy państwami, które przyjęły dorobek Schengen. Wspólna polityka migracyjna i azylowa są częścią ustawodawstwa Unii w tym zakresie. Tzw. starzy członkowie Wspólnoty mieli możliwość zdecydowania o przyjęciu lub odrzuceniu zawartego w Schengen układu. Sytuacją pożądaną było jednak przekonanie do idei otwartych granic jak największej liczby państw należących do Unii Europejskiej. Dlatego też nowi członkowie Wspólnoty (państwa, które wstąpiły do Unii w 2004 roku – w tym Polska oraz dwaj nowi członkowie z 2007 roku) nie otrzymali możliwości takiego wyboru i musieli dostosować swoje ustawodawstwo do regulacji opartej na dorobku Schengen. Unia Europejska szczególne bacznie przyglądała się wdrażaniu dorobku Schengen w państwach kandydujących, których granice po przystąpieniu do Wspólnoty miały stać się zewnętrznymi granicami Unii. Jako, że jednym z takich państw jest Polska, ustawodawca krajowy musiał dołożyć szczególnej staranności, aby sprostać wymaganiom stawianym kandydatom w tej dziedzinie. Ponadto, na państwach granicznych ciąży de facto większa odpowiedzialność za bezpieczeństwo Wspólnoty w sferze polityki migracyjnej niż na pozostałych członkach. Dlatego Polska powinna implementować do porządku wewnętrznego wszelkie regulacje odnoszące się do wykorzystania technologii biometrycznej, która sprzyja prowadzeniu wspólnej polityki migracyjnej na terenie strefy Schengen. Zaletą użycia identyfikatorów biometrycznych jest również to, że pozwalają one na przyspieszenie i usprawnienie kontroli granicznej oraz procesu ubiegania się o azyl na terenie jednego z państw członkowskich Unii Europejskiej. Bez implementacji tych norm nie mógł zostać spełniony jeden z bardzo ważnych celów traktatu z Schengen, a mianowicie likwidacja granic wewnętrznych oraz swobodny przepływ osób. Bez nowoczesnych zabezpieczeń nie można bowiem liczyć na harmonijną współpracę państw oraz prowadzenie spójnej polityki azylowej.

Kolejnym ważnym zagadnieniem, z którym polski ustawodawca musiał sobie poradzić było zapewnienie należytej ochrony danym biometrycznym przed nieprawidłowym ich przechowywaniem, przetwarzaniem oraz udostępnianiem podmiotom zewnętrznym. Od 1997 roku obowiązywała w Polsce Ustawa o ochronie danych osobowych. Regulacja ta była zgodna z wprowadzoną w 2004 roku Dyrektywą 95/46/EC Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Chociaż ustawa nie wymieniała wprost danych biometrycznych jako

danych osobowych, jej przepisy nie pozostawiały wątpliwości w tym zakresie. Obecnie zarówno dyrektywa nr 95/46, jak i polska ustawa o ochronie danych osobowych straciły moc prawną na rzecz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), tzw. RODO. Jest to podstawowy akt prawny dotyczący ochrony danych osobowych, który jako pierwszy zdefiniował pojęcie danych biometrycznych.

Specyfika danych biometrycznych zmusza ustawodawcę również do lepszego technologicznego zabezpieczania systemów, w których zapisane są informacje dotyczące odcisków palców oraz wizerunku twarzy osoby (a w przyszłości prawdopodobnie i innych identyfikatorów). Pamiętać należy, że wyciek informacji dotyczących cech biometrycznych ze względu na ścisłe związanie tych cech z osobą może mieć dużo bardziej negatywne skutki niż ujawnienie danych, które nazwać można konwencjonalnymi (takich jak np. nazwisko).

Na przestrzeni ostatnich kilku lat możemy zaobserwować wzrost wykorzystania technologii biometrycznych w otaczającym świecie. Elektroniczny podpis czy komputer zabezpieczony urządzeniem skanującym odcisk palca przestały być czymś niezwykłym, a stały się ułatwieniem dla wielu osób wypierając tradycyjne hasła czy kody. Identyfikatory biometryczne wkradły się również do dokumentów czy też systemów mających chronić nasze bezpieczeństwo oraz usprawniać podróżowanie. Czy tego chcemy czy nie identyfikatory biometryczne coraz częściej pojawiają się jako forma zabezpieczania dokumentów oraz dostępu do pomieszczeń czy urządzeń. Tak jak w każdej innej dziedzinie tak i w tej technologia idzie naprzód, a próba zatrzymania jej rozwoju mogłaby spowodować zwiększenie zagrożenia w zakresie bezpieczeństwa. Musimy jednak zrozumieć, że ceną jaką płacimy za minimalizowanie ryzyka jest coraz mniejsza anonimowość jednostki we współczesnym świecie. Koszt taki może się niektórym wydawać zbyt wysoki, jednakże w obecnym stanie rozwoju cywilizacyjnego wycofanie się z wykorzystywania identyfikatorów biometrycznych wydaje się niemożliwe. Zdawanie sobie jednak sprawy z problemów, jakie rodzić może wdrażanie biometrii, powinno skłaniać do przemyśleń w zakresie implementacji takich mechanizmów, które pozwolą na znalezienie równowagi pomiędzy podnoszeniem poziomu bezpieczeństwa, a prawem do prywatności jednostki.

Celem niniejszej pracy nie było wyczerpanie tematu wykorzystania technologii biometrycznej na terenie Unii Europejskiej, a jedynie wskazanie historycznego kontekstu implementacji norm biometrycznych do polskiego porządku prawnego. Podjęcie takiej tematyki pozwoliło bowiem

zwrócić uwagę na pierwotne problemy z wdrażaniem biometrii na terenie Wspólnoty. Część z nich rozwiązana została dzięki rozwojowi technologii, pozostałe natomiast – dotyczące zwłaszcza ochrony prawnej jednostki od której pobierane są wzorce - pozostają aktualne również dzisiaj.

Bibliografia

Literatura

Ballantyne M., Boyer R., Hines L., *Woody Bledsoe: His life and legacy*, „AI Magazine" 1996, t. 17, nr 1.

Czajka A., Pacut A., *Biometria podpisu odręcznego*, w: P. Zając, S. Kwaśniowski (red.), *Automatyczna identyfikacja w systemach logistycznych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.

Cichowicz J., *Mamy to w jednym palcu*, „Człowiek i Dokumenty" 2008, nr 10.

Cichowicz J., *O biometrii w Las Vegas*, „Człowiek i Dokumenty" 2008, nr 9.

Daugman J., *How iris recognition works*, „IEEE Transactions on Circuits and Systems for Video Technology" 2004, t. 14, nr 1.

Dzwonek A., Kling T., *Biometria w dokumentach podróży*, „Człowiek i Dokumenty" 2008, nr 10.

Galton F., *Finger Prints*, McMillan, London 1982.

Heizmann C. (oprac. Anna Henschke), *Podwyższenie sprawności kontroli granicznej dzięki kartom chipowym*, „Problemy Kryminalistyki" 2005, nr 253.

Horoszowski P., *Kryminalistyka*, Państwowe Wydawnictwo Naukowe, Warszawa 1958, wyd. 2.

Jiang X., Lu Y., Tang H., Tsai J., Ng E., Daneman M., Boser B., Horsley D., *Monolithic ultrasound fingerprint sensor*, „Microsystems and Nanoengineering" 2017, t. 3.

Jones P., *Using biometric technology to advance law enforcement*, „Forensic Magazine", sierpien/wrzesień 2006.

Lei Y., Bennamoun M., Hayat M., Guo Y., *An efficient 3D face recognition approach using local geometrical signatures*, „Pattern Recognition" 2004, t. 47(2).

Majekodunmi T., Idachaba F., *A review of the fingerprint, speaker recognition, face recognition and iris recognition based biometric identification technologies*, „Proceedings of the World Congress on Engineering" 2011, t. II WCE 2011, July 6–8, 2011, London, U.K (http://eprints.covenantuniversity.edu.ng/3946/1/WCE2011_pp1681-1687.pdf).

Marcialis G., Roli F., *Fingerprint verification by fusion of optical and capacitive sensors*, „Pattern Recognition Letters" 2004, t. 25.

Kirby M., Sirovich L., *Low-dimensional procedure for the characterisation of human faces*, „Journal of the Optical Society of America" 1987, t. 4(3).

Krassowski K., Sołtyszewski I., *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252.

Krzemińska B., *System AFIS w polskiej Policji – wczoraj, dzisiaj, jutro*, „Problemy Kryminalistyki" 2018, nr 300.

Ratha N., Govindaraju V. (red.), *Advances in Biometrics. Sensors, Algorithms and Systems*, Springer, New York 2008.

Sanchez-Reillo R., Sanchez-Avila C., Gonzalez-Marcos A., *Biometric identification through hand geometry measurements*, „IEEE Transactions on Pattern Analysis and Machine Intelligence" 2000, t. 22, nr 10.

Satonkar Suhas S., Kurhe Ajay B., Prakash Khanale B., *Face recognition using principal component analysis and linear discriminant analysis on holistic approach in facial images database*, „Journal of Engineering" 2012, t. 2(12).

Shaheed K., Liu H., Yang G., Qureshi I., Gou J., Yin Y., *A systematic review of finger vein recognition techniques*, „Information" 2018, t. 9.

Shaver C., Acken J., *A Brief Review of Speaker Recognition Technology*, Electrical and Computer Engineering Faculty Publications and Presentations, 2016.

Szczepański T., *Daktyloskopia na przestrzeni wieków*, „Problemy Kryminalistyki" 2019, nr 303.

Ślaski K., *Dokumenty podróży*, „Człowiek i Dokumenty" 2008, nr 8.

Wiskott L., Krüger N., Kuiger N., von der Malsburg C., *Face recognition by elastic bunch graph matching*, „IEEE Transactions on Pattern Analysis and Machine Intelligence" 1997, t. 19, nr 7.

Wołowski F., *Paszport biometryczny – fakty i mity*, „Człowiek i Dokumenty" 2008, nr 8.

Turk M., Pentland A., *Eigenfaces for Recognition*, „Journal of Cognitive Neuroscience" 1991, t. 3.

Źródła prawa

Biometrics at the Frontiers: Assessing the Impact on Society – EUR 21585.

Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final.

Decyzja Komisji z 28.02.2005 roku, C(2005)409, ustanawiająca specyfikacje techniczne dla norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie.

Decyzja Komisji z 28.06.2006 r. ustanawiająca specyfikacje techniczne dla norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie.

Decyzja Komisji z dnia 4 marca 2008 roku w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla Systemu Informacyjnego Schengen drugiej generacji (SIS II), notyfikowana jako dokument nr C(2008) 774, Dz. Urz. z 2008 r., L 123.

Decyzja Rady (WE) nr 512/2004 z dnia 8 czerwca 2004 roku w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz. Urz. z 2004 r., L 213.

Decyzja Rady 2007/533 z dnia 12 czerwca 2007 roku w sprawie utworzenia, funkcjonowania i używania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. z 2007 r., L 205.

Decyzja Rady nr 633/2008 z dnia 23 czerwca 2008 roku w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS)

do celów jego przeglądania w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz. Urz. z 2008 r., L 218.

Decyzja Rady z dnia 6 grudnia 2001 roku w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. z 2001 r., L 328.

Dyrektywa 95/46/EC Parlamentu Europejskiego i Rady z 14 października 2004 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz. Urz. z 1995 r., L 281.

Konwencja Rady Europy o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r.

Konwencja Wiedeńska z dnia 18 kwietnia 1961 r. o stosunkach dyplomatycznych.

Konwencja wykonawcza do Układu z Schengen z dnia 14 czerwca 1985 r. w sprawie stopniowego znoszenia kontroli na wspólnych granicach z 1990 roku, Dz. Urz. z 2000 r., L 239.

Opinia Europejskiego Inspektora Danych Osobowych z 27 października 2006 r. dotycząca wniosku 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, Dz. U. z 2006 r., C 321.

Opinia Europejskiego Inspektora Ochrony Danych dotycząca rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie, Dz. Urz. z 2008 r., C 200.

Opinia Europejskiego Inspektora Ochrony Danych Osobowych z dnia 23 marca 2005 r. 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, Dz. Urz. C 181 z 23 lipca 2005 r., Dz. Urz. z 2005 r., C 181.

Opinia Europejskiego Inspektora Ochrony Danych Osobowych z października 2006 r., Dz. Urz. z 2006 r., C 91/38:

- w sprawie wniosku dotyczącego decyzji Rady w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II),
- w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie utworzenia, eksploatacji i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II),
- w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie dostępu służb odpowiedzialnych w Państwach Członkowskich za wydawanie.

Opinia Grupy Roboczej nr 3/2005 w sprawie wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie.

Opinia 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.

Program dla uczestnictwa Rzeczypospolitej Polskiej w realizacji tytułu IV konwencji wykonawczej Schengen, MSWiA, Warszawa, październik 2004 r., dostępny na stronie: www.mswia.gov.pl.

Program dostosowania organów administracji państwowej do współpracy z Systemem Informacyjnym Schengen II (SIS II) i Systemem Informacji Wizowej (VIS), 2006 r., dostępny na archiwalnej stronie: https://archiwum.premier.gov.pl.

Program dostosowania systemu paszportowego oraz dokumentów podróży wydawanych cudzoziemcom przez władze polskie do wymogów prawa unijnego, dostępny na archiwalnej stronie: https://archiwum.premier.gov.pl.

Projekt rezolucji legislacyjnej Parlamentu Europejskiego w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie, PE 405.718v02 – 00 A6 – 0500/2008.

Rozporządzenie 45/2001/EC Parlamentu Europejskiego i Rady z 18 grudnia 2000 roku o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie danych, Dz. Urz. z 2001 r., L 8.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 2010 r. w sprawie dokumentów paszportowych, Dz. U. z 2010 r. Nr 151, poz. 1026 ze zm.

Rozporządzenie nr 343/2003/EC ustanawiające kryteria i mechanizmy określenia Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl wniesionego w jednym z Państw Członkowskich przez obywatela Państwa Trzeciego (zwane Dublin II), Dz. Urz. z 2003 r., L 50.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona), Dz. Urz. z 2013 r., L. 180.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1985/2006 w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. z 2006 r., L 381.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 roku w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz. Urz. z 2008 r., L. 218 ze zm.

Rozporządzenie Parlamentu Europejskiego i Rady(UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. z 2016 r., L119 (tzw. RODO).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca, Dz. Urz. z 2013 r., L 180.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 444/2009 z dnia 28 maja 2009 r. zmieniające rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i w dokumentach podróży wydawanych przez państwa członkowskie, Dz. Urz. z 2009, L 142.

Rozporządzenie Rady (WE) nr 2424/2001 z dnia 6 grudnia 2001 roku w sprawie rozwoju Systemu Informacyjnego Schengen drugiej generacji, Dz. Urz. z 2001 r., L 328.

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

Rozporządzenie Rady (WE) nr 2725/2000 dotyczące ustanowienia systemu EURODAC do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, Dz. Urz. z 2002 r., L 62.

Sprawozdanie Komisji do Parlamentu Europejskiego i Rady z oceny systemu dublińskiego (COM(2007)299 wersja ostateczna) {SEC(2007) 742}.

The Rapid DNA Act of 2017 (Public Law 115-50).

Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych, Dz. U. z 2006 r. Nr 143, poz. 1027 ze zm.

Ustawa z dnia 17 czerwca 2004 r. o zmianie ustawy o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych oraz niektórych innych ustaw, Dz. U. z 2004 r. Nr 179, poz. 1842 ze zm.

Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej, Dz. U. z 2007 r. Nr 165, poz. 1170 ze zm.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 3 grudnia 2008 r. powołującego system EURODAC do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr […/…] [ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela kraju trzeciego lub bezpaństwowca], COM(2008) 825, wersja ostateczna.

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady z dnia 31 maja 2006 roku zmieniający Wspólne Instrukcje Konsularne dla misji dyplomatycznych i urzędów konsularnych dotyczący wiz w związku z wprowadzeniem technologii biometrycznych, łącznie z przepisami dotyczącymi organizacji przyjmowania i rozpatrywania wniosków

wizowych (wniosek przedstawiony przez Komisję), COM/2006/0269 końcowy – COD 2006/0088.

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, COM(2007) 619, wersja ostateczna.

Wyrok Trybunału (Wielka Izba) z dnia 18.12.2007 roku w sprawie C-137/05.

Źródła internetowe

https://www.fbi.gov
https://www.dhs.gov/biometrics
http://www.biometriclabs.pl/
http://www.mswia.gov.pl
http://www.warschau.diplo.de
https://eur-lex.europa.eu
https://uodo.gov.pl/
https://clkp.policja.pl
http://gazetapolicyjna.policja.pl
https://www.nask.pl/
http://bezpieczenstwo.idg.pl/
https://ec.europa.eu
https://www.gov.pl
https://www.biometricupdate.com