Adam Kirpsza*

RELACJE TRANSATLANTYCKIE W ZAKRESIE BIOMETRYZACJI PRZEPŁYWU OSÓB Z PERSPEKTYWY UNII EUROPEJSKIEJ I POLSKI

1. Pojęcie biometrii

Biometria[1] jest dziedziną nauki zajmującą się rozpoznawaniem tożsamości jednostki ludzkiej na podstawie jej cech[2]. Cechy te określa się mianem biometryk fizjologicznych i behawioralnych. Pierwsze zawierają informacje o charakterystyce fizycznej danej osoby – są to przede wszystkim odciski palców[3], obraz twarzy[4], geometria dłoni[5], kształt ucha[6], zapach ciała[7], obraz tęczówki[8], obraz siatkówki[9],

* Mgr Adam Kirpsza – absolwent stosunków międzynarodowych na Uniwersytecie Jagiellońskim, obecnie doktorant w Instytucie Nauk Politycznych i Stosunków Międzynarodowych UJ, student IV roku prawa UJ.

[1] Z greckiego: bios – życie, metron – miara, wielkość.

[2] R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, *Biometria*, Warszawa 2008, s. 4–10.

[3] H.C. Lee, R. Gaensslen, *Advances in Fingerprint Technology*, Boca Raton 1994, s. 1–38; M. Ścibior, *Na rękę i na oko*, „Polityka", 2004, nr 4; R. Bolle et alt., *Biometria…*, s. 36–29.

[4] J. Woodward, N. Orlans, P. Higgins, *Biometrics*, New York 2003, s. 73–74; M. Turk, A. Pentland, *Eigenfaces for Recognition*, „Journal of Cognitive Neuro Science", 1991, nr 3, s. 71–86.

[5] R. Zunkel, *Hand geometry based authentication*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal Identification in Networked Society,* Norwell 1999, s. 87–102.

[6] M. Burge, W. Burger, *Ear biometrics*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…*, s. 273–285.

[7] K. C. Persaud, D. H. Lee, H. G. Buyn, *Objective odoru measurements*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…,* s. 251–270.

[8] A. Pacut, A. Czajka, *Tęczówka, palec, dłoń… Biometryczne metody identyfikacji tożsamości*, „Biuletyn NASK", wrzesień–październik–listopad 2003, s. 14–15; J. Daugman, *Recognizing persons by their iris pattern*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…*, s. 103–122.

[9] J. Woodward, N. Orlans, P. Higgins, *op. cit*., s. 95–96; R. Hill, *Retina identification*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…,* s. 123–142.

DNA[10], termogramy[11]. Zasadą ich funkcjonowania jest niezmierna trwałość i niezależność od społecznych lub genetycznych transformacji. Drugie natomiast obrazują mechanizmy i sposoby wykonywania pewnych powtarzalnych czynności przez człowieka, takich jak podpis[12], głos[13], tempo pisania[14], chodu[15] czy ruch ust[16]. Ludzie ciągle uczą się biometryk behawioralnych, dlatego cechują się one zmiennością temporalną[17]. Ostatnio pracuje się także nad biometrykami kognitywnymi, to znaczy profilami mózgowymi otrzymywanymi na podstawie reakcji mózgu na bodźce zapachu czy percepcję twarzy[18].

Biometria jest odpowiedzią na krytykę tradycyjnych metod ustalania tożsamości, które polegają się 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[19]. Istotny element tej koncepcji stanowi zatem rozróżnienie podmiotu (jednostki)

---

[10] S. Pinker, *My Genome, My Self,* „The New York Times", 7 stycznia 2009, http://www.nytimes.com/2009/01/11/magazine/11Genome-t.html?_r=2&ref=magazine&pagewanted=all.

[11] F. Prokoski, R. Riedel, *Infrared identification of faces and body parts*, [w:] A. Jain, R. Bolle, R. Pankanti (red.), *Biometrics: Personal…,* s. 191–212.

[12] R. Plamondon, G. Lorette, *Automatic signature verification and writer identification – The state of the art*, „Pattern Recognition", 1989, nr 22, s. 107–131; R, Bolle et alt., *Biometria…*, s. 54–55.

[13] J. Campbell, *Speaker recognition*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…*, s. 165–190; R. Bolle et alt, *Biometria...,* s. 44–45; S. Furui, *Recent advances in speaker recognition*, „Lecture Notes in Computer Science", 1997, vol. 1206, s. 237–252.

[14] A. Pacut, A. Czajka, *Tęczówka, palec, dłoń…,* s. 15.

[15] Badaniem rozpoznawania chodu zajmuje się DARPA (Defence Advanced Research Projects Agency) – amerykańska agencja zajmującą się rozwojem militariów. Patrz: strona agencji i jej badania w zakresie *Human ID data a Distance*: http://www.darpa.mil/iao/HID.htm.

[16] Strona internetowa BioID, produktu firmy HumanScan, zajmującej się biometryką ruchu ust: http://www.bioid.com/.

[17] R. Bolle et alt., *Biometria…,* s. 12.

[18] Biometryki te są badane za pomocą testu Dooplera zwanego naukowo functional Transcranial Doppler (fTCD). Jednostka wykonuje kognitywne zadania (np. poddawana jest zapachowi), w wyniku których rejestruje się aktywność neuronów, a tym samym zmianę prędkości przepływającej przez mózg krwi. Zjawisko to pozwala określić w jaki sposób krew i mózg reagują na dany bodziec i na tej podstawie stworzyć profil biometryczny badanego. Patrz: P.C. Njemanze, *Cerebral lateralisation in random letter task in the visual modality: A transcranial Doppler study*, "Brain and Language", 1996, vol. 53, 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, s. 213–231.

[19] A. K. Jain, R. Bolle, S. Pankanti, *Introduction To Biometrics*, [w:] A. K. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…,* s. 3.

od przedmiotu (klucza, wiedzy), który jest jedynie środkiem weryfikacyjnym wyizolowanym od osoby. Problemem tradycyjnych metod rozpoznawania tożsamości jest łatwość zgubienia lub kradzieży obiektów identyfikujących, a w przypadku wiedzy – jej zapomnienia. Jak pokazują sondaże, prawie 25% respondentów przyznało, że zapisuje kod PIN na swoich kartach kredytowych, co czyni z nich potencjalne ofiary rabunków[20].

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, ponieważ 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. Ponadto, charakteryzują się one niemożliwością kradzieży czy zapomnienia – ich utrata może być spowodowana wyłącznie znacznym naruszeniem integralności fizycznej (odcięciem palca, wydłubaniem oka, odcięciem głowy itp.)[21].

Rozpoznawanie tożsamości jednostki jest dla biometrii celem, który może być realizowany w dwóch procesach: weryfikacji lub identyfikacji. Pierwszy polega na odpowiedzi na pytanie „Czy to jest X?". Osoba wprowadza do czytnika obiekt zawierający swoją biometrykę (np. odcisk palca w karcie ID) oraz dodatkowo samodzielnie umieszcza ją jeszcze raz na odpowiednim sensorze. Obie biometryki są następnie porównywane przez system między sobą oraz z poprzednio pobranymi od danej osoby weryfikatorami wprowadzonymi do bazy danych. Proces ten często określa się metodą *one-to-one matching* (1:1), ponieważ poprzez komparację danych jednostki zawartych w karcie, infrastrukturze informacyjnej i wprowadzanych „na żywo" otrzymuje się pozytywne lub negatywne określenie zgodności tożsamości danej jednostki[22].

Identyfikacja natomiast stara się odpowiedzieć na pytanie „Kim jest X?". Metoda ta polega na wprowadzeniu przez jednostkę własnej biometryki do czytnika, bez użycia jakichkolwiek obiektów dodatkowych (np. kart), po czym system poszukuje jej podobieństw z umieszczonymi wcześniej w bazie danych personaliami. Proces ten określa się *one-to-many matching* (1:N) – w wyniku porównywania nieznanej biometryki z innymi dochodzi do pozytywnego lub negatywnego odnalezienia pasujących informacji o tożsamości badanej

[20] J. Woodward, N. Orlans, P. Higgins, op. cit., s. 9.

[21] A. K. Jain, R. Bolle, S. Pankanti, *Introduction To Biometrics*, [w:] A. K. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…,* s. 4.

[22] J. Woodward, N. Orlans, P. Higgins, *op. cit.*, s.7.

osoby[23]. Identyfikacja jest popularna w kryminalistyce, pozwala określić nieznanego przestępcę na podstawie zostawionych przez niego śladów. Funkcjonuje jeszcze trzeci, nieformalny sposób potwierdzania tożsamości, zwany *one-to-few matching* (1:F). Jest on stosowany w małych grupach społecznych (np. rodzinach), liczących od 5 do 20 osób i przeważnie służy do uzyskania dostępu do archiwów lub mieszkań[24].

Pojawienie się na dużą skalę rozwiązań biometrycznych miało miejsce na początku lat 90. W Stanach Zjednoczonych FBI zbudowało system IAFIS (*Integrated Automated Fingerprint Identification System),* który jest obecnie największą na świecie bazą zawierającą biometryki 47 mln osób. Składa się on z danych dotyczących odcisków palców oraz obrazów twarzy wraz z przyporządkowanymi informacjami na temat ich posiadaczy, zbieranych z kryminalnych lub pozakryminalnych źródeł[25]. Obecnie FBI pracuje nad nowym systemem zwanym Next Generation Identification realizowanym przez Lockheed Martin, który ma zastąpić IAFIS[26]. W 2004 roku Wenezuela wprowadziła pobieranie odcisków palców od wyborców, aby zapobiegać podwójnemu głosowaniu[27]. W Stanach Zjednoczonych, Wielkiej Brytanii, Belgii, Szwecji czy Francji skanery odcisków są używane w celu bezgotówkowego płacenia za szkolne obiady dla dzieci oraz umożliwienia rodzicom i władzom placówki monitoringu obecności, mobilności i odżywiania ich pociech, co wywołuje wiele kontrowersji natury prawnej[28].

Technikę ustalania tożsamości na podstawie obrazu twarzy można spotkać na międzynarodowym lotnisku we Frankfurcie nad Menem czy w portach lotniczych w Australii, gdzie działa system SmartGate, identyfikujący przyjezdnych za pomocą porównania ich zdjęć robionych na granicy z obrazem twarzy zawartym

---

[23] *Ibidem*., s. 8.

[24] L. O'Gorman, *Fingerprint verification*, [w:] A. Jain, R. Bolle, S. Pankanti (red.), *Biometrics: Personal…,* s. 45.

[25] *Integrated Automated Fingerprint Identification System or IAFIS*, strona internetowa Federalnego Biura Śledczego, http://www.fbi.gov/hq/cjisd/iafis.htm. Dane są zbierane przez stanowe i lokalne agencje FBI, pochodzą one zarówno od osób aresztowanych, przestępców czy z prowadzonych śledztw, jak i z cywilnych źródeł: programu US-VISIT, danych finansowych, pracowniczych oraz danych prywatnych czy publicznych.

[26] E. Nakashima, *FBI Prepares Vast Database Of Biometrics*, „The Washington Post", 22 grudnia 2007 r., http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html?hpid=topnews.

[27] Dotychczas przeprowadzono 11 wyborów z identyfikacją odcisków, w bazie danych znajduje się prawie 17 milionów wyborców.

[28] W. Grossman, *Is School Fingerprinting Out of Bounds*, „The Guardian", 30 marca 2006 r., http://www.guardian.co.uk/technology/2006/mar/30/schools.guardianweeklytechnologysection.

w mikroczipie e-paszportu czy wizy[29]. Technika ta jest także wykorzystywana przez brytyjską policję w związku ze zniknięciem 3 maja 2007 roku Madeleine McCann i opiera się na wykorzystaniu zebranych zdjęć twarzy osób, które tego dnia przebywały w pobliżu klubu Ocean Club w Praia de Luz – miejscu porwania – w celu ich rozpoznania[30]. Natomiast w czasie meczu o Super Bowl w Tampa Bay w 2001 roku po raz pierwszy zastosowano ten system identyfikacji na imprezie sportowej, w celu wytropienia przez policyjne kamery osób podejrzanych o terroryzm czy byłych przestępców znajdujących się na widowni[31].

Czytniki tęczówki stosuje się przede wszystkim na przejściach granicznych, m.in. w ramach programów imigracyjnych CANPASS Air[32] i NEXUS[33]. Również w Wielkiej Brytanii i Zjednoczonych Emiratach Arabskich funkcjonuje taki system analizy dla obcokrajowców wkraczających do tych krajów[34]. Pakistan natomiast wprowadził tę biometrykę dla afgańskich uchodźców wspieranych finansowo przez UNHCR w celu uniknięcia oszustwa podwójnej pomocy dla jednej osoby[35]. Jednym z najbardziej znanych w historii przykładów zastosowania tej biometryki była identyfikacja afgańskiej dziewczynki (Sharbat Gula) o niezwykłych oczach, która znalazła się na okładce „National Geographic" z 1985 roku, co zajęło prawie 17 lat[36].

---

[29] SmartGate, strona systemu, Australian Government. Custom and Border Protection Service, http://www.customs.gov.au/site/page.cfm?u=5552.

[30] D. Brown, S. Bird, *We will travel anywhere to find Madeleine, say parents,* „The Times", 23 maja 2007 r., http://www.timesonline.co.uk/tol/news/world/europe/article1826735.ece.

[31] K. Smith, *Face Recognition*, National Science and Technology Council (NIST), http://www.biometrics.gov/Documents/FaceRec.pdf.

[32] CANPASS Canada Border Services Agency, http://www.cbsa-asfc.gc.ca/canpass/. Jest to kanadyjski program pozwalający na szybkie przekraczanie granicy tego państwa przez rezydentów Kanady i USA przy użyciu specjalnych kart i ich tęczówki oka. CANPASS to zbiór mniejszych programów wyspecjalizowanych nie tylko pod kątem przelotów, ale również imigracji wodnymi środkami transportu.

[33] NEXUS Canada Border Services Agency, http://www.cbsa-asfc.gc.ca/prog/nexus/. NEXUS jest wspólnym projektem amerykańsko-kanadyjskim. Umożliwia on szybkie przemieszczanie się między Stanami Zjednoczonymi i Kanadą dzięki specjalnym kioskom wyposażonym w weryfikatory tęczówek. Z NEXUSA mogą korzystać jedynie obywatele lub stali rezydenci tych państw, którzy mieszkają na ich terenie co najmniej trzy lata.

[34] W Wielkiej Brytanii jest Iris *Recognition Immigration System* (IRIS), który funkcjonuje na lotniskach Heathrow, Manchester, Birmingham i Gatwick.

[35] *UNHCR passes 200,000 mark in returnee iris testing,* United Nations High Commissioner For Refugees In Pakistan, 10 listopada 2003 r., http://www.un.org.pk/unhcr/press/Oct_10_03.htm.

[36] M. Ścibior, op. cit., *How the Afghan Girl was Identified by Her Iris Patterns,* http://www.cl.cam.ac.uk/~jgd1000/afghan.html.

Biometrykę geometrii dłoni najpowszechniej zastosowano w INSPASS (*INS Passenger Accelerated Service System),* pierwszym na olbrzymią skalę programie migracyjnym posługującym się biometrią. Projekt ten wprowadzono w 1993 roku na lotniskach JFK i Newark, potem rozszerzono go na inne, w tym kanadyjskie w Toronto. W INSPASS obywatele USA lub państw „zaufanych", wjeżdżając do tego kraju, byli identyfikowani na podstawie porównywania ich geometryk dłoni z poprzednio zebranymi w bazie danych. Podróżni nie musieli przechodzić przez sformalizowany wywiad służb granicznych, lecz udawali się do specjalnego kiosku inspekcji federalnej[37]. INSPASS zakończono w 2003 roku zastępując go USPASS[38]. Czytniki dłoni są również stosowane w szkołach, m.in. od 1999 roku w dostępie do kantyn w katolickiej szkole Institution Immaculee Conception w Angers[39] oraz od 2002 r. w liceum Joliot-Curie w Var k. Angers, gdzie służą podglądaniu czynności i obecności uczniów[40]. Natomiast w czasie igrzysk olimpijskich w Atlancie w 1996 roku systemy oparte na tej biometryce zapewniały kontrolę i dostęp do wioski olimpijskiej[41].

Biometryki wdraża się również w sektorze prywatnym. Walt Disney World, park zabaw położony na Florydzie, stosuje system BioMet Partners', polegający na pobieraniu od odwiedzających dwóch odcisków palców w celu uzyskania pewności, że wydany danej osobie bilet będzie używany tylko przez nią[42]. W Japonii banki takie jak Sumitomo Mitsui, Japan Post Bank czy Mizuho wprowadziły opracowaną przez Hitachi technologię weryfikacji odcisków palców w swoich bankomatach i telerach[43].

---

[37] *Immigration and Naturalization Service Passenger Accelerated Service System Pilot Program*, Audit Report 95-8 (3/95), http://www.usdoj.gov/oig/reports/INS/a9508/index.htm.

[38] U.S. Passenger Accelerated Service System (USPASS), Portal GlobalSecurity.org, http://www.globalsecurity.org/security/systems/inspass.htm.

[39] T. Dupont, *Quand la biometrie s'installe dans les cantines au nez et a la barbe de la CNIL*, portal ZDNet.fr, 9 września 2003 r., http://www.zdnet.fr/actualites/informatique/0,39040745,39122509,00.htm.

[40] *Principal du collège Joliot-Curie de Carqueiranne (Var) – biométrie,* Big Brother Awards – France, 2005, http://bigbrotherawards.eu.org/Principal-du-college-Joliot-Curie.html. Szkoła ta wygrała w 2005 r. nagrodę Big Brother Award, która jest przyznawana dla podmiotów, które przyczyniają się do likwidowania prywatności ludzkiej. Patrz: *Palmares 2005*, 4 lutego 2006 r., http://bigbrotherawards.eu.org/Palmares-2005.html.

[41] K. Smith, *Hand geometry*, National Science and Technology Council (NSTC), http://www.biometrics.gov/Documents/HandGeometry.pdf.

[42] J. Woodward, N. Orlans, P. Higgins, op. cit., s. 67–68.

[43] K. Hall, *Biometrics: Vein Scanners Show Promise*, „The Business Week", 6 lutego 2007 r., http://www.businessweek.com/globalbiz/content/feb2007/gb20070206_099354.htm. Aby pobrać pieniądze, należy włożyć kartę bankową z czipem zawierającym odcisk palca,

2. Rozwiązania biometryczne w Unii Europejskiej

Problematyka biometrii po raz pierwszy pojawiała się w Unii Europejskiej na sympozjach z udziałem Komisji Europejskiej organizowanych przez prezydencję Luksemburga w grudniu 1997 roku w Brunnen oraz prezydencję Niemiec w czerwcu 1999 roku w Norymberdze[44]. Głównym tematem rozmów była biometryzacja i elektronizacja dokumentów unijnych, przede wszystkim podróży. Debata ta przeniosła się ze sfery eksperckiej do politycznej, efektem czego był komunikat Rady Europejskiej z czerwca 2003 roku obradującej w Salonikach. Stwierdzał on, że „Unii Europejskiej potrzebne jest spójne podejście do identyfikacji biometrycznej lub danych biometrycznych, które mogłyby stanowić zharmonizowane rozwiązania dla dokumentów wydawanych obywatelom państw trzecich, paszportom unijnym i systemom informacyjnym (VIS I SIS II). Rada Europejska wzywa Komisję do przygotowania odpowiednich propozycji (…)"[45].

Na przyspieszenie biometryzacji obszarów unijnych istotny wpływ miały trzy czynniki. Po pierwsze, zamach z 11 września 2001 roku zbudował nowy konstrukt społeczny o charakterze globalnym, który opisywał świat jako niebezpieczny. Aby obniżyć ten poziom, państwa zaczęły wprowadzać środki ochrony przepływu osób ponad granicami, jak również ograniczać prawa i wolności swoich obywateli w celu zapewnienia bezpieczeństwa. Podstawowym narzędziem takiej polityki okazała się biometria, która uzyskała opinię skutecznej metody weryfikacji i identyfikacji tożsamości osób pozwalającej tym samym wytropić podejrzanych lub przyszłych terrorystów. Powyższy problem dotknął także Europę, kiedy miały miejsce zamachy w Madrycie w 2004 roku i w Londynie w 2005 roku. Okazało się, że rozpoznani zamachowcy byli obywatelami UE, a nawet urodzili się na terenie państw zaatakowanych. Zjawisko to wymagało podjęcia wewnętrznych środków ochrony i kontroli społecznej, z których biometria obrazowała się jako najlepsza.

Po drugie, pojawiło się silne lobby ze strony Stanów Zjednoczonych oraz ICAO (Międzynarodowej Organizacji Lotnictwa Cywilnego) zachęcające Unię Europejską do wprowadzenia biometrii. W 2002 roku Kongres USA uchwalił

---

a następnie położyć ten sam palec na sensorze bankomatowym. System weryfikuje zgodność obu biometryk po zaledwie 0,5 sekundy, po czym umożliwia dostęp do wypłaty.

[44] F. Jasiński, *Zagadnienia biometrii w Unii Europejskiej*, „Materiały Robocze Centrum Europejskiego Natolin", 2006, nr 4, s. 18–19.

[45] *Thessaloniki European Council 19 and 20 June 2003: Presidency Conclusions*, Council of The European Union, 11638/03, 1 października 2003 r., http://register.consilium.europa.eu/pdf/en/03/st11/st11638 en03.pdf, s. 3.

Enhanced Border Security and Visa Entry Reform Act, na mocy którego wprowadzono system US-VISIT (*United States Visitor and Immigrant Status Indicator Technology*), nakazujący pobranie na przejściu granicznym wszystkim obcokrajowcom wkraczającym do Stanów Zjednoczonych na podstawie uzyskanej wizy 10 lub 2 odcisków palców oraz cyfrowego zdjęcia ich twarzy[46]. Główną celem takiego przepisu była próba zapobiegania migracji do Ameryki terrorystów, którzy wykorzystując wady tradycyjnych dokumentów, mogliby podszywać się pod tożsamość innych jednostek[47]. Obowiązek składania biometryk został również określony dla obywateli państw objętych ruchem bezwizowym ze Stanami Zjednoczonymi[48]. Waszyngton zażądał, aby od 26 października 2004 roku identyfikatory biometryczne znalazły się w paszportach unijnych tych osób[49]. Postulat ten istotnie wpłynął na przyspieszenie przez instytucje UE prac biometryzacyjnych, przy czym w odniesieniu do paszportów odbywały się one bezkrytycznie i były pozbawione dyskusji publicznej. ICAO natomiast wypracowała i przyjęła 28 maja 2003 roku globalny standard identyfikacji biometrycznej w paszportach oraz innych dokumentach podróży odczytywanych maszynowo (*machine-readable* – MR), postulując jego implementację we wszystkich państwach[50]. W pracach ICAO brała udział Komisja Europejska, która zobowiązała się do wdrożenia powyższego projektu do dokumentów Unii Europejskiej.

---

[46] Strona internetowa programu US-VISIT, Departament Bezpieczeństwa Wewnętrznego, http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm. Podobny system weryfikacji i identyfikacji biometrycznej cudzoziemców wprowadziła 30 listopada 2007 r. Japonia – zwany J-VIS. Polega on na pobraniu na przejściu granicznym dwóch odcisków palców oraz obrazu twarzy obcokrajowców wkraczających do tego kraju. System wywołuje sprzeciw społeczny ze względu na wkraczanie w prywatność i łamanie praw człowieka. Patrz: *New entry procedure will start*, http://www.immi-moj.go.jp/keiziban/happyou/pdf/poster-english.pdf; *Fingerprinting: Amnesty/SMJ Appeal for Noon Nov 20 Public Appeal outside Justice Ministry*, 9 listopada 2007 r., portal debito.org, http://www.debito.org/?p=708. Od stycznia 2004 r. podobny system funkcjonuje także w Brazylii, a od 2010 r. zamierza go wprowadzić Korea Południowa.

[47] P. Zbysiński, *Z sercem i anteną*, „Polityka", 21 sierpnia 2006 r.

[48] Chodzi o *Visa Waiver Programme* (*VWP*).

[49] F. Jasiński, *op. cit.*, s. 31. UE nie zdążyła zrealizować tego postulatu w terminie, dlatego został on przedłużony do 26 października 2006 r.

[50] 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. Patrz: *ICAO MRTD Report*, 2006, vol. 1, nr 1, http://www2.icao.int/en/MRTD/Downloads/ ICAO%20MRTD%20Report/ ICAO% 20 MRTD%20Report%20Vol.%201%20No.%201,%202006.pdf.

Po trzecie, biometria zaczęła szybko wkraczać do prywatnego sektora gospodarki. Coraz więcej firm wprowadzało identyfikatory, e-czipy, dokumenty umożliwiające dostęp do baz danych za pomocą biometryk[51]. Internetyzacja umów, pojawienie się elektronicznych form oświadczeń woli oraz kompresja czasowo-przestrzenna[52] wywoływały także silną presję na dostosowanie się administracji publicznej do tych globalnych warunków. W konsekwencji pojawiła się potrzeba prawnej regulacji procesu biometryzacji i elektronizacji życia społecznego, jak i zbudowania odpowiedniej e-administracji opartej na cyfrowej infrastrukturze.

2.1. Biometria w paszportach unijnych

Biometryczne paszporty jako pierwsze pojawiły się w 1998 roku w Malezji, ale ich popularność wzrosła zaraz po zamachach z 11 września 2001 roku[53]. Jeszcze w tym roku Departament Stanu Stanów Zjednoczonych rozpoczął wydawanie paszportów odczytywanych maszynowo (MRP – *Machine Readable Passports*) zawierających cyfrową biometrykę twarzy[54]. Natomiast w 2006 roku powszechnie wprowadzono standardowe e-paszporty wyposażone w 64-bitowy,

[51] M. Ścibior, *Na rękę i na oko*, *op. cit*. Biometryzacje sektora prywatnego widać także w Polsce. ING Bank Śląski stosuje kontrolę dostępu do ważnych pomieszczeń, wykorzystując system rozpoznawania geometrii dłoni, a w centrali Eurobanku zainstalowano kamery identyfikujące pracowników na podstawie wzoru tęczówki oka.

[52] O. R. Young, *Interdependence In World Politics*, "International Journal", 1969, vol. 24, s. 740–750; R. Robertson, *Globalization. Social Theory and Global Culture*, London 1992, s. 8. Kompresja czaso-przestrzenna oznacza ścieśnianie się czasu i przestrzeni, co obrazuje się gwałtownym przyspieszeniem działań społecznych oraz przepływu informacji o nich do najdalszych obszarów świata. Kompresja powoduje deterytorializację procesów i obiektów, które poruszają się w wirtualnym świecie bez swojego terytorialnego odpowiednika, przyczyny. W kontekście administracji zjawisko to naciska na organy publiczne, aby ich decydenci wykonywali swoje obowiązki coraz szybciej, a odbiorcy mogli bez kolejki i wirtualnie otrzymywać efekty działań administracyjnych.

[53] Strona internetowa Immigration Department of Malaysia, http://www.imi.gov.my/eng/perkhidmatan/im_Kenyataan.asp. Malezyjski paszport został zaprojektowany przez korporację IRIS. W jego mikroczipie zawarte są biometryki twarzy oraz odciski dwóch kciuków oraz informacje o tożsamości właściciela dokumentu. Ponadto, paszport posiada dane o historii podróży właściciela dotyczącej ostatnich dziesięciu wyjazdów i wjazdów do Malezji. Malezyjski paszport nie spełnia jednak standardów międzynarodowych Paszportu, a państwo to nie jest członkiem amerykańskiego *Visa Waiver Programme*.

[54] Stany Zjednoczone już w 1981 r., jako pierwsze państwo na świecie, wprowadziły paszporty odczytywane maszynowo, jednak pozbawione czipa z danymi. Informacje były odczytywane z kodu kreskowego, podobnego do kodu zawartego na odwrocie polskich plastykowych dowodów osobistych.

elektroniczny czip ze zdjęciem, danymi dokumentu oraz informacjami na temat jego posiadacza[55].

W listopadzie 2003 roku ICAO opublikowała pierwsze paszporty biometryczne. Uznano, że podstawową biometryką zawartą w ich mikroczipach będzie obraz twarzy, natomiast zapis tęczówki oka i odcisków palców uzyskały charakter fakultatywny. Komisja Europejska zaakceptowała pomysł i w lutym 2004 roku przedstawiła projekt legislacyjny nowego standardu dokumentów paszportowych.

Po debacie nad projektem, Rada Wspólnot Europejskich uchwaliła Rozporządzenie (WE) nr 2252/2004 z dnia 13 grudnia 2004 roku w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie[56]. Dokument posiada moc obowiązującą w stosunku do wszystkich stron *acquis* Schengen, a więc bez Danii, Wielkiej Brytanii i Irlandii oraz wobec pozaunijnych członków Europejskiego Obszaru Gospodarczego, czyli Islandii, Norwegii i Szwajcarii. Ostatecznie Dania notyfikowała przystąpienie do regulacji e-paszportów, natomiast Wielka Brytania i Irlandia wprowadziły własne paszporty biometryczne, które nie są ograniczone specyfikacjami unijnymi[57].

Na podstawie rozporządzenia państwa zostały zobligowane do wprowadzenia do paszportów i innych dokumentów podróży środka pamięci (*storage medium*) zawierającego dwa poziomy zabezpieczeń. Pierwszy to zapis obrazu twarzy, który powinien być wprowadzony do paszportów na 18 miesięcy od daty przyjęcia specyfikacji technicznych, czyli do 28 sierpnia 2006 roku. Drugi poziom to biometryka odcisków palca wskazującego lewej i prawej dłoni, a okres jego implementacji miał trwać do 36 miesięcy od wydania specyfikacji, czyli do 28 czerwca 2009 roku. Różnice terminów wynikają z odmiennych metod dostępu do tych zabezpieczeń. Obraz twarzy będzie polegał na tzw. podstawowej kontroli dostępu (BAC-Basic Acces Control), czyli maszynowym odczycie danych w czipie, niewymagającym skomplikowanego sprzętu czy dostosowań[58]. Natomiast odciski palców będą sprawdzana rozszerzoną kontrolą

[55] Od sierpnia 2007 r. Departament Stanu wydaje swoim obywatelom wyłącznie paszporty biometryczne, przy czym stare dokumenty będą w obrocie aż do ich okresowego wygaśnięcia ważności.

[56] Dz. Urz. UE, L 385/1, 29 grudnia 2004 r.

[57] Na przykład paszport brytyjski nie zawiera zapisu odcisków palców, a wyłącznie cyfrowy obraz twarzy właściciela.

[58] Więcej: A. Juels, D. Molnar, D. Wagner, *Security and Privacy Issues in E-passports*, marzec 2006, http://eprint.iacr.org/2005/095.pdf, s. 8 i nast.

dostępu (EAC – Extended Access Control)[59] opartej na specjalnym systemie szyfrującym zwanym Infrastrukturą Klucza Publicznego (PKI), co wymaga czasochłonnego wdrożenia oprogramowania oraz sprzętu na wszystkich punktach granicznych UE.

2.1.1. Polski paszport biometryczny

System prawny Polski dostosowuje się do wymogów identyfikacji biometrycznej stawianych przez unijne *acquis*. 28 sierpnia 2006 roku weszła w życie *Ustawa o dokumentach paszportowych*, która wprowadza nowe paszporty, wyposażone w 32-kilobajtowy czip zawierający biometryki posiadaczy[60].

Polski e-paszport, liczący 40 stron, ma bordową okładkę z napisem w języku polskim „Unia Europejska" i „Rzeczpospolita Polska". Na środku umieszczone jest godło RP, a poniżej napis „paszport" w języku polskim, angielskim i francuskim[61]. Czip biometryczny znajduje się wewnątrz strony ze zdjęciem i danymi właściciela dokumentu. Składa się on z tzw. tagu oraz anteny umieszczonej wzdłuż krawędzi strony. W tagu zapisane są informacje takie jak: cyfrowe zdjęcie twarzy, dane osobiste, termin ważności oraz dane potwierdzające wydanie paszportu przez uprawniony organ, natomiast antena służy do radiowego połączenia z czytnikiem[62]. Kluczowe znaczenie odgrywa jednak biometryczny obraz twarzy właściciela, który umożliwia strażnikowi weryfikację poprzez porównanie jej z tradycyjnie zrobionym zdjęciem na przejściu granicznym. Koszt wyrobienia takiego dokumentu w urzędzie wojewódzkim wynosi 140 zł, a okres oczeki-

---

[59] Patrz: *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC),* Bundesamt für Sicherheit in der Informationstechnik 2008, http://www.bsi.de/literat/tr/tr03110/TR-03110_v111.pdf.

[60] Dz. U. 2006 Nr 143, poz. 1027. Zgodnie z ustawą paszporty zastąpią tradycyjne dokumenty 1 stycznia 2011 r.

[61] Wzór dokumentu znajduje się w formie załącznika w rozporządzeniu ministra spraw wewnętrznych i administracji. Patrz: *Rozporządzenie 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. 2006, Nr 152, poz.1090.

[62] Polski paszport jest oparty na technologii RFID (*Radio Freguency Identification*), stosowanej min. w kartach bankomatowych czy w sklepach w celu identyfikacji towarów. Jej działanie polega na tym, że czytnik za pomocą fal radiowych wytwarza pole elektromagnetyczne na antenie , zasilając *tag*, który emituje odpowiedź dekodowaną przez czytnik. Patrz: L. B. Ayre, *RFID and Libraries*, http://www.galecia.com/included/docs/position_rfid_permission.pdf; *Radio Frequency Identification,* ITAA, czerwiec 2004 r., http://www.itaa.org/rfid/docs/rfid.pdf.

wania to cztery tygodnie[63]. Wprowadzono jednak rozbudowany system ulg i zwolnień[64].

Do końca roku 2008 wydano 2,5 mln biometrycznych paszportów, co uważa się za liczbę małą. Główną przyczyną niskiego popytu jest cena[65]. Należy tutaj podkreślić, że w przypadku utraty lub zniszczenia dokumentu z własnej, choćby nieumyślnej winy osoba musi zapłacić za wydanie nowego paszportu aż o 200% więcej, czyli 420 zł. Porównując jednak koszty wydawania w innych państwach członkowskich, Polska wprowadziła jedne z najniższych opłat w całej UE[66]. Być może czynnikiem, który zwiększy popyt na biopaszporty okażą się dodatkowe przywileje związane z ich posiadaniem. Na przykład od 1 stycznia 2009 roku Kanada zniosła obowiązek wizowy wyłącznie dla obywateli RP, którzy legitymują się takim dokumentem[67].

2.2. Dokumenty tożsamości w UE

Biometria dotarła także do dokumentów tożsamości, czego przykładem są obecne debaty nad jej umieszczeniem w prawach jazdy i dowodach osobistych. Jednak dyskusja ta trafia na problem kompetencji, albowiem zgodnie z interpretacją art. 18 TWE, przepisy odnoszące się do paszportów, dowodów tożsamości, dokumentów pobytowych oraz jakichkolwiek innych podobnych dokumentów mogą być jedynie przyjmowane w odniesieniu do bezpieczeństwa tych dokumentów i przekraczania granic zewnętrznych UE[68]. O ile zatem można było przyjąć przepisy o zabezpieczeniach w transgranicznych paszportach, o tyle jest to prawnie niemożliwe w przypadku krajowych dowodów.

Mimo problemów legislacyjnych, państwa członkowskie podjęły próby harmonizacji i biometryzacji dowodów tożsamości. W dokumencie prezydencji z 11 lipca 2005 roku przekazano mandat Komitetowi Art. 6, aby do marca 2006

---

[63] *Rozporządzenie Rady Ministrów z dnia 25 sierpnia 2006 r. w sprawie opłat za wydanie dokumentu paszportowego oraz ich zwrotu*, Dz. U. 2006, Nr 153, poz. 1091.

[64] *Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych*, Dz. U. 2006 Nr 143, poz. 1027 z późn. zm., Art. 7–11.

[65] *Ibidem*., art. 10.3.

[66] W przeliczeniu na złotówki, wyższe opłaty są m.in. w Szwecji (348,40 zł), Belgii (668,95 zł), Norwegii (511, 53 zł), Wielkiej Brytanii (301,10 zł) czy Francji (241,79 zł). Więcej na stronie internetowej Ministerstwa Spraw Wewnętrznych i Administracji, http://www.mswia.gov.pl/ index.php?dzial=298&id=3998.

[67] *Od stycznia 2009 r. do Kanady bez wizy tylko z paszportem biometrycznym*, „Wprost24", 31 grudnia 2008, http://www.wprost.pl/ar/148835/Od-stycznia-2009-r-do-Kanady-bez-wizy-tylko-z-paszportem-biometrycznym.

[68] F. Jasiński, op. cit., s. 57.

roku przygotował wspólne standardy bezpieczeństwa dowodów osobistych, wzorując się na doświadczeniach paszportu biometrycznego i ICAO[69]. 18 listopada 2005 roku reprezentanci rządów państw członkowskich przedstawili swoje konkluzje ze spotkania, w których zaproponowali wprowadzenie do dowodów osobistych biometryk obrazu twarzy i dwóch płaskich odcisków palca, które razem mieściłyby się w mikroczipie wykorzystującym kanały radiowe (RFID)[70]. Jednak mimo prac nie udało się rozwiązać problemu art. 18 TWE.

Fiasko ustalania wspólnych standardów dokumentów tożsamości spowodowało, że państwa członkowskie podjęły samodzielne działania w celu biometryzacji krajowych dowodów osobistych, zgodnie z wezwaniem instytucji UE. Na początku 2000 roku Finlandia jako pierwszy kraj w UE wprowadziła nowe biometryczne dokumenty tożsamości wyposażone w czip zawierający dane personalne oraz podpis elektroniczny. Nie jest to jednak dowód biometryczny (bioID), lecz elektroniczny (eID), ponieważ nie zawiera biometryk posiadacza. Dokument, obok potwierdzania tożsamości, umożliwia również korzystanie z e-usług administracyjnych czy transakcji bankowych[71]. Podobne e-dowody wprowadziły m.in: Austria, Szwecja, Włochy, Hiszpania, Portugalia i Belgia. W lipcu 2007 roku e-dowody zostały wprowadzone w Niemczech. Nowe dokumenty zawierają czip ze zdjęciem, fakultatywnym odciskiem palców oraz identyfikatorem elektronicznym tożsamości; e-dowód jest wielofunkcyjny, pozwala zawierać transakcje handlowe, bankowe, internetowe oraz ma funkcjonować jako karta pracy czy zdrowia[72]. Największe zastosowanie ma jednak estoński dokument tożsamości, który umożliwia elektroniczne korzystanie z prawie wszystkich usług bankowych, administracyjnych, transportowych[73]. Estonia jest pierwszym krajem, który w 2007 roku wprowadził głosowanie w wyborach przez Internet i właśnie eID stanowi weryfikator ważności głosu[74]. Większe państwa członkowskie także starają się wprowadzić e-dowody. We Francji Nicolas Sarkozy jako minister

---

[69] *Minimum common standards for national identity cards*, Council of The European Union, 11092/05.

[70] *Draft Conclusions of the Representatives of the Governments of the Member States on common minimum security standards for Member States' national identity cards,* Council of The European Union, 14622/05.

[71] R. Nitschke, *National ID Card. Electronic ID card becomes reality in Europe*, http://www.novosec.com/documents/eCommerce_NationalIDcard_020930.pdf.

[72] R. Susło, *Niemcy wprowadzają wszystko mające dowody*, Portal money.pl, 23 lipca 2007 r., http://news.money.pl/artykul/niemcy;wprowadza;wszystkomajace;e-dowody,234,0,357098.html.

[73] Patrz: strona internetowa eID, http://www.id.ee/.

[74] *Elections and E-voting*, http://www.valimised.ee/teema_eng.html.

spraw wewnętrznych chciał wprowadzić w 2005 roku obowiązkowe biometryczne dowody osobiste, jednak za sprawą społecznego oporu projekt został porzucony i przekazany do udoskonalenia[75]. Natomiast w Wielkiej Brytanii, na mocy National Cards Act z 2006 roku uchwalono implementację biometrycznych dowodów osobistych z odciskami palców i ewentualnie obrazem tęczówki, które będą powszechnie wydawane w 2011–2012 roku[76].

2.2.1. Polski biometryczny (elektroniczny) dowód osobisty

Wraz z trendem światowym również w Polsce pojawił się pomysł wprowadzenia biometrycznych lub elektronicznych dowodów osobistych. W czasie wykładu na Politechnice Warszawskiej, który odbył się 16 stycznia 2007 roku, wiceminister MSWiA Piotr Piętak zapowiedział wprowadzenie takich dokumentów jeszcze w 2008 roku, co się jednak nie udało[77]. Ostatecznie ustalono, że nowa reforma będzie opierała się na dwóch projektach: PESEL II oraz pl.ID. Pierwszy rozpoczęto w czerwcu 2005 roku, a jego założenia zostały zawarte w dokumencie MSWiA zatytułowanym „Podstawowy Dokument Programu PESEL2. Przebudowa i integracja systemów państwowych. Sposób budowy systemu"[78]. Priorytetem projektu jest zbudowanie zintegrowanego systemu informacyjnego, który będzie służył lepszej obsłudze obywatela i przedsiębiorcy poprzez umożliwienie im dostępu do zasobów informacyjnych rejestru PESEL[79]

---

[75] Projekt ten, zwany INES – Identité Nationale Electronique Sécurisée, został po raz pierwszy zaproponowany w 2001 r. przez premiera Jeana-Pierre'a Raffarina.

[76] *Identity Cards Act 2006*, Office of Public Sector Information, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060015_en_1#sch1; *ID card scheme cost put at £5.4bn*, BBC News, 9 listopada 2006 r., http://news.bbc.co.uk/2/hi/uk_news/politics/6033687.stm; strona internetowa projektu, http://www.ips.gov.uk/identity/press-2008-09-25.asp.

[77] *Wykład wiceministra Piotra Piętaka pt. „Dlaczego Polska wprowadza elektroniczny dowód osobisty w 2008 r.*", MSWiA, http://www2.mswia.gov.pl/portal/pl/2/4382/.

[78] *PESEL2. Stan realizacji projektu*, Komisja Administracji i Spraw Wewnętrznych Sejmu Rzeczpospolitej Polskiej Warszawa, 11 czerwca 2008 r., http://www.cpi.mswia.gov.pl/portal/cpi/37/144/PESEL2.html. Projekt MSWiA wygrał konkurs zorganizowany przez Ministerstwo Nauki i Informatyzacji ogłoszony w 2005 r. w ramach działania 1.5 Programu SPO WKP. Proces jego wdrożenia rozpoczęto w sierpniu 2006 r.

[79] PESEL (Powszechny Elektroniczny System Ewidencji Ludności) prowadzony jest od 1979 roku i zawiera dane osób przebywających stale na terytorium RP, zameldowanych na pobyt stały lub czasowy trwający ponad 3 miesiące, osób ubiegających się o wydanie dowodu osobistego lub paszportu, a także osób, dla których odrębne przepisy przewidują potrzebę posiadania numeru PESEL. System ten zawiera następujące dane: nazwiska, imiona, data urodzenia, imiona i nazwiska rodowe rodziców, płeć, obywatelstwo, stan cywilny, imię i nazwisko małżonka, adres zameldowania, seria i numer aktualnego i poprzednich dowodów osobistych,

przy jednoczesnej przebudowie istniejących baz państwowych. Nowa infrastruktura będzie zawierała te same dane co dotychczasowy PESEL, pomniejszony o takie informacje jak np. służba wojskowa[80]. Konstrukcja PESEL2 zakończyła się 30 września 2008 roku[81]. Natomiast pl.ID – polska karta ID – zakłada stworzenie wielofunkcyjnego, elektronicznego dowodu osobistego (dowodu biometrycznego) wyposażonego w mikroprocesor, zawierający podpis elektroniczny zgodny z unijnymi standardami potwierdzania tożsamości (eID). Dokument umożliwi posiadaczowi wirtualne poruszanie się i dostęp do systemów informacyjnych administracji, otrzymywanie e-usług publicznych i urzędowych oraz wirtualne załatwianie spraw administracyjnych[82]. Dowód nie będzie nośnikiem danych, lecz kluczem, za jego pomocą uzyska się dostęp do informacji zebranych w zintegrowanych systemach, w tym w PESEL2. Dostęp taki będzie możliwy w urzędzie lub przez Internet, a uprawnionymi do niego osobami będą urzędnik i właściciel dokumentu. Wprowadzenie biometrycznych dowodów osobistych jest przewidywane na 2010 roku w formie testowej, a od 2011 roku powszechnie[83].

W kontekście powyższych projektów pojawia się pytanie o udział w nich biometrii. W PESEL2 zrezygnowano z jej użycia, w dużej mierze za sprawą społecznej krytyki zbyt dalekiego wkraczania państwa w życie społeczne[84]. Porzucono również pomysł umieszczenia w tym systemie danych m.in. o wysokości zarobków i podatków, miejscu leczenia i jego powodów, ilości mandatów za złe parkowania, zalegania ze składkami ZUS, statusie rozliczeń z urzędem skarbowym, kontach bankowych czy statusie stosunków z policją, nie zakłada się także przetwarzania informacji o fakcie korzystania z pomocy opieki społecznej[85]. Natomiast

datę zgonu i numer aktu zgonu. Warto odnotować, że system ten wciąż opiera się na oprogramowaniu JANTAR z lat 70., który całkowicie zostanie zmieniony reformą PESEL2.

[80] *Informacja o stanie realizacji projektu PESEL2,* Sejmowa Komisja Administracji i Spraw Wewnętrznych, 11 czerwca 2008 r., http://www.cpi.mswia.gov.pl/portal/cpi/37/144/PESEL2.html.

[81] *Komunikat o zakończeniu realizacji Projektu PESEL2*, MSWiA, 17 listopada 2008 r., http://pesel2.mswia.gov.pl/portal/P2/1/175/Komunikat_o_zakonczeniu_realizacji_Projektu_PESEL2.html. PESEL2 miał być zrealizowany już w maju 2008 r. Ze względu na opóźnienia, w grudniu 2007 r. MSWiA opracowało plan naprawczy, który przyspieszył prace.

[82] Patrz: strona internetowa Centrum Projektów Informatycznych MSWiA, projekt pl.ID, http://www.cpi.mswia.gov.pl/portal/cpi/38/178/plID.html.

[83] *Od 2011 r. nowe chipowe dowody osobiste*, PAP-Nauka Polska, 24 grudnia 2008 r., http://www.naukawpolsce.pap.pl/palio/html.run?_Instance=cms_naukapl.pap.pl&_PageID=1&s=szablon.depesza&dz=szablon.depesza&dep=357930&data=&lang=&_CheckSum=-1215571988;

[84] A. Szozda, J. Stróżyk, *Widzą nas!,* „Wprost", 2006, nr 31.

[85] *Komunikat o zakończeniu projektu PESEL2*, op. cit., s. 2.

w przypadku pl.ID sprawa jest ciągle otwarta. W MSWiA wciąż jest popularny pomysł umieszczenia w nim fotografii twarzy, na co wskazuje także posługiwanie się w dokumentach wymiennie terminami elektroniczny i biometryczny dowód osobisty, choć pojęcia te nie są tożsame[86]. Ponadto, pojawił się postulat pozycjonowania w dokumentach tożsamości informacji o grupie krwi posiadacza, która w przypadku nagłych wypadków umożliwi szybką reakcję lekarską. Pomysłowi sprzeciwił się jednak minister zdrowia, stwierdzając, że grupa krwi może być umieszczona wyłącznie przez pracownika służby zdrowia, a nie organu gminy[87]. Do chwili obecnej MSWiA nie wymyśliło rozwiązania tej sytuacji, poza pomysłem stworzeniem dodatkowego dokumentu – karty identyfikacyjnej[88].

PESEL2 i pl.ID są fundamentalnymi projektami przyszłego elektronicznego (biometrycznego) dowodu osobistego. Mimo ustalenia pewnych ram czasowych na ich implementację, kolejne rządy nie rozpoczynają debaty społecznej na ich temat oraz nie są w stanie przedstawić ostatecznego ich kształtu. Jest to zjawisko smutne, tym bardziej, że instytucje eksperckie doszczętnie obnażają wady tych projektów[89].

---

[86] G. Osiecki, *Dowody osobiste dostaniemy za darmo*, „Dziennik", 4 września 2008 r., http://www.dziennik.pl/wydarzenia/article232236/Nowe_dowody_osobiste_dostaniemy_za_darmo.html; Elektroniczny dowód nie zawiera biometryk, a wyłącznie kody dostępu, dzięki którym uzyskuje się akces do baz danych. W przypadku biometrycznego dokumentu, znajdujące się na nim odciski palców lub fotografia stanowi obiekt weryfikacji i identyfikacji posiadacza, po których uzyskuje on dostęp. Pomysł implementacji biometryk potwierdził wiceszef MSWiA Witold Drożdż, stwierdzając, że „jeśli pojawią się istotne argumenty przemawiające za tym, by to zrobić, sprawa zostanie jeszcze rozważona". Patrz: *Od 2011 r. nowe chipowe dowody osobiste, op. cit*.

[87] A. Łukasiewicz, *Dowód i prawo jazdy z grupą krwi*, „Rzeczpospolita", 24 czerwca 2008 r., http://www.rp.pl/artykul/68861,152764_Dowod_i_prawo_jazdy_z_grupa_krwi.html.

[88] *Od 2001 r. nowe dowody osobiste,* op. cit. W latach 2008–2010 ponad 700 mln zł ma zostać przeznaczone na stworzenie Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych. Dzięki platformie ZOZ-y, apteki, praktyki lekarskie będą mogły gromadzić dane o zdarzeniach dotyczących naszego zdrowia. Administracja państwowa będzie też mogła analizować przepływy finansowe i statystyczne dotyczące ochrony zdrowia. Dzięki temu będzie można dokładniej planować działanie opieki zdrowotnej. Jeśli ktoś z takim kartą w ręku uda się do lekarza, dzięki niemu będzie on mógł otworzyć naszą elektroniczną kartę choroby.

[89] R. Kępczyński, K. Komorowski, P. Kociński, T. Chełkowski, *Czy PESEL2 jest potrzebny?,* „Raport Instytutu Sobieskiego", Nr 26, 2007 r., http://www.sobieski.org.pl//panel/plugins/newsy/files/Raport_IS_Kepczynski_Pesel2_2007_03.pdf.

3. Ocena zjawiska biometryzacji

Wyższość biometrii nad klasycznymi metodami identyfikacji jest tłumaczona tym, że o ile dowód, paszport, kartę kredytową czy nawet hasła PIN można zgubić lub zapomnieć, o tyle jest to niemożliwe w przypadku części własnego ciała lub zachowań behawioralnych. Teza ta trafia jednak na trzy kontrargumenty. Po pierwsze, choć biometryki praktycznie nie podlegają utracie, to istnieje łatwość ich podrobienia. Dowodem na to są pozytywne badania prof. Tsutomu Matsumoto z Uniwersytetu w Jokohamie[90] oraz „kradzież" i opublikowanie przez grupę hakerską CCC odcisków palców ministra spraw wewnętrznych Niemiec, Wolfganga Schauble w magazynie *Datenschleuder* w marcu 2008 roku[91]. Oparcie na biometrykach prawie wszystkich kluczowych czynności życia społecznego, takich jak operacje bankowe, załatwianie spraw administracyjnych czy przekraczanie granic powoduje, że zdobycie zaledwie jednego odcisku palca umożliwia złodziejowi dotarcie do wrażliwych sfer życia ofiary, generując dla niej potężne straty. Sytuacja ta nie jest tożsama dla klasycznych identyfikatorów, wyspecjalizowanych w dostępie do jednej czynności, których utrata nie pozwala na wkroczenie do wszystkich istotnych aspektów ludzkiej egzystencji.

Po drugie, „kradzież" danych biometrycznych jest bardziej niebezpieczna niż zdobycie konwencjonalnych środków rozpoznawania tożsamości, ponieważ jest nieświadoma dla ofiary. Człowiek może szybko spostrzec brak portfela czy karty kredytowej, co daje mu możliwość zablokowania dostępu do wrażliwych informacji (konta) w odpowiednim czasie. Natomiast w przypadku biometryk nie wie nawet, czy i kiedy je skopiowano, a informację o tym wydarzeniu uzyskuje *post fatum*, gdy już jest za późno.

---

[90] Badania wykazały, że, aby podrobić odciski palców, wystarczy uzyskać odcisk w miękkiej masie plastycznej, następie go zdjąć, zrobić formę, a potem odlew z nasyconego roztworu żelatyny spożywczej. Po stężeniu odlew doskonale imituje kształt palca z liniami papilarnymi. Inna metoda kopiowania polega na przeniesieniu odcisku pozostawionego na gładkiej powierzchni (szyba) na folię i papier, a następnie jego zeskanowanie. Za pomocą techniki wytwarzania pieczątek można wtedy stworzyć trójwymiarową formę odcisku palca i zastosować ją w identyfikatorach elektronicznych. Patrz: M. Karpiński, *Wytrych z palca*, „Wprost", Nr 24, 2002. Odpowiedzią na badania prof. Matsumoto jest pomysł wprowadzenia do czytników linii papilarnych technologii sprawdzania czy palec jest „żywy", co zaproponowała m.in. wrocławska firma Optel. Patrz: Strona internetowa firmy, http://www.optel.com.pl/.

[91] *CCC publishes fingerprints of Wolfgang Schäuble, the German Home Secretary*, portal heise online, 31 marca 2008 r., http://www.heise.de/english/newsticker/news/105728. CCC dołączyła ponadto do magazynu specjalny film nakładany na palec, który pozwala oszukać czytniki linii papilarnych albo wykorzystać ukradziony odcisk do uzyskania dostępu do danych. Patrz: *How To Fake Fingerprints*, CCC, http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml.

Po trzecie, utrata konwencjonalnych narzędzi identyfikujących nie ma charakteru bezwzględnego – ofiara może uzyskać nowe, wyposażone w inne kody szyfrujące dokumenty, anulując moc sprawczą tych zgubionych. W przypadku biometryk jest to niemożliwe, są one niezmienne przez całe życie człowieka. Nie można na przykład zmienić tęczówki oka czy odcisku palca. Oznacza to, że „kradzież" tych danych eliminuje całkowicie zdolność uczestnictwa poszkodowanych osób w systemach biometrycznych, a więc korzystania z wiz, paszportów, e-usług, e-bankomatów czy e-administracji. Taka sytuacja determinuje stworzenie dla okradzionych alternatywnej infrastruktury opartej albo na innych biometrykach, albo na środkach konwencjonalnych. Postulat ten nie jest jednak racjonalny dla korporacji, jego realizacja bowiem wykreuje dodatkowe koszty, utratę zysków z efektu skali oraz podwójne standardy. Wszystko zatem wskazuje, że skopiowanie biometryk może prowadzić nawet do śmierci cywilnej poszkodowanych osób.

Biometryzacja prowadzi do traktowania na równi ludzi i przedmioty dostępu, co określić można reifikacją człowieka. Obecnie jednostka posługuje się rzeczami w celu uzyskania akcesu do określonego świadczenia, ma zatem świadomość władzy nad nimi, jako zewnętrzny „poruszyciel" wprowadza je w ruch. Biometria powoduje, że jednostka staje się „kluczem", materialnym przedmiotem dostępu, którego ciało jest wykorzystywane do określonych czynności, co tworzy konstrukt utraty godności i zgubienia podmiotowości na rzecz uprzedmiotowienia w stosunkach społecznych. Ponadto, poprzez proces reifikacji człowieka przestępca będzie traktował potencjalną ofiarę nie jako jednostkę ludzką, ale jako „przedmiot dostępu" do celu. Taka racjonalizacja powoduje, że nie będzie miał oporów przed znacznym uszkodzeniem danej osoby (wydłubaniem oka, odcięciem palca itp.), będąc świadomy, że jest to jedyna droga zdobycia łupu. Na takie zjawisko wskazują przypadki odcinania palców właścicielom biometrycznych mercedesów S-Class w Malezji[92].

Systemy biometryczne opierają się na bazach danych, w których gromadzone są informacje o obywatelach. Dzięki użyciu czipa z biometryką lub samej biometryki jest ona weryfikowana z tą bazą i jeśli wynik okaże się pozytywny, umożliwia danej osobie dostęp. Problem polega na tym, że bazy te będą zamieszczone na serwerach, do których mogą włamać się hakerzy. A uczynią to z wielką motywacją, bowiem dotarcie do tak potężnej kopalni wiedzy o obywatelach przyniesie olbrzymie profity. O tym, że wycieki danych zainstalowanych na serwerach lub dyskach CD są powszechne, nie trzeba przekonywać. Posługując się przykładami, w listopadzie 2007 roku w Wielkiej Brytanii wyciekły z urzędu HM Revenue

[92] J. Kent, *Malaysia car thieves steal finger*, BBC News, 31 marca 2005 r., http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

and Customs dane 25 milionów obywateli zawierające numery kont bankowych oraz informacje o zasiłkach wychowawczych, a w grudniu 2008 roku prywatna firma współpracująca z rządem w zakresie przechowywania personaliów zagubiła dane osobowe kolejnych 3 mln osób[93]. W maju 2008 roku w Chile haker wykradł personalia 6 milionów obywateli zamieszczone na serwerach wojska i ministerstwa edukacji, po czym umieścił je na swoim blogu[94]. W Polsce podobny przypadek miał miejsce w Łodzi w marcu 2008 roku, kiedy na stronach internetowych Urzędu Miejskiego pojawiły się informacje petentów placówki wraz z imieniem i nazwiskiem, adresem zamieszkania, numerem PESEL i dowodu[95]. Dane te zostały szybko przechwycone przez hakerów i opublikowane na forach lub wykorzystane do phishingu[96]. Liczne przecieki informacji wpływają na świadomość Polaków, zaledwie 8% z nich ufa w bezpieczeństwo swoich danych przechowywanych w instytucjach państwowych[97].

Biometryzacja wywołuje wiele pytań natury prawnej. Przede wszystkim odnoszą się one do kwestii przymusowego pobierania odcisków palców jako jedynej drogi do uzyskania dostępu do usługi, co stanowi naruszenie wolności wyboru. Jednostka posiada prawnie zapewnioną wolność podejmowania własnych decyzji, dlatego powinna mieć możliwość odmowy okazania biometryki. Ponadto, istnieje obawa naruszenia prawa do prywatności. Udostępnienie biometryk władzom państwa powoduje, że jednostka, korzystając w jakimkolwiek miejscu z e-usług administracyjnych czy bankowych, będzie mogła być śledzona. Wystarczy, że wykona czynność za pomocą zawartego w dokumencie czipa z odciskiem palca, a zostanie szybko zidentyfikowana wraz z miejscem pobytu w danej chwili. Rozwój metod rozpoznawania twarzy spowoduje, że umieszczone w punktach publicznych kamery policyjne będą mogły z łatwością określić tożsamość każdej podpatrzonej osoby. Państwo i sektor prywatny są już na tyle odważni w swoich

[93] *Round-up: The HMRC data breach*, portal computerworld.uk, http://www.computerworlduk.com/management/government-law/public-sector/in-depth/index.cfm?articleid=953.

[94] M. Chudziński, *Dane 6 milionów Chilijczyków on-line*, „Dziennik Internautów", 13 maja 2008 r., http://di.com.pl/news/20823,1,0.html. Wśród wykradzionych danych były personalia jednej z dwóch córek prezydent Chile Michelle Bachelet.

[95] M. Masłowski, *Dane Łodzian wyciekły ze strony UMŁ*, „Gazeta Wyborcza", 31 marca 2008 r.

[96] Wiele przykładów kradzieży danych z serwerów jest zawartych w: *Why Biometrics and RFID are not a Panacea to Introduction to Biometrics,* http://www.cs.auckland.ac.nz/~pgut001/pubs/biometrics.pdf.

[97] *7 procent Polaków przyznaje, że padło ofiarą kradzieży tożsamości*, „Polityka.pl", 21 października 2008 r., http://www.polityka.pl/7-procent-polakow-przyznaje-ze-padlo-ofiara-kradziezy-tozsamosci/ Text01, 1009, 271490,16.

dążeniach do kontroli ludzi, że zobowiązują niektóre osoby do wszczepienia sobie czipa RFID. W Barcelonie klub Baja Beach umieszcza mikroskopijne tagi w ramieniu każdego ze swoich klientów, aby śledzić ich obecność, ograniczać anonimowość oraz umożliwić obrót bezgotówkowy w klubie[98]. Kuriozum jest decyzja US Food And Drug Administration (FDA) z 2004 roku umożliwiająca wszczepianie ludziom czipów pozwalających uzyskać im dostęp do swoich kart i historii chorobowych[99].

Wiele obaw dotyczy podmiotów uprawnionych do dostępu do personaliów zawartych w krajowych bazach danych. Posługując się jako przykładem polską *Ustawą o dokumentach paszportowych*, w art. 52 ust. 1, 2, 3 wymienia ona następujące podmioty: organ paszportowy, Komendant Główny Straży Granicznej, ABW, AW, CBA, 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. Biorąc pod uwagę wrażliwość biometryk oraz ich częstsze wykorzystywanie w sektorze prywatnym, pojawia się pytanie, czy przy tak dużej ilości organów uprawnionych do ich wglądu istnieje jeszcze jakakolwiek prywatność.

Pojawia się wątpliwość, czy regulacje unijne dotyczące biometryzacji są zgodne z art. 8 ust. 2 Konwencji Rady Europy o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 roku. W dniu 4 grudnia 2008 roku Europejski Trybunał Praw Człowieka w Strasburgu wydał w tej kwestii precedensowy wyrok, rozwiązując spór *S. i Marper przeciwko Wielkiej Brytanii*[100]. Teza orzeczenia stwierdza, że „Bezterminowe przechowywanie danych zawartych w profilach DNA, próbkach komórkowych oraz odciskach linii papilarnych osób, wobec których zakończono postępowanie karne bez skazania, stanowi naruszenie art. 8 Konwencji (prawo do ochrony życia prywatnego)". Można zatem *a fortiori* interpretować, że skoro naruszeniem prywatności jest bezterminowe posiadanie danych osoby uniewinnionej po postępowaniu karnym, to tym bardziej jest nim przechowywanie biometryk od osób, których postępowanie karne nie dotyczy, a więc wszystkich obywateli. Trybunał stwierdził zresztą inaczej niż poprzednie orzeczenia, że przechowywanie odcisków linii papilarnych i próbek biologicznych jest samo w sobie ingerencją w prawo do prywatności i może być uzasadnione

[98] *Barcelona clubbers get chipped*, BBC News, 29 września 2004 r., http://news.bbc.co.uk/2/hi/technology/3697940.stm.

[99] T. Greene, *Feds approve human RFID*, „The Register", 14 listopada 2004 r., http://www.theregister.co.uk/2004/10/14/human_rfid_implants/.

[100] *S. i Marper przeciwko Wielkiej Brytanii*, Europejski Trybunał Praw Człowieka, 4 grudnia 2008 r., 30562/04.

tylko „koniecznością w demokratycznym społeczeństwie". Wydaje się, że ten warunek nie jest spełniony w przypadku unijnych rozwiązań biometrycznych, ponieważ jest nieproporcjonalny do zagrożenia (dotyczy wszystkich osób, a nie podejrzanych), a interes prywatny ulega znacznemu uszczerbkowi na rzecz interesu publicznego, co nie jest „demokratyczne".

W kontekście powyższego wyroku należy stwierdzić, że również polskie ustawodawstwo biometryczne zawiera prawne kontrowersje. Stawia się pytanie, czy rozporządzenie o dokumentach paszportowych jest zgodne z Konstytucją[101]. Chodzi tu paragraf 4.2 nakazujący osobie, która chce załączyć do dokumentu zdjęcie z nakryciem głowy, przedstawienie zaświadczenia o przynależności do związku wyznaniowego. Przepis ten narusza art. 53 ust. 7 Konstytucji w brzmieniu: „Nikt nie może być obowiązany przez organy władzy publicznej do ujawnienia swojego światopoglądu, przekonań religijnych lub wyznania". Pojawia się również pytanie, czy tak ważne kwestie proceduralne dotyczące pobierania biometryk nie powinny, ze względu na ich wrażliwość dla praw człowieka, znaleźć się w ustawie jako gwarantującej obywatelowi bezpośrednią ochronę. Wskazuje na to cytowany już art. 8 ust. 2 Konwencji, który w odniesieniu do warunków ingerencji władzy publicznej w prawo do prywatności, obok „konieczności w społeczeństwie demokratycznym" podkreśla jej ustawowy charakter. Tymczasem w prawie polskim podstawa tej ingerencji jest zawarta w rozporządzeniu. Wydaje się zatem, że powyższa sądowa i legislacyjna analiza prawa do prywatności prowadzi do wniosku, że zarówno ustawa o dokumentach paszportowych, jak i akt wykonawczy do niej jest niezgodny z Konstytucją i prawem europejskim (Rady Europy).

Biometryzacja generuje również wiele problemów technicznych. Jednym z nich jest bezpieczeństwo danych zawartych w mikroczipie RFID. Pozwala on w sposób bezdotykowy, drogą bezprzewodową, transmitować informacje do czytników. Obszar zasięgu tej transmisji wynosi 10–60 cm, co oznacza, że osoba stojąca blisko jego właściciela może łatwo i bez żadnych podejrzeń odczytać zawarte w nim dane. W sierpniu 2006 roku hakerzy po raz pierwszy przedstawili skuteczną metodę takiego kopiowania tagów z brytyjskich paszportów biometrycznych, mimo że władze twierdziły, że jest to najlepiej zabezpieczony dokument na świecie. Okazało się, że wystarczy zakupić wyposażenie techniczne o wartości 200 $ (600 zł) oraz ustawić się w miejscu zasięgu fal radiowych, np. w autobusie, a następnie „ukraść" dane i umieścić je na nowym czipie zlokali-

[101] Rozporządzenie 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. 2006, Nr 152, poz. 1090.

zowanym w podrobionym paszporcie[102]. Doświadczenia Holandii oraz Stanów Zjednoczonych również pokazują, że hakerzy często i łatwo kradną dane właśnie w taki sposób, bez jakiejkolwiek wiedzy właściciela dokumentu[103].

Wkraczanie biometrii do życia społecznego jest tym bardziej niebezpieczne, że nie towarzyszy jej debata społeczna. Komisja Europejska w przeciągu zaledwie roku od zaproponowanych standardów ICAO oraz nacisków amerykańskich wprowadziła paszporty biometryczne na mocy rozporządzenia z 2004 roku. W dość kontrowersyjny sposób zinterpretowano art. 18 TWE, pozwalając sobie na stworzenie standardu bezpieczeństwa takiego dokumentu. Nie przeprowadzono w tej kwestii żadnych krajowych konsultacji społecznych, nie uwzględniono zdania obywateli państw członkowskich. W odniesieniu do regulacji biometryzacji innych dziedzin życia społecznego władze UE nie uwzględniły wątpliwości Europejskiego Inspektora Danych Osobowych czy Parlamentu Europejskiego. Wydaje się jednak, że prędzej czy później organy UE, ale przede wszystkim władze państw, zmierzą się z kosztami takiego bezkrytycznego postępowania. Grudniowe orzeczenie ETPCz jest tego pierwszym sygnałem.

Autor proponuje konstruktywnie, aby zastąpić ten program częściową elektronizacją życia ekonomicznego opartą na gwarancjach prawnych. Polegałaby ona na stworzeniu elektronicznych dokumentów wyposażonych wyłącznie w hasła i podpis elektroniczny, które nie będzie zawierał więcej informacji niż na obecnym dowodzie osobistym. Zabieg ten pozwoli zapobiec uprzedmiotowieniu człowieka, powstrzyma nadmierne wkraczanie państwa w stosunki prywatne oraz umożliwi osobom okradzionym z tożsamości poradzenie sobie z tym problemem.

[102] B. Johnson, *Hackers crack new biometric passports*, „The Guardian", 7 sierpnia 2006 r.
[103] *Hakerzy kradną dane z nowych paszportów*, „Dziennik", 30 października 2006 r.