Adam Kirpsza

Biometryczna identyfikacja tożsamości ludzkiej w świetle standardów praw człowieka: przykład paszportu biometrycznego

Wstęp

Od początku XXI wieku, zwłaszcza od momentu zamachów terrorystycznych z 11 września 2001 r., w prawodawstwie Unii Europejskiej uwidacznia się zjawisko zwane biometryzacją. Polega ono na przyjmowaniu aktów normatywnych umożliwiających wykorzystywanie charakterystycznych i niepowtarzalnych cech człowieka (np. odcisków palców, tęczówki oka, profili DNA) w celu ustalenia jego tożsamości. Przejawem tego zjawiska jest ustanowienie paszportów biometrycznych; Eurodac, czyli centralnej bazy odcisków palców pobieranych od osób, które wnioskują o azyl, są uchodźcami lub próbują nielegalnie przekroczyć granice zewnętrzne UE[1]; Wizowego Systemu Informacyjnego (VIS) - bazy danych zawierającej fotografie i odciski palców osób ubiegających się o wizę[2]; Systemu Informacyjnego Schengen (SIS II) - bazy danych składającej się z odcisków palców i fotografii twarzy osób, którym odmówiono pozwolenia na wjazd i pobyt do/w UE, poszukiwanych w celu aresztowania lub ekstradycji, zaginionych, których obecność jest wymagana do celów procedury sądowej oraz co do których wymagane są kontrole niejawne lub szczególne[3]; oraz TECS - Systemu Informacyjnego Europolu zawierającego dane daktyloskopijne i profile DNA osób podejrzanych lub skazanych za popełnienie przestępstwa wchodzącego w zakres kompetencji Europolu[4]. Jak zatem widać, zastosowanie biometrii w UE jest bardzo szerokie.

---

[1] *Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej*, „Dziennik Urzędowy WE" z 15 grudnia 2000 r., L 316, s. 1-10.

[2] *Decyzja Rady2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS)*, „Dziennik Urzędowy UE" z 15 czerwca 2004 r., L 213, s. 5-7; *Rozporządzenie Parlamentu Europejskiego oraz Rady nr 767/2008 w sprawie systemu VIS i wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych* „Dziennik Urzędowy UE" z 13 sierpnia 2008, L 218, s. 60-81.

[3] *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1987/2006 z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II)*, „Dziennik Urzędowy UE" z 28 grudnia 2006 r., L 381, s. 4-23; *Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II)*, „Dziennik Urzędowy UE" z 7 sierpnia 2007 r., L 205, s. 63-84.

[4] *Decyzja Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol)*, „Dziennik Urzędowy UE" z 15 maja 2009 r., L 121, s. 37-66.

Trzeba jednak stwierdzić, że choć biometria jest coraz powszechniej implementowana w życiu społecznym, to wciąż brakuje opracowań badających jej legalność i zakres unormowania w konkretnych aktach prawnych. Niniejszy artykuł próbuje wypełnić tę lukę. Analizuje on prawne aspekty zastosowania biometrii w unijnym i polskim paszporcie biometrycznym, ogniskując się na krytyce poszczególnych rozwiązań. Rozdział pierwszy koncentruje się na technicznych aspektach biometrii, w szczególności wyjaśnia główne pojęcia z nią związane, opisuje dwie metody biometrycznego uwierzytelniania - weryfikację i identyfikację oraz sprawdza ich skuteczność przy ustalaniu tożsamości. W rozdziale drugim ma miejsce krytyczna analiza postanowień rozporządzenia ustanawiającego paszporty biometryczne. Natomiast rozdział trzeci przedstawia zarzuty w stosunku do polskich unormowań paszportowych. Konkluzje podsumowują uzyskane wnioski.

Pojęcie biometrii

Biometria[5] jest dziedziną nauki zajmującą się mierzeniem ciała i zachowań istot żywych. Jej szczególnie rozwiniętym odłamem jest biometria tożsamości, która koncentruje się metodach i możliwościach zautomatyzowanego rozpoznawania tożsamości jednostki ludzkiej na podstawie jej cech charakterystycznych zwanych biometrykami[6]. Wyróżnia się trzy rodzaje biometryk: fizjologiczne, behawioralne i kognitywne. Pierwsze zawierają informacje o charakterystyce fizycznej danej osoby, są to przede wszystkim odciski palców, obraz twarzy, geometria dłoni i rzut tęczówki. Zasadą ich funkcjonowania jest wysoka trwałość i niezależność od społecznych lub genetycznych transformacji. Biometryki behawioralne są to mechanizmy i sposoby wykonywania pewnych powtarzalnych czynności przez człowieka, która różnicują się w zależności od realizującej je osoby. Należą do nich: podpis, głos, ruch ust czy tempo pisania. Ponieważ ludzie ciągle uczą się biometryk behawioralnych, dlatego cechują się one zmiennością temporalną, co stanowi ich poważną wadę[7]. Trzecim rodzajem są biometryki kognitywne, czyli reakcje mózgu na zewnętrzne bodźce, takie jak: zapach czy percepcja twarzy. Najbardziej znaną z nich jest fala P300, czyli specyficzny, elektryczny sygnał neuronów, który odzwierciedla różny dla każdego człowieka

[5] Z greckiego: *bios* - życie, *metron* - miara, wielkość.
[6] R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, *Biometria*, Warszawa 2008, s. 4-10; N. Moradoff, *Biometrics: Proliferation and Constraints to Emerging and New Technologies*, „Security Journal" 2010, vol. 23, nr 4, s. 277.
[7] R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, op. cit., s. 7.

rytm aktywności mózgowej[8]. Wyjątkowy i indywidualny charakter biometryk kognitywnych pozwala wygenerować profil mózgowy identyfikujący daną osobę[9].

Biometria jest odpowiedzią na krytykę tradycyjnych metod ustalania tożsamości, które polegają na przedmiotowych sposobach rozpoznawania osób. Opierają się one na posiadaniu przez jednostkę obiektu (klucz, dowód osobisty – „coś, co posiada") lub wiedzy (kod PIN, PUK – „coś, co wie"), dzięki którym może ona potwierdzić swoje personalia i uzyskać dostęp do określonych usług[10]. Istotnym elementem tej koncepcji jest zatem rozróżnienie podmiotu (jednostki) od przedmiotu (klucza, wiedzy), który jest jedynie środkiem weryfikacyjnym, wyizolowanym od osoby. Problemem tradycyjnych metod rozpoznawania tożsamości jest jednak łatwość zgubienia lub kradzieży obiektów identyfikujących, a w przypadku wiedzy – zapomnienia. Jak pokazują sondaże, prawie 25% osób mieszkających w USA zapisuje kod PIN na swoich kartach kredytowych, co czyni z nich potencjalne ofiary rabunków[11]. Co więcej, ok. 20% z nich jako hasło do różnych systemów finansowych wybiera swoje nazwisko, a 10% - datę swoich urodzin, co jest niezmiernie łatwe do wykrycia dla hakerów[12]. Ponadto, tradycyjne identyfikatory są pod całkowitą kontrolą ich właściciela, przez co ich ujawnienie jest podatne na oddziaływanie inżynierii społecznej. Znamienny jest eksperyment przeprowadzony w Londynie, kiedy organizatorzy europejskiego święta handlu, wykorzystując zdolności społeczne, pytali pracowników o hasła do ich komputerów biurowych - 70% z nich ujawniło te informacje bez wahania[13].

Chcąc zapobiec powyższym problemom, biometria wypracowała inny model ustalania tożsamości w oparciu o „coś, kim jesteś". Oznacza to, że jednostka nie musi już posiadać wyizolowanego od niej przedmiotu czy wiedzy weryfikującej, lecz sama jest własnym identyfikatorem. Rolę taką odgrywają biometryki, które występują prawie u wszystkich ludzi, a jednocześnie cechują się niepowtarzalnością i różnorodnością. Poprzez stworzenie odpowiednich czytników lub sensorów te właściwości ludzkie mogą być odczytywane bardzo szybko i z dużym stopniem pewności potwierdzać tożsamość danej osoby. Ponadto,

---

[8] A. Michalski, *Okno na świat*, „Wiedza i Życie" 2000, nr 3.
[9] Zob.: P. Njemanze, *Cerebral Lateralisation in Random Letter Task in the Visual Modality: A Transcranial Doppler Study*, „Brain and Language" 1996, vol. 53, nr 3, s. 315-325; N. Stroobant, G. Vingerhoets, *Transcranial Doppler Ultrasonography Monitoring of Cerebral Hemodynamics During Performance of Cognitive Tasks. A Review*, „Neuropsychological Review" 2000, vol. 10, nr 4, s. 213-231.
[10] A. K. Jain, R. Bolle, S. Pankanti, *Introduction to Biometrics*, [w:] A. K. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal Identification in Networked Society,* Norwell 1999, s. 3.
[11] J. Woodward, N. Orlans, P. Higgins, *Biometrics*, New York 2003, s. 9.
[12] W. Summers, E. Bosworth, *Password Policy: The Good, the Bad, and the Ugly*, paper presented at the Winter International Symposium on Information and Communication Technologies, WISICT'04, Cancun, Mexico, 5-8 January 2004.
[13] K. Murphy, *Psst: a Candy Bar for Your Password?*, „The Australian", 27 April 2004, s. 6.

charakteryzują się one niemożliwością kradzieży czy zapomnienia, ich utrata może być spowodowana wyłącznie znacznym naruszeniem integralności fizycznej (odcięciem palca, wydłubaniem oka, odcięciem głowy itp.)[14]. W rezultacie, dzięki biometrii nie trzeba już pamiętać kodów PIN czy tworzyć łatwych do odgadnięcia haseł - hasłem jest sam człowiek.

Biometria opracowała dwie metody korzystania z tego „hasła" - weryfikację i identyfikację. Weryfikacja polega na odpowiedzi na pytanie „Czy to jest X?". Osoba umieszcza na sensorze swoją biometrykę (np. odcisk palca) oraz dodatkowo wprowadza do czytnika obiekt zawierający tę biometrykę (np. osoba chce wypłacić gotówkę z bankomatu biometrycznego, kładzie więc na sensorze bankomatu swój odcisk palca i jednocześnie wprowadza do niego kartę bankową zawierającą pobrane wcześniej własne dane daktyloskopijne). Po przetworzeniu obie biometryki są porównywane między sobą przez system. W przypadku ich zgodności, komputer potwierdza prawdziwą tożsamość właściciela i umożliwia mu skorzystanie z danej usługi[15]. Identyfikacja natomiast stara się odpowiedzieć na pytanie „Kim jest X?", czyli ma nie tyle potwierdzić tożsamość, ile ją poznać i określić. Osoba umieszcza na sensorze tylko swoją biometrykę (np. odcisk palca), alternatywnie wprowadza do czytnika obiekt ją zawierający (np. kartę ID). Po przetworzeniu biometryki system porównuje ją z wszystkimi biometrykami zgromadzonymi wcześniej w centralnej bazie danych. W sytuacji gdy komputer odnajdzie w niej biometrykę zgodną z tą oddaną na sensorze, stwierdza pozytywną komparację, to znaczy określa tożsamość danej osoby jako uprawnioną do korzystania z usługi[16].

Należy podkreślić, że z perspektywy prawa do prywatności lepszą metodą ustalania tożsamości jest weryfikacja. Przede wszystkim, odbywa się ona w warunkach wewnętrznych, to znaczy osoba porównuje się sama ze sobą, podczas gdy system jest w tej operacji tylko pośrednikiem. Weryfikacja wykorzystuje tylko jedną biometrykę, która jest w pełni kontrolowana przez jej właściciela, nie istnieje zatem groźba jej systemowego wycieku czy niekontrolowanego gromadzenia w systemie. Wreszcie, celem tej procedury nie jest poznanie osoby pragnącej skorzystać z danej usługi, lecz tylko sprawdzenie, czy to jest właściwa osoba, za którą się podaje. Istnieje zatem bariera tożsamościowa - system nigdy się nie dowie, kim jesteśmy, ponieważ nie ma własnych biometryk. Inaczej to wygląda w przypadku identyfikacji. Operacja porównawcza odbywa się w warunkach zewnętrznych - biometryka osoby jest porównywana z danymi biometrycznymi znajdującymi się w systemie. Jednostka

[14] A. K. Jain, R. Bolle, S. Pankanti, op. cit., s. 4.
[15] Ibidem, s. 7-8.
[16] Ibidem, s. 8.

nie jest zatem samodzielnym uczestnikiem procedury, gdyż taki sam status posiada system. Identyfikacja dokonuje komparacji danej biometryki z wieloma innymi wcześniej pobranymi, co grozi niebezpieczeństwem pomyłki, błędnymi identyfikacjami i niekontrolowanym przez osobę procesem uwierzytelniania. Ponadto, kluczowym elementem identyfikacji jest istnienie centralnej bazy biometryk, co generuje groźbę nieuprawnionego dostępu i ich wykorzystywania, wycieku lub monitorowania operacji i ruchu danej osoby. W sytuacji, gdy taka baza ma charakter państwowy oraz zawiera biometryki wszystkich swoich obywateli, widmo orwellowskiego „Wielkiego Brata" staje się realne. Wreszcie, celem identyfikacji jest poznanie tożsamości osoby pragnącej skorzystać z usługi - po udanej komparacji system wie, kim ona jest i wiedzę tę może łatwo wykorzystać podmiot nim zarządzający. Reasumując, stosowanie biometrii w celach weryfikacji jest odpowiednie, w miarę bezpiecznie i prawnie dozwolone, natomiast identyfikacja generuje poważne wątpliwości i zagrożenia, dlatego powinna być unikana.

Kwestią zasadniczą przy analizie biometrycznych metod ustalania tożsamości ludzkiej jest ocena ich skuteczności, rozumianej jako poziom dokładności i liczba błędów przy porównywaniu biometryk między sobą. Istnieją dwa narzędzia matematyczne umożliwiające jej określenie - wskaźnik błędnych akceptacji (FAR - *False Acceptance Rate*), pokazujący, w ilu przypadkach system uznał dwie różne biometryki za zgodne, mimo że nie są kompatybilne, oraz wskaźnik błędnych odrzuceń (FRR - *False Rejection Rate*)[17], oznaczający liczbę przypadków, w których system uznaje dwie takie same biometryki za niezgodne, mimo że są kompatybilne. FAR mówi zatem, ile razy ma miejsce sytuacja, kiedy zgłoszona przy użyciu biometryki tożsamość jest uprawniona, podczas gdy w rzeczywistości jest to oszust, podczas gdy FRR - ile razy ma miejsce sytuacja, kiedy zgłoszona tożsamość nie jest uprawniona, podczas gdy w rzeczywistości jest.

Tabela nr 1 przedstawia wartości powyższych wskaźników dla wybranych biometryk. Najniższym wskaźnikiem błędnych akceptacji cechuje się tęczówka oka, co oznacza, że ryzyko jej podrobienia i pozytywnego przejścia przez weryfikację jest minimalne (zaledwie 0,001%). Podobną skuteczność wykazują odciski palców, jednak uzyskane wyniki posiadają szeroki zakres, w efekcie, nawet w 10 przypadkach na 100000 oszust jest w stanie ominąć system biometryczny. Biorąc pod uwagę szerokie zastosowanie danych daktyloskopijnych, jest to poziom bardzo istotny, a więc niebezpieczny. Pozostałe biometryki, za wyjątkiem obrazu twarzy, wykazują wysoki FAR, co powoduje, że ich wykorzystanie jest wielce

[17] B. Schouten, B. Jacobs, *Biometrics And Their Use in E-passports*, „Image and Vision Computing" 2009, vol. 27, nr 3, s. 306; R. Bolle, J. Connel, S. Pankanti, N. Ratha, A. Senior, op.cit., s. 77.

ryzykowne. Co ważne, w przypadku podpisu aż 5 weryfikacji na 100 jest błędnie akceptowanych, co pokazuje dość małą przydatność tej biometryki przy ustalaniu tożsamości.

Przechodząc do błędnych odrzuceń, najlepiej w tej kategorii wypada odcisk palca. Nie mniej wartość 0,3-0,7% jest bardzo wysoka przy tak szerokim ich zastosowaniu. Oznacza to, że od 3 do 7 weryfikacji na 1000 jest błędnie odrzucanych, uniemożliwiając uprawnionej osobie skorzystanie z danej usługi. Pozostałe biometryki, w tym równie powszechnie implementowany obraz twarzy, uzyskują wysokie i znacznie dalekie wartości, sięgające nawet 20%. Te wyniki należy ocenić negatywnie, gdyż prowadzą do wniosku, że biometryczna weryfikacja może generować dla jednostek poważne problemy uwierzytelniające, skutkujące brakiem uprawnionego dostępu oraz wykluczeniem.

Tabela nr 1. Przybliżone stopy błędów przy wybranych metodach biometrycznego ustalania tożsamości

Biometryka	FAR	FRR
Odcisk palca	1 do 10 ze 100000 **(0,001-0,01%)**	3 do 7 z 1000 **(0,3-0,7%)**
Obraz twarzy	100 do 1000 ze 100000 **(0,1-1%)**	10 do 20 ze 100 **(10-20%)**
Głos	2000 do 5000 ze 100000 **(2-5%)**	10 do 20 ze 100 **(10-20%)**
Tęczówka	$\geq 10^{-5}$ **(0,001%)**	2 do 10 ze 100 **(2-10%)**
Geometria dłoni	10 do 20 z 1000 **(1-2%)**	1 do 2 ze 100 **(1-2%)**
Podpis	2 do 5 ze 100 **(2-5%)**	10 do 20 ze 100 **(10-20%)**

Źródło: R. Bolle, J. Connel, S. Pankanti, N. Ratha, A. Senior, op.cit., s. 133.

Z powyższych badań wypływa wniosek, że biometryczne metody ustalania tożsamości cechują się dość wysokim wartościami błędnych weryfikacji. Choć w skali mikro wyniki FAR i FRR są minimalne, to w obszarze makro mają one istotne znaczenie dla powodzenia procedur uwierzytelniania, gdyż zwiększają prawdopodobieństwo oszustw lub problemów tożsamościowych. Wydaje się zatem, że bazowanie wyłącznie na samych biometrykach jest niewłaściwe, muszą być one uzupełnione o dodatkowe, awaryjne procedury weryfikacyjne, które wyeliminują luki. Rzeczone procedury muszą siłą rzeczy opierać się na tradycyjnych identyfikatorach[18].

Biometria w paszportach państw członkowskich UE

[18] Zob. także: *Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, Article 29 Data Protection Working Party, 1710/05/EN-rev, WP 112, Brussels, 30 September 2005, s. 8.

Paszporty biometryczne pojawiły sie w Unii Europejskiej pod wpływem trzech czynników. Po pierwsze, w wyniku zamachów z 11 września 2001 r. powstała idea zwiększenia bezpieczeństwa w ruchu powietrznym m.in. poprzez rozbudowaną kontrolę pasażerów oraz wprowadzenie specjalnych dokumentów podróży zawierających biometryki, uznawane wówczas za najlepszą formę sprawdzania tożsamości[19]. Takie działania miały zapobiegać przenikaniu ponad granicami terrorystów lub osób o fałszywych tożsamościach. Już w roku zamachów wrześniowych Departament Stanu Stanów Zjednoczonych rozpoczął wydawanie paszportów odczytywanych maszynowo (MRP - *Machine Readable Passports*) zawierających cyfrową biometrykę twarzy. Idea biometrycznego bezpieczeństwa znalazła również poparcie w Europie, przede wszystkim po zamachach terrorystycznych w Madrycie (11 marca 2004 r.) i w Londynie (7 lipca 2005 r.)[20].

Po drugie, postulat implementacji paszportów biometrycznych pojawił się na forum Organizacji Narodów Zjednoczonych (ONZ) oraz jej agencji wyspecjalizowanych[21]. Już 28 maja 2003 r. Międzynarodowa Organizacja Lotnictwa Cywilnego (ICAO) przyjęła strategię „*Blueprint*", w której zalecała umieszczanie w paszportach bezkontaktowego, zintegrowanego obwodu (czipa) o minimalnej pojemności 32 kilobajtów (KB), zawierającego obraz twarzy (10 KB) lub, fakultatywnie, odciski palców (12 KB) i/lub tęczówkę oka (30 KB)[22]. W pracach ICAO brała udział Komisja Europejska, która zobowiązała się do wdrożenia powyższego standardu do prawodawstwa UE.

Po trzecie, istotnym czynnikiem wprowadzenia biometrii do paszportów były działania Stanów Zjednoczonych. W 2002 r. Kongres USA uchwalił *Enhanced Border Security and Visa Entry Reform Act*, na mocy którego wprowadzono system US VISIT (*United States Visitor and Immigrant Status Indicator Technology*), nakazujący pobieranie dziesięciu lub dwóch odcisków palców oraz cyfrowego zdjęcia twarzy wszystkich obcokrajowców wkraczających do Stanów Zjednoczonych na podstawie wizy[23]. Głównym

---

[19] N. Moradoff, op.cit., s. 279-281; A. Kirpsza, *Implikacje wydarzeń z 11 września dla rzeczywistości politycznej z perspektywy konstruktywizmu społecznego*, [w:] D. Kliabanau, W. Kudela-Świątek, U. Trojanowska, A. Wawrzyńczak (red.), *Świat po katastrofie. Materiały z konferencji*, Kraków 2010, s. 99-115.

[20] Zob.: A. Kirpsza, *Relacje transatlantyckie w zakresie biometryzacji przepływu osób z perspektywy Unii Europejskiej i Polski*, [w:] J. Cisek (red.), *Współczesne relacje transatlantyckie*, Kraków 2010, s. 28.

[21] Zob.: *World Economic and Social Survey 2004. International Migration*, Department of Economic and Social Affairs, United Nations, New York 2004, s. 83.

[22] Specyfikacje są zawarte w dokumencie zwanym Doc 9303, składającym się z trzech części: „*Machine readable Passports*", „*Machine Readable Visas*", „*Machine Readable Official Travels Documents*". Dokument jest publikowany od 1980 r., a każda z jego części ma swoje okresowe nowelizacje. Zob.: *ICAO MRTD Report*, vol. 1, nr 1, 2006, http://www2.icao.int/en/MRTD/Downloads/ ICAO%20MRTD%20Report/ ICAO% 20 MRTD%20Report%20Vol.%201%20No.%201,%202006.pdf.

[23] *Ustawa z roku 2002 w sprawie zwiększenia bezpieczeństwa granicznego i reformy wiz wjazdowych (Enhanced Border Security and Visa Entry Reform Act)*, H.R. 3525, sekcja 303.

celem takiego rozwiązania była próba zapobiegania niekontrolowanej migracji do tego państwa terrorystów, którzy, wykorzystując wady tradycyjnych dokumentów, mogliby podszywać się pod tożsamość innych osób. Obowiązek składania biometryk został również określony dla obywateli państw objętych ruchem bezwizowym ze Stanami Zjednoczonymi (tzw. *Visa Waiver Program VWP* - program uchylenia wymogu posiadania wizy). Każdy kraj przyjęty do VWP miał najpóźniej do 26 października 2004 r. wprowadzić program wydawania swoim obywatelom paszportów do odczytu maszynowego zabezpieczonych przed fałszowaniem i zawierających identyfikatory biometryczne spełniające standardy ICAO[24]. Termin ten został później przesunięty o dwa lata, do 26 października 2006 r.[25]. Państwa, które nie dostosowałyby się do tego wymogu, miały być usunięte z VWP.

W wyniku powyższych czynników, Komisja Europejska przedstawiła 18 lutego 2004 r. projekt rozporządzenia w sprawie nowego standardu dokumentów paszportowych w Unii Europejskiej[26]. Po zaledwie kilku miesiącach regulacja została przyjęta 13 grudnia 2004 r. w ramach procedury konsultacji[27]. Uzyskała ona moc obowiązującą w stosunku do wszystkich stron *acquis* Schengen, a więc bez Danii (która jednak w 2006 r. przystąpiła do implementacji rozporządzenia), Wielkiej Brytanii, Irlandii oraz wobec pozaunijnych członków Europejskiego Obszaru Gospodarczego, czyli Islandii, Norwegii, Lichtensteinu i Szwajcarii. Rozporządzenie zostało znowelizowane w 2009 r.[28].

W tym miejscu należy stwierdzić, że proces uchwalania rozporządzenia i jego nowelizacji był daleki od demokratycznych standardów. Otóż, art. 28 ust. 2 rozporządzenia nr 45/2001[29] stanowi, że „przyjmując projekty aktu prawnego odnoszącego się do ochrony praw i wolności osoby fizycznej w odniesieniu do przetwarzania danych osobowych, Komisja konsultuje się z europejskim inspektorem ochrony danych". Projekt pierwotnej regulacji dotyczącej paszportów biometrycznych spełniał te kryteria, ponieważ został zaproponowany przez Komisję w lutym 2004 r., a więc już po ustanowieniu Europejskiego Inspektora

[24] Ibidem, akapit b ust. 3.
[25] H.R. 4417 z dnia 9 sierpnia 2004 r.
[26] *Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports*, Commission of the European Communities, COM/2004/0116 final, Brussels, 18 February 2004.
[27] *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*, „Dziennik Urzędowy UE" z 29 grudnia 2004 r., L 385, s. 1-6.
[28] *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*, „Dziennik Urzędowy UE" z 6 czerwca 2009 r., L 142, s. 1-4.
[29] *Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych*, „Dziennik Urzędowy WE" z 12 stycznia 2001 r., L 8, s. 1-23.

Ochrony Danych (dalej EIOD)[30] i wejściu w życie rozporządzenia 45/2001[31], oraz zawierał postanowienia o przetwarzaniu danych osobowych, jakimi są biometryki. Mimo to, Komisja nie zawnioskowała o opinię inspektora, przez co rozporządzenie zostało przyjęte bez kontroli pod kątem jego konsekwencji dla prywatności obywateli UE. Co więcej, Komisja nie wywiązała się z ciążącego na niej obowiązku konsultacji także w przypadku nowelizacji tej regulacji (rozporządzenie nr 444/2009), przez co EIOD musiał zaproponować swoją opinię z urzędu[32]. Można zatem stwierdzić, że przepisy w sprawie paszportów biometrycznych zostały uchwalone ze złamaniem prawa wtórnego UE.

Kolejnym zarzutem dotyczącym procesu uchwalania rozporządzenia w sprawie paszportów biometrycznych jest brak szerokiej debaty publicznej. Postulowali o nią uczestnicy 27 Międzynarodowej Konferencji Rzeczników Ochrony Prywatności i Danych Osobowych w Montreux, wskazując w przyjętej rezolucji, że „powszechne stosowanie technologii biometrycznych pociągnie za sobą dalekosiężne skutki dla bezpieczeństwa światowego, powinno zatem stanowić przedmiot globalnej debaty"[33]. Biorąc pod uwagę fakt, że rozporządzenie o paszportach było pierwszą regulacją implementującą biometrię na tak szeroką skalę w Unii Europejskiej oraz że w istotny sposób ingeruje ona w prywatność, projekt powinien być długo i powszechnie dyskutowany w gronie ekspertów i organizacji pozarządowych. Tymczasem, rozporządzenie zostało przyjęte po zaledwie dziewięciu miesiącach negocjacji, z których wyłączeni byli obywatele, Parlament (z racji procedury konsultacji)[34], a nawet EIOD. Proces uchwalania nie spełnił zatem standardów demokratycznych zawartych w Traktatach UE[35].

Rozporządzenie obliguje państwa członkowskie do umieszczenia w krajowych paszportach środka pamięci (*storage medium*) w formie czipa zawierającego dwa poziomy zabezpieczeń biometrycznych (art. 1 ust. 2 i art. 6 rozporządzenia). Pierwszy ma charakter

---

[30] *Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor)*, „Dziennik Urzędowy WE" z 17 stycznia 2004 r., L 12, s. 47. EIOD zaczął funkcjonować od 1 stycznia 2004 r.

[31] Rozporządzenie weszło w życie dwudziestego dnia po publikacji w „Dzienniku Urzędowym WE", a więc 1 lutego 2001 r. Zob.: art. 5 rozporządzenia.

[32] *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*, „Dziennik Urzędowy UE" z 6 sierpnia 2008 r., C 200, s. 1-5.

[33] *Rezolucja XXVII Międzynarodowej konferencji rzeczników ochrony prywatności i danych osobowych w Montreux o stosowaniu danych biometrycznych w paszportach, dowodach tożsamości i dokumentach podróży*, http://www.privacyconference2005.org/.

[34] Parlament posiada słabą pozycję w procedurze konsultacji, ograniczającą się do proponowania niewiążących opinii. Zob.: R. Kardasheva, *The Power to Delay: The European Parliament's Influence in the Consultation Procedure*, „Journal of Common Market Studies" 2009, vol. 47, nr 2, s. 385-409.

[35] Zob.: art. 10 TUE.

obligatoryjny i jest to zapis obrazu twarzy, który miał być wprowadzony do paszportów na 18 miesięcy od daty przyjęcia specyfikacji technicznych, czyli do 28 sierpnia 2006 r.[36]. Drugi poziom jest fakultatywny i stanowi dwa odciski palca (wskazującego lewej i prawej dłoni), a okres jego implementacji miał trwać do 36 miesięcy od wydania specyfikacji, czyli do 28 czerwca 2009 r.[37]. Art. 4 ust. 3 rozporządzenia dodaje, że dane biometryczne zgromadzone w nośniku pamięci mogą być wykorzystywane tylko w dwóch celach: sprawdzania autentyczności paszportu i sprawdzania tożsamości jego posiadacza, przy czym to drugie tylko w przypadkach, gdy okazanie paszportu jest wymagane przepisami prawa.

Powyższe postanowienia generują co najmniej cztery wątpliwości. Po pierwsze, rozporządzenie umożliwia wykorzystywanie i przechowywanie danych biometrycznych, co należy uznać za ingerencję w prawo do prywatności. Takie stanowisko wynika z faktu, że biometria zmienia w sposób nieodwracalny stosunek pomiędzy ciałem a tożsamością: cechy ciała ludzkiego stają się przedmiotem odczytu maszynowego, mogą być dalej wykorzystywane bez względu na miejsce przebywania ich właściciela oraz zawierają wrażliwe informacje o ich posiadaczu, np. o stanie zdrowia, płci, wieku, sposobie życia czy chorobach[38]. Pogląd ten potwierdza wyrok *S. i M. Marper* z 2008 r., w którym Europejski Trybunał Praw Człowieka zmienił dotychczasową linię orzeczniczą[39] i uznał, że gromadzenie odcisków palców już samo w sobie jest ingerencją w prawo do prywatności[40]. Oznacza to, że rozporządzenie musi spełniać wymogi, jakie nakłada art. 8 ust. 2 Konwencji Rady Europy o Ochronie Praw Człowieka i Podstawowych Wolności (dalej EKPCZ)[41], stanowiący, że „niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem

---

[36] Specyfikacje techniczne dotyczące wizerunku twarzy zostały przyjęte decyzją Komisji Europejskiej z 28 lutego 2005 r. Zob.: *Commission Decision C(2005) 409 of 28 February 2005 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (Decision not published in Official Journal)*.

[37] Specyfikacje techniczne dotyczące odcisków palców zostały przyjęte decyzją Komisji Europejskiej z 28 czerwca 2006 r. Zob.: *Commission Decision C(2006) 2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (subsequent amendments contained in the Commission Decision C(2009) 7476 of 5 October 2009 and the Commission Decision C(2011) 5499 of 4 August 2011)*.

[38] Y. Liu, *Identifying Legal Concerns in the Biometric Context*, „Journal of International Commercial Law and Technology" 2008, vol. 3, nr 1, s. 46.

[39] Raport z dnia 18 marca 1981 r. w sprawie *McVeigh O'Neill i Evans przeciwko Zjednoczonemu Królestwu*, „Decisions and Reports", tom. 24, s. 15 i nast.; U. Kilkelly, *The right to respect for private and family life. A guide to the impementation of Article 8 of the European Convention on Human Rights*, „Human Rights Handbooks" 2001, nr 1, s. 35-36; *Kinnunen przeciwko Finlandii*, decyzja z dnia 15 maja 1996 r., skarga nr 24950/94; *P.G. i J.H. przeciwko Zjednoczonemu Królestwu*, wyrok z dnia 25 września 2001 r., skarga nr 44767/98; Raport Komisji z dnia 19 maja 1994 r. przyjęty w sprawie *Ludwig Friedl przeciwko Austrii*, skarga nr 15225/89; *Van der Velden przeciwko Niderlandom*, decyzja z dnia 7 grudnia 2006 r., skarga nr 29514/05.

[40] *S. and M. Marper przeciwko Zjednoczonemu Królestwu Wielkiej Brytanii*, wyrok Wielkiej Izby Trybunału z dnia 4 grudnia 2008 r., skargi nr 30562/04 i 30566/04.

[41] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności*, Dz. U. z 1993 r., Nr 61, poz. 284.

przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób". Analiza regulacji prowadzi do wniosku, że choć spełnia ona test ustawy, gdyż w świetle art. 289 TfUE stanowi akt ustawodawczy przyjęty w ramach specjalnej procedury ustawodawczej, to trudno stwierdzić, że jest konieczna w demokratycznym społeczeństwie. Zakres rozporządzenia nie dotyczy bowiem wymienionych w art. 8 ust 2 EKPCZ interesów stanowiących podstawę do legalnego ograniczenia prawa. Jak pokazuje motyw 2 rozporządzenia, jego celem jest tylko „określenie wzmocnionych, zharmonizowanych norm dotyczących zabezpieczeń służących ochronie paszportów i dokumentów podróży przed fałszerstwami", natomiast art. 4 ust. 3 rzeczonej regulacji ogranicza wykorzystanie biometryk do celów sprawdzania autentyczności dokumentów i tożsamości ich posiadaczy. Nie są to zatem postanowienia mające na celu zapewnianie bezpieczeństwa publicznego, ochronę porządku czy zapobieganie przestępczości, lecz wyłącznie techniczne unormowania określające standard ograniczający zjawisko podrabiania paszportów i ich wykorzystywania w bezprawnych celach. Takie cele mogą być w zupełności osiągnięte tradycyjnymi środkami bez użycia biometryk, chociażby poprzez restrykcyjne kontrole na przejściach granicznych, odpowiednie procedury wydawania paszportów czy wyrafinowany standard zabezpieczeń alfanumerycznych w tych dokumentach. W tym kontekście, trudno uzasadnić konieczność zastosowania biometrii w paszportach.

Po drugie, oparcie systemu uwierzytelniania paszportów na dwóch biometrykach narusza zasadę proporcjonalności[42]. Zgodnie z art. 6 ust. 1 dyrektywy 95/46/WE[43] dane osobowe, jakimi są biometryki, muszą być „gromadzone do określonych, jednoznacznych i legalnych celów" oraz „stosowne i nie nadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone". Trudno zatem uznać, że wykorzystanie aż dwóch danych biometrycznych jest stosowne i nie nadmierne ilościowo w stosunku do celów, które rozporządzenie określa jako sprawdzanie autentyczności paszportu i tożsamości jego posiadacza[44]. Wydaje się, że już sama obecność biometryki twarzy jest właściwym środkiem uwierzytelniania danej osoby, która w połączeniu z procedurą awaryjną znacznie obniżyłaby

[42] Zob.: Y. Liu, *The Principle of Proportionality in Biometrics: Case Studies from Norway*, „Computer Law & Security Review" 2009, vol. 25, nr 3, s. 237-250.

[43] *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*, „Dziennik Urzędowy WE" z 23 listopada 1995 r., L 281, s. 31-51.

[44] Podobne stanowisko zajęła Grupa Robocza ds. Ochrony Danych ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Zob.: *Opinia 3/2005 w sprawie wprowadzenia w życie rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r....*, op.cit., s. 6.

ryzyko podrabiania dokumentów. Ponadto, pobieranie odcisków palców jest standardem wyłącznie w celach policyjno-kryminalnych, do których polityka paszportowa z pewnością nie należy. Wreszcie, może często się zdarzyć sytuacja, że jedna biometryka będzie poświadczać personalia jej właściciela, podczas gdy druga już nie, co oznacza niepewność co do właściwej tożsamości tej osoby. Brak dwukrotnej weryfikacji z powodów technicznych przy braku procedury awaryjnej może rodzić poważne konsekwencje dla posiadaczy paszportów.

Po trzecie, użycie przez ustawodawcę terminu „sprawdzania tożsamości" oznacza, że dane biometryczne mogą być wykorzystane zarówno w celu weryfikacji jak i identyfikacji, co zależy od sposobu regulacji tej kwestii w prawie krajowym. Tym sposobem rozporządzenie umożliwia państwom członkowskim wprowadzenie modelu identyfikacyjnego, polegającego na zbudowaniu centralnej bazy danych zawierającej biometryki osób aplikujących o paszporty. Jak już pokazano powyżej, mechanizm ten jest szczególnie niebezpieczny, gdyż najmocniej ingeruje w prywatność jednostek, umożliwiając organom państwowym, a w przypadku współpracy transgranicznej także podmiotom z innych państw, na rozpoznawanie pełnej tożsamości obywatela i wykorzystywania związanych z nią informacji w sposób niekontrolowany i w celach policyjnych. Praktyka pokazuje, że państwa członkowskie bardzo chętnie korzystają z powyższej furtki pozostawionej przez rozporządzenie i wybierają model identyfikacyjny. W 2007 r. Grupa robocza powołana na mocy art. 29 dyrektywy 95/48/WE przeprowadziła sondaż wśród narodowych inspektorów ochrony danych osobowych państw członkowskich na temat stosowania postanowień rozporządzenia o paszportach[45]. Wynika z niego, że na stan prawny z 2007 r. tylko nieliczna grupa krajów stosuje system weryfikacyjny (Francja, Litwa, Włochy, Szwecja, Holandia Niemcy), jednak część z nich już wtedy planowała utworzyć centralną bazę danych[46]. Reszta bazuje na systemie identyfikacyjnym.

Należy również dodać, że w memorandum do projektu rozporządzenia Komisja zasugerowała utworzenie w długoterminowej perspektywie centralnego, europejskiego rejestru paszportów wraz ze znajdującymi się w nich danymi biometrycznymi[47]. Taki pomysł jest bardzo kontrowersyjny i skłania do wniosku, że jego realizacja stanowiłaby przekroczenie kompetencji Unii Europejskiej przyznanych jej przez państwa członkowskie (tzw. zasada

[45] *Letter dated 10 December 2007 from the Chairman of the Article 29 Working Party to Mr. Jean-Marie Cavada, Chairman of the LIBE Committee, on EU passports*, European Commission: DG Justice, D (2007) 17402, Brussels, 10 December 2007, s. 2.
[46] *Annex: Replies by National Data Protection Authorities*, [w:] Ibidem, s. 3.
[47] Zob.: *Sprawozdanie w sprawie projektu Komisji dotyczącego rozporządzenia Rady w sprawie norm dla funkcji bezpieczeństwa i biometrii w paszportach obywateli UE (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS))*, PE 347.098v03-00, A6-0028/2004, 28 października 2004 r.

przyznania)[48]. Utworzenie scentralizowanej bazy danych łamałoby również zasadę proporcjonalności, trudno bowiem znaleźć powód i adekwatność tak poważnej ingerencji w prywatność osób w zakresie korzystania z prawa do poruszania się. Ponadto, europejska baza byłaby trudniejsza do kontroli niż baza krajowa, zwiększałaby ryzyko nadużyć w postaci niezgodnego z przeznaczeniem wykorzystywania biometryk (tzw. pełzające kompetencje - *creeping competences*)[49] lub użycia ich jako „klucza dostępu" do innych baz danych (np. SIS II), a przez to do łączenia pomiędzy sobą serii danych. Ponieważ w rozporządzeniu nie znalazła się poprawka Parlamentu zakazująca utworzenia w przyszłości centralnej bazy danych biometrycznych zawartych w paszportach, trudno wykluczyć jej powstanie[50].

Po czwarte, jak pokazano w pierwszej części, uwierzytelnianie za pomocą odcisków palców i obrazu twarzy wcale nie doprowadzi do skutecznej identyfikacji właścicieli paszportu, gdyż cechuje się wysokim poziomem błędów. Potwierdzają to dane statystyczne US VISIT z 2004 r. - na 118 000 osób, które przechodzą przezeń każdego dnia, 22 350 osób jest poddawanych drugiej, awaryjnej kontroli tożsamości, podczas gdy 1 811 osób jest odrzucanych z zakazem wjazdu. Co istotne, spośród osób, wobec których zastosowano zapasową kontrolę tożsamości, aż 92% zostało zweryfikowanych pozytywnie. Oznacza to, że skuteczność metod biometrycznych jest niska, gdyż nie potrafią one prawidłowo zweryfikować aż 20 562 osób (92% z 22 350) w ciągu jednego dnia[51]. Te same obserwacje wynikają z badań holenderskiego urzędu paszportowego, w których ok. 16% osób, których odciski były wpisane do bazy danych, nie mogło być poprawnie zweryfikowanych z powodu uszkodzonych, brudnych, suchych czy przetłuszczonych palców[52]. Bazowanie wyłącznie na biometrykach może zatem prowadzić do negatywnych konsekwencji w postaci zawrócenia na granicy osoby uprawnionej do wstępu do danego kraju, uznania za terrorystę czy pozytywnej weryfikacji oszusta podszywającego się pod inną osobę. W celu pokonania tych problemów potrzebna jest awaryjna, alternatywna procedura o charakterze niebiometrycznym, a więc mechanizm pozwalający weryfikować daną osobę za pomocą innych informacji alfanumerycznych (np. dowodu osobistego), w sytuacji gdy biometryki zawiodą[53]. Rozporządzenie nie przewiduje jednak takiej procedury.

---

[48] Art. 4 ust. 1 TUE.

[49] Zob.: M. Pollack, *The End of Creeping Competences? EU Policy-Making Since Maastricht*, „Journal of Common Market Studies" 2000, vol. 38, nr 3, s. 519-538; idem, *Creeping Competence: The Expanding Agenda of the European Community*, „Journal of Public Policy" 1994, vol. 14, nr 2, s. 95-145.

[50] Zob. *Sprawozdanie w sprawie projektu Komisji dotyczącego rozporządzenia Rady...*, op.cit., poprawka 5.

[51] D. Moss, *Biometrics: still much too unreliable for everyday use*, „Nature" 2007, vol. 449, nr 7162, s. 535.

[52] B. Schouten, B. Jacobs, op.cit., s. 310.

[53] Zob.: Raport Ministerstwa Spraw Wewnętrznych Holandii, *2b or not to 2b*, The Ministry of the Interior and Kingdom Relations, The Netherlands, 2005, http://www.minbzk.nl/contents/pages/43760/evaluatierapport1.pdf/.

Rozporządzenie nie określa również grupy osób, od których należy pobierać dane biometryczne do paszportów. Oznacza to, że obowiązek ten dotyczy wszystkich, którzy w świetle prawa krajowego są uprawnieni do uzyskania tego dokumentu. Od tej zasady istnieje jednak kilka wyjątków. Po pierwsze, rozporządzenie stanowi, że o ile obraz twarzy jest pobierany od wszystkich osób ubiegających się o paszport, o tyle z obowiązku oddawania odcisków palców zwolnione są dzieci do 12 roku życia[54]. Takie unormowanie wynika z licznych badań empirycznych wskazujących, że pobieranie danych daktyloskopijnych od dzieci jest praktycznie niemożliwe, gdyż w tak młodym wieku odciski się dopiero formują, a do szóstego roku życia są nawet niewidoczne[55]. Po drugie, art. 1 ust. 2a rozporządzenia zwalnia z oddawania odcisków palców osoby, od których pobranie tych biometryk jest fizycznie niemożliwe. Jest to zrozumiałe, biorąc pod uwagę fakt, że nie wszystkie osoby mają linie papilarne, co może być spowodowane utratą dłoni lub palców, ale także chorobą genetyczną (np. adermatoglifia), zażywaniem leków przeciwnowotworowych (np. popularnej kapecitabiny) czy celowego ich usuwania za pomocą zabiegu dermatologicznego zwanego dermabrazją. Po trzecie, art. 1 ust. 2 b rozporządzenia stanowi, że w przypadku gdy pobranie jakichkolwiek odcisków palców jest chwilowo niemożliwe, państwa członkowskie mogą wydać paszport tymczasowy o okresie ważności wynoszącym 12 miesięcy lub mniej. Co jednak istotne, o ile akt prawny określa dolną granicę wieku osób, od których wymaga się oddania danych daktyloskopijnych, o tyle nie przewiduje on górnego wieku osób, które nie muszą przedstawiać swoich biometryk, aby uzyskać paszport. Brak takiego postanowienia stanowi problem, gdyż badania empiryczne pokazują, że dokładność i możliwość wykorzystywania odcisków palców maleje wraz z wiekiem[56], a jakość linii papilarnych u osób powyżej 65 roku życia jest już tak słaba, że w praktyce prowadzi do dramatycznego wzrostu ryzyka błędów identyfikacyjnych[57]. W efekcie, osoby starsze mogą stać się podmiotem błędnych odczytów, a nawet komplikacji związanych z używaniem paszportów na przejściach granicznych, co w ich wieku jest szczególnie uciążliwe. Brak w rozporządzeniu górnej granicy wiekowej poboru biometryk jest zresztą wyjątkiem w skali globalnej - np. system paszportowo-wizowy Stanów Zjednoczonych US-VISIT określa go na 79 lat[58].

---

[54] Granica 12 lat ma charakter tymczasowy. Do 26 czerwca 2012 r. Komisja ma przedstawić sprawozdanie w kwestii ostatecznej dolnej granicy wiekowej poboru odcisków palców. Zob.: art. 1 ust. 2a i art. 5a rozporządzenia.

[55] B. Schouten, B. Jacobs, op.cit., s. 310; Zob.: motyw 3 rozporządzenia.

[56] N. Sickler, S. Elliott, *An Evaluation of Fingerprint Image Quality Across An Elderly Population vis-a-vis An 18-25 Year Old Population*, Proceedings of the 39th Annual International Carnahan Conference on Security Technology (ICCST), Las Palmas de G. C., Spain 2005, s. 61-68; A. Hicklin, R. Khanna, op.cit., s. 19.

[57] B. Schouten, B. Jacobs, op.cit., s. 307.

[58] *DHS Issues RFI to Improve US VISIT Identification Capabilities*, „Terror Response Technology Report" 2011,

Motyw trzeci rozporządzenia stanowi, że przy technicznej implementacji danych biometrycznych do paszportów „należy wziąć pod uwagę wymogi Międzynarodowej Organizacji Lotnictwa Cywilnego (ICAO), w szczególności zawarte w dokumencie 9303 dotyczącym dokumentów podróży nadających się do odczytu maszynowego". Jednakże umieszczenie powyższych wymogów jako źródła prawa, według którego zabezpiecza się biometryki, jest niewłaściwe. Dokumenty ICAO są zwykłymi wytycznymi zaliczanymi do *soft law*, które nie mają charakteru bezpośrednio wiążącego i co roku są poddawane ciągłym poprawkom w niejasnej i pozbawionej demokratycznego mandatu procedurze[59]. Co więcej, dotyczą sposobów gromadzenia i technicznych standardów biometryk, a więc kwestii ingerujących w prawo do prywatności, co oznacza, że zgodnie z art. 8 ust. 2 EKPCZ muszą posiadać status aktu ustawodawczego. Trudno jednak przyznać, aby wytyczne ten wymóg spełniały. Biorąc pod uwagę fakt, że kwestia zabezpieczenia tak wrażliwych danych, jakimi są biometryki, jest w kontekście prawa do prywatności kluczowa, powinna bazować na pewniejszych, stabilnych, przyjmowanych w demokratyczny sposób i zaskarżalnych przepisach na gruncie prawie UE.

W motywie ósmym i art. 4 ust. 2 rozporządzenia można także znaleźć stwierdzenie, że „w paszporcie lub dokumencie podróży nie umieszcza się żadnych informacji w formie nadającej się do odczytu maszynowego, o ile nie stanowi o tym niniejsze rozporządzenie lub załącznik do niego, lub o ile informacja o tym nie została umieszczona w paszporcie lub dokumencie podróży przez wydające państwo członkowskie zgodnie z jego przepisami krajowymi". Przepis ten otwiera drogę do tylnego wprowadzania przez państwa członkowskie innych danych osobowych lub biometrycznych (pod warunkiem, że nie są odczytywane maszynowo, a np. ręcznie) za pomocą załączników czy nawet odpowiedniej klauzuli umieszczanej na dokumencie podróży. Z pewnością nie są to instrumenty prawne o charakterze ustawowym, przez co regulacja ta narusza art. 8 ust. 2 EKPCZ. Należałoby zatem jednoznacznie określić, jakie dokładnie informacje mają być przechowywane w paszporcie i nie ustanawiać żadnych przepisów umożliwiających wyjątki od tej zasady.

Polski paszport biometryczny

Uchwalenie unijnego rozporządzenia w sprawie paszportów biometrycznych doprowadziło do rozpoczęcia prac na dostosowaniem do niego polskiego dokumentu

---

vol. 7, nr 15, s. 16.

[59] Zob.: *Sprawozdanie w sprawie projektu Komisji dotyczącego rozporządzenia Rady...*, op.cit., poprawka 3.

podróży[60]. Ich efektem jest ustawa o dokumentach paszportowych, która weszła w życie 28 sierpnia 2006 r.[61]. Analizując przepisy regulujące polski paszport biometryczny, można przedstawić cztery zarzuty.

Po pierwsze, w ustawie przyjęto identyfikacyjny model ustalania tożsamości. Zgodnie z art. 49 ust. 3 ustawy, pobrane biometryki są najpierw gromadzone w ewidencjach administrowanych przez organy paszportowe, które niezwłocznie po podjęciu decyzji o wydaniu, odmowie wydania lub unieważnieniu dokumentu paszportowego przekazują je do Centralnej Ewidencji Wydawanych i Unieważnianych Paszportów prowadzonej przez ministra właściwego do spraw wewnętrznych. Po wydaniu i przyjęciu paszportu z ewidencji organów paszportowych usuwa się odciski palców (obraz twarzy zostaje) i od tego momentu wszystkie dane biometryczne są przechowywane w centralnej ewidencji. Kwestie funkcjonowania ewidencji centralnej i paszportowych reguluje rozporządzenie[62]. Jak już kilka razy podkreślano, model identyfikacyjny jest najbardziej ingerencyjnym i wrażliwym sposobem ustalania tożsamości, trudno więc zrozumieć, po co władzom tak rozbudowana baza danych osobowych swoich obywateli, skoro celem regulacji paszportowych jest tylko sprawdzanie autentyczności dokumentów i tożsamości ich posiadacza. Cele te mogą być całkowicie i skutecznie realizowane przy użyciu weryfikacji.

Po drugie, efektem ustanowienia centralnej bazy danych biometrycznych w odniesieniu do paszportów jest zapewnienie odpowiednim organom dostępu do zawartych w niej informacji. Katalog tych podmiotów określa art. 52 ust. 1-3 ustawy - są to: organ paszportowy, Komendant Główny Straży Granicznej, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, minister właściwy do spraw finansów publicznych, policja, prokurator, sąd, Służba Więzienna, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Żandarmeria Wojskowa i państwa, którym dostęp do danych umożliwiają umowy międzynarodowe, których stroną jest Polska. Tak duża liczba organów uprawnionych do przeszukiwania bazy danych biometrycznych stanowi złamanie zasady proporcjonalności, gdyż z jednej strony nie jest adekwatna do celów wyrażonych w art. 1 ustawy[63], z drugiej zaś, cechuje się obecnością

[60] Zob.: *Program dostosowania systemu paszportowego oraz dokumentów podróży wydawanych cudzoziemcom przez władze polskie do wymogów prawa unijnego*, Ministerstwo Spraw Wewnętrznych i Administracji, Urząd do spraw Repatriacji i Cudzoziemców, Warszawa 2006.

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

[62] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 lutego 2010 r. w sprawie ewidencji paszportowych i centralnej ewidencji*, Dz. U z 2010 r., Nr 26, poz. 131.

[63] Zgodnie z art. 1, ustawa określa: 1) rodzaje dokumentów paszportowych; 2) właściwość organów wydających dokumenty paszportowe; 3) okoliczności uzasadniające odmowę wydania lub unieważnienie dokumentu paszportowego; 4) zakres danych wpisywanych do dokumentu paszportowego; 5) zakres danych zawartych w

wielu podmiotów o kompetencjach policyjnych, których rola w polityce paszportowej i zakresie ustawy jest trudna do zdefiniowania. Trudno również znaleźć uzasadnienie dla konieczności w demokratycznym społeczeństwie aż tak szerokiego dostępu do biometryk.

Po trzecie, w kontekście dokumentów paszportowych kluczową rolę odgrywają rozporządzenia wykonawcze. Ustawa w kilku miejscach deleguje na rzecz ministra właściwego do spraw wewnętrznych upoważnienie do wydawania aktów wykonawczych. Szczególne znaczenie posiada zawarte w art. 20 ust. 2 pkt 2 ustawy uprawnienie do określenia w drodze rozporządzenia „sposobu pobierania danych biometrycznych i zamieszczania ich w dokumentach paszportowych", którego efektem jest rozporządzenie w sprawie dokumentów paszportowych [64]. Pojawia się jednak pytanie czy tak ważne i wrażliwe kwestie proceduralne dotyczące pobierania biometryk nie powinny znaleźć się w ustawie jako gwarancja lepszej i bezpośredniej ochrony danych obywateli. Rozporządzenie zawiera szczegółowe i techniczne metody pobierania i gromadzenia biometryk, a zatem stanowi ingerencję w prywatność. Dlatego nie spełnia testu legalności zawartego w art. 8 ust. 2 EKPCZ, gdyż naruszenie tego prawa musi być uregulowane w ustawie.

Po czwarte, kontrowersje budzi również § 3 ust. 3 powyższego rozporządzenia, który stanowi, że „osoba nosząca nakrycie głowy zgodnie z zasadami swojego wyznania, ubiegająca się o wydanie paszportu albo paszportu tymczasowego, może złożyć fotografię przedstawiającą ją w nakryciu głowy, które nie może zakrywać ani zniekształcać owalu twarzy. W takim przypadku należy przedłożyć zaświadczenie o przynależności do wspólnoty wyznaniowej zarejestrowanej w Rzeczypospolitej Polskiej"[65]. Pojawia się pytanie, czy przepis ten nie jest niekonstytucyjny. Zgodnie bowiem z art. 53 ust. 7 Konstytucji: „Nikt nie może być obowiązany przez organy władzy publicznej do ujawnienia swojego światopoglądu, przekonań religijnych lub wyznania"[66]. Tymczasem rozporządzenie ewidentnie wymaga, aby takie przekonania ujawnić, co jest warunkiem *sine qua non* otrzymania paszportu[67].

Konkluzje

---

ewidencjach paszportowych oraz sposób prowadzenia tych ewidencji i zasady udostępniania danych w nich gromadzonych oraz organy właściwe w tych sprawach.

[64] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 2010 r. w sprawie dokumentów paszportowych*, Dz. U. z 2010 r., Nr 152, poz. 1026.

[65] Ibidem, s. 11741. Wcześniej § 4 ust. 2 *Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 24 sierpnia 2006 r. w sprawie dokumentów paszportowych oraz trybu postępowania w przypadku ujawnienia fałszerstw lub wad w tych dokumentach oraz w sytuacji ich zniszczenia*, Dz. U. z 2006 r., Nr 152, poz. 1090.

[66] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Dz. U. z 1997 r., Nr 78, poz. 483 z późn. zm.

[67] Zob także: A. Kirpsza, *Status prawny mniejszości narodowych i etnicznych w Polsce w świetle standardów Rady Europy*, [w:] J. Jaskiernia (red.), *Efektywność europejskiego systemu ochrony praw człowieka. Obszary analizy skuteczności europejskiego systemu praw człowieka*, Toruń 2012, s. 747.

Przeprowadzona w niniejszym artykule analiza implementacji biometrii w paszportach unijnych pokazała, że generuje ona liczne problemy i zagrożenia. Biometryczne metody uwierzytelniania stanowią poważną ingerencję w prywatność człowieka, prowadząc do nieodwracalnej zmiany stosunku jego ciała do tożsamości. Ten fakt nie jest bez znaczenia dla prawa, ponieważ generuje potrzebę redefinicji takich pojęć jak prywatność, integralność fizyczna czy przetwarzanie danych osobowych. Negatywne konsekwencje mogą także wynikać z powszechnego przyjmowania w Unii Europejskiej modelu biometrycznej identyfikacji polegającego na gromadzeniu wszystkich biometryk w państwowej, centralnej bazie danych. Podmioty posiadające do niej dostęp mogą nie tylko w sposób niekontrolowany monitorować poruszanie się i czynności osób, ale także dokładnie określić ich tożsamość, co stanowi ryzyko orwellowskiego „Wielkiego Brata". Wreszcie, biometryczne metody uwierzytelniania, wbrew powszechnej opinii, nie są idealnie skuteczne. Biometryki podlegają bowiem zmianom naturalnym lub mechanicznym, dlatego ich gromadzenie, wykorzystywanie i porównywanie jest niezmiernie utrudnione, a czasem nawet niemożliwe. Potwierdziła to analiza empiryczna, wykazując, że systemy biometryczne cechują się wysokim poziomem błędnych akceptacji (FAR) i odrzuceń (FRR), co grozi pozytywnym uwierzytelnianiem oszustów podszywających się pod tożsamość innych osób oraz zablokowanie dostępu do usług osobom uprawnionym.

Niestety, powyższe problemy i zagrożenia nie znajdują rozwiązania w rozporządzeniu o paszportach biometrycznych. Przede wszystkim, regulacja ta nie zalicza testu „konieczności w demokratycznym społeczeństwie" zawartego w art. 8 ust. 2 EKPCZ. Jej celem jest harmonizacja technicznych zabezpieczeń w paszportach zapewniających skuteczniejsze uwierzytelniania autentyczności dokumentów podróży i tożsamości ich posiadaczy, co nie pokrywa się z wyznaczonymi w Konwencji interesami umożliwiającymi legalną ingerencję w prawo do prywatności, takimi jak zapewnienie bezpieczeństwa publicznego, zapobieganie przestępstwom czy ochrona porządku publicznego. Rozporządzenie narusza również zdefiniowaną w dyrektywie 95/48/WE zasadę proporcjonalności, gdyż użycie dwóch biometryk jest nieadekwatne i nadmierne ilościowo w stosunku do przyjętych celów. Brakuje również wyraźnego określenia modelu sprawdzania tożsamości, co oznacza, że państwa członkowskie mogą wybierać szczególnie wrażliwy dla prywatności model identyfikacyjny. Praktyka pokazuje, że robią to bardzo chętnie, mówi się nawet o utworzeniu europejskiej centralnej bazy danych. Poza tym, regulacje paszportowe nie przewidują górnego wieku osób zobligowanych do oddania swoich biometryk, nie zawierają procedur awaryjnych

stosowanych w sytuacji, gdy biometryki okażą się zawodne oraz bazują na standardzie zabezpieczeń biometrycznych zaproponowanych w dokumentach ICAO, które nie mają statusu ustawy, nie są zaskarżalne i są przyjmowane w niedemokratycznej i niejasnej procedurze. Polski ustawodawca powiększa powyższą listę mankamentów, określając w regulacjach dotyczących krajowego paszportu biometrycznego szeroki zakres podmiotów, w tym policyjnych, posiadających dostęp do biometryk obywateli, umieszczając wrażliwe dla prywatności postanowienia w akcie wykonawczym, co jest niezgodne z art. 8 ust. 2 EKPCZ, a nawet wprowadzając niekonstytucyjne rozwiązania.