Remigiusz Lewandowski

Biometria – nowe zastosowania

Wstęp

Biometria to wiedza o rozpoznawaniu żywych osób na podstawie pomiarów cech biologicznych (anatomicznych i fizjologicznych), zarówno pasywnych (jak np. wzór tęczówki i siatkówki oka, odciski palców, wygląd twarzy, geometria dłoni, układ naczyń krwionośnych), jak i aktywnych (np. dynamika pisma ręcznego, głos, ruch warg, chód)[1]. Przy poszukiwaniu optymalnego wyboru danej cechy biometrycznej jako narzędzia identyfikacji należy brać pod uwagę wiele różnych czynników, z których część przedstawiono w tabeli. Jak z niej wynika, każde ze stosowanych rozwiązań ma swoje mocne i słabe strony, a dokonując ostatecznego wyboru, powinno się przede wszystkim uwzględniać adekwatność rozwiązania do zaspokajanej potrzeby związanej z identyfikacją.

Tabela. Porównanie wybranych cech biometrycznych.

Charakterystyka	Odcisk palca	Geometria dłoni	Siatkówka oka	Tęczówka oka	Twarz	Podpis	Głos
Łatwość użycia	duża	duża	mała	średnia	średnia	duża	duża
Podatność na błędy	suchość skóry, zabrudzenia, wiek	zranienie dłoni	okulary	słabe oświetlenie	słabe oświetlenie, wiek, okulary, fryzura	zmiany we własnym podpisie	hałas, przeziębienie, pogoda
Dokładność	duża	duża	bardzo duża	bardzo duża	duża	duża	duża
Akceptowalność przez użytkownika	średnia	średnia	średnia	średnia	średnia	bardzo duża	duża

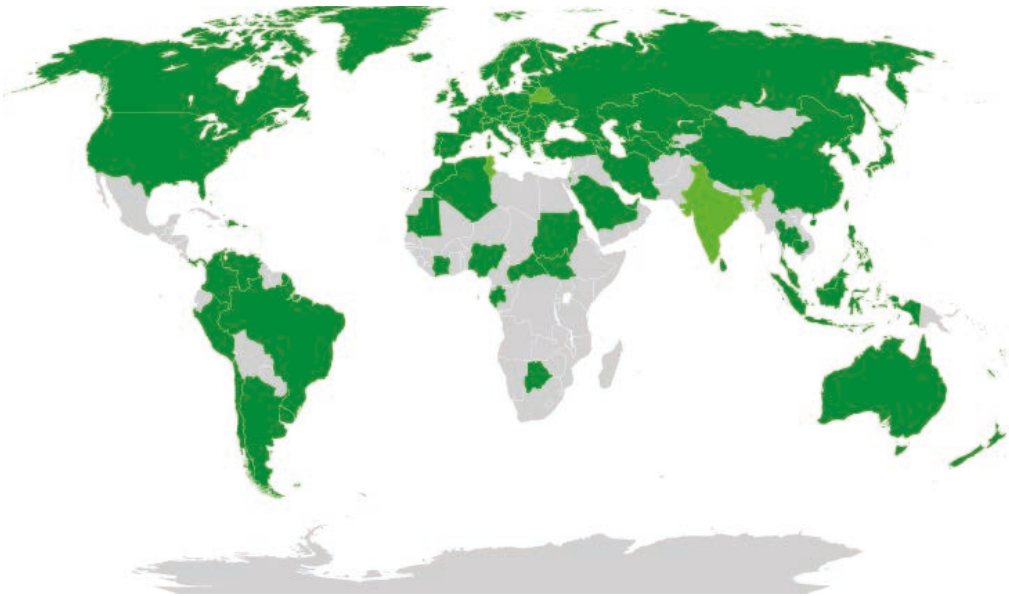
[1] B. Hołyst, J. Pomykała, *Biometria w systemach uwierzytelniania*, „Biuletyn WAT" 2011, t. 60, nr 4, s. 418–419.

Charakterystyka	Odcisk palca	Geometria dłoni	Siatkówka oka	Tęczówka oka	Twarz	Podpis	Głos
Wymagany poziom bezpieczeństwa	duży	średni	duży	bardzo duży	średni	średni	średni
Długoterminowa stabilność	duża	średnia	duża	duża	średnia	średnia	średnia

Skala: bardzo mały, mały, średni, duży, bardzo duży.

Źródło: Opracowanie własne na podstawie: S. Prabhakar, S. Pankat, A.K. Jain, *Biometric Recognition: Security and Privacy Concern*, „IEEE Transactions on Security & Privacy" 2003, nr 1, s. 33–42.

Obecnie biometria stanowi stałe, a zarazem najważniejsze ogniwo łańcucha wartości dokumentów identyfikacyjnych. Rozwiązania biometryczne znajdują zastosowanie w paszportach znacznej liczby państw. Paszport biometryczny praktycznie staje się standardem, co przedstawiono na rysunku 1.



Rys. 1. Państwa, w których wprowadzono i w których planuje się wprowadzenie paszportów biometrycznych.

Legenda: kolor ciemnozielony – państwa, w których wprowadzono paszporty biometryczne; kolor jasnozielony – państwa, w których planuje się wprowadzenie paszportów biometrycznych.

Źródło: https://commons.wikimedia.org/w/index.php?curid=47470662 [dostęp: 10 X 2016].

1. Biometria w dokumentach publicznych

Praktycznie rzecz biorąc, paszporty niebiometryczne obowiązują jedynie w państwach afrykańskich (z pewnymi wyjątkami), w wybranych państwach Ameryki Środkowej i Południowej oraz w Azji. Stosowanie w paszportach rozwiązań biometrycznych promuje Międzynarodowa Organizacja Lotnictwa Cywilnego (ICAO). Załącznik 9 do *Konwencji o międzynarodowym lotnictwie cywilnym* zawiera zalecenie, aby strony *Konwencji* stosowały dane biometryczne w wydawanych przez nie paszportach, wizach oraz innych oficjalnych dokumentach podróży i używały jednej lub więcej dodatkowych technologii służących do zapisywania danych (pkt 3.9). Wśród opcjonalnych danych biometrycznych (poza obowiązkowym, zapisanym cyfrowo wizerunkiem twarzy) wskazuje się obrazy odcisków palca (palców) oraz tęczówki. Polski paszport w zakresie danych biometrycznych zawiera jedynie odcisk palca. Jak ważny jest rozwój technik biometrycznych wskazuje próba obejścia systemów opartych na biometrii. Klasycznym przykładem może być tu próba przejścia przez bramkę biometryczną na granicy przez osobę ukrywającą pod ubraniem dziecko. Ten przykład obrazuje, jak wiele rozwiązań należy stosować w sytuacjach automatyzacji kontroli, zwłaszcza kontroli granicznej. W omawianym przypadku rozwiązaniem może być wdrożenie systemu weryfikującego, czy rzeczywiście przez bramkę przechodzi jedna osoba (np. przez rejestrację w momencie przejścia przez bramkę), czy odgłos bicia serca pochodzi od jednej osoby, czy od większej liczby osób. Testową bramkę biometryczną opracowaną przez Wojskową Akademię Techniczną przedstawiono na rys. 2.

Rys. 2. Testowa bramka biometryczna opracowana przez Wojskową Akademię Techniczną.
Źródło: http://www.ioe.wat.edu.pl/aktualnosci3/testy-systemu-do-automatycznej-odprawy-osob-na-przejsciu-granicznym-w-medyce/ [dostęp: 10 XII 2016].

Niezwykle interesujący jest projekt PROTECT[2] realizowany przez konsorcjum międzynarodowe (z udziałem polskiej specjalistycznej firmy ITTI Sp. z o.o.). Stanowi on zaawansowany multimodalny system identyfikacji biometrycznej, który ma być odpowiedzią na rosnącą liczbę podróżnych i ograniczoną przepustowość europejskich przejść granicznych. Tworzony system ma potencjał, aby być zastosowanym na wszystkich typach przejść granicznych (tj. na przejściach lądowych, morskich i na lotniskach). Zaletą omawianego systemu będzie możliwość weryfikacji podróżnych bez potrzeby ich zatrzymywania ze zminimalizowanym wymogiem interakcji z systemem. Osiągnięcie wspomnianych założeń ma zostać spełnione m.in. dzięki zastosowaniu nowoczesnych rozwiązań z dziedziny biometrii i wizji komputerowej. System ma umożliwić weryfikację tożsamości na podstawie cech antropometrycznych oraz charakterystyki chodu. Oparty jest na sieci kamer głębi, które generują obraz 3D oraz modelują sylwetkę obserwowanej osoby. Na podstawie zebranych danych tworzony algorytm wykorzystuje unikatowe cechy antropometryczne (np. odcinki wybranych części ciała) oraz cechy charakterystyczne wyznaczone z sekwencji chodu danej osoby w celu zweryfikowania jej tożsamości. Zaletą tego rozwiązania jest weryfikacja osób w ruchu oraz podwyższona odporność na powszechne próby podrabiania wzorca biometrycznego.

Coraz częściej biometria znajduje zastosowanie także przy opracowywaniu dowodów osobistych. W Europie elektroniczny dowód osobisty wyposażony w mikroprocesor z danymi biometrycznymi staje się rozwiązaniem standardowym. Obecnie dowód elektroniczny obowiązuje w 27 państwach naszego kontynentu. W Polsce wprowadzenie elektronicznych dowodów osobistych jest planowane od 2007 r., ale jak dotychczas, z różnych przyczyn, nie zostało zrealizowane. Niemniej jednak, w lutym 2017 r. Ministerstwo Cyfryzacji opublikowało koncepcję wdrożenia polskiego dowodu osobistego z warstwą elektroniczną[3]. Dokument, o którym mowa, to poprawiona wersja koncepcji z 2016 r. Zgodnie z nią, w nowym dowodzie osobistym mają być wprowadzone dane biometryczne, tj. wizerunek twarzy.

Oprócz paszportów i dowodów osobistych władze państwowe emitują także inne dokumenty zawierające dane biometryczne zapisane na mikroprocesorach. W Polsce jest to np. biometryczna karta pobytu (z odciskiem palca). Niektóre państwa emitują elektroniczne prawa jazdy – zgodnie z normą ISO 18013[4] i (lub) rozporządzeniem Komisji UE 383/2012[5]. Są to: Salwador, wybrane stany w Indiach, Japonia, Maroko, Meksyk, Indonezja, stan Queensland w Australii, Chorwacja, Irlandia i Holandia[6].

---

[2] Projekt realizowany w ramach programu Horyzont 2020, nr grantu: 700259.

[3] https://mc.gov.pl/aktualnosci/nowa-koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna [dostęp: 27 II 2017].

[4] Ustanawia ramy dotyczące formatu wzoru i zawartości danych prawa jazdy.

[5] *Rozporządzenie Komisji (UE) nr 383/2012 z dnia 4 maja 2012 roku określajace wymagania techniczne wobec praw jazdy zawierających elektroniczny nośnik informacji (mikroprocesor)* – Dz. Urz. UE L 120 z 5 V 2012 r., s. 1.

[6] M. Stoltz, *Electronic Driver's Licences: Driving Towards the Future*, „ID & Secure Documents News" 2016, t. 4 [online], https://www.reconnaissance.net/secure-document-news/issues/may-2016/ [dostęp: 10 XII 2016].

Włączanie do tych dokumentów danych biometrycznych jest rozwiązane indywidualnie przez każde z wyżej wskazanych państw. Rozporządzenie Komisji UE 383/2012 dopuszcza umieszczenie na mikroprocesorze prawa jazdy danych dodatkowych w postaci wzoru tęczówki oka i odcisku palca posiadacza.

Rosnące zastosowanie biometrii w dokumentach nie powinno dziwić. Jest to jedna z najbardziej niezawodnych metod uwierzytelniania i weryfikacji tożsamości człowieka (lub identyfikacji osoby), ale jej skuteczność nie jest bezwarunkowa. W literaturze przedmiotu wskazuje się na warunki konieczne, które muszą towarzyszyć skutecznemu uwierzytelnianiu biometrycznemu, takie jak optymalne warunki dokonania pomiaru biometrycznego, aktualizacja tego pomiaru oraz optymalny poziom tolerancji[7]. Skuteczność biometrii można znacząco podnieść przez wprowadzenie pomiaru nie jednej, ale co najmniej dwóch cech biometrycznych. W ten sposób jeszcze bardziej można powiązać daną osobę z dokumentem, którym się ona posługuje. Niemniej jednak do biometrii, tak jak do każdej innej technologii, nie należy podchodzić bezkrytycznie[8].

W odniesieniu do dokumentów najczęściej stosowanym modelem uwierzytelniania biometrycznego jest weryfikacja. Polega ona na porównaniu w skali 1:1 zestawu cech biometrycznych danej osoby (pobranych podczas weryfikacji) z danymi biometrycznymi zapisanymi w dokumencie. W przypadku zgodności danych, które zostały pobrane w czasie weryfikacji, z danymi zapisanymi można mówić o pozytywnym efekcie sprawdzenia, tj. można stwierdzić, że osoba posługująca się danym dokumentem jest osobą, której ów dokument dotyczy. Zaletą tej metody jest szybkość weryfikacji (wyższa niż w przypadku identyfikacji[9]) oraz bezpieczeństwo danych. Dane biometryczne są bowiem przechowywane przez posiadacza dokumentu wraz z dokumentem i nie są tworzone centralne bazy danych biometrycznych obywateli.

Skuteczność rozwiązań biometrycznych dostrzegana przez władze publiczne w sytuacjach związanych z bezpieczeństwem państwa i migracją obywateli nie uszła też uwadze innych sektorów gospodarczych. Biometria coraz częściej znajduje zastosowanie w obrocie handlowym. Dotyczy to choćby tabletów, notebooków i smartfonów, w których często są instalowane czujniki odcisku palca pozwalające na biometryczne związanie urządzenia (i przechowywanych na nim danych) z jego posiadaczem. W niektórych państwach karty identyfikacyjne z zapisanymi danymi biometrycznymi są stosowane przez uniwersytety w celu poprawy jakości kontroli dostępu i efektywnej identyfikacji studentów podczas egzaminów[10]. System biometryczny był wykorzystywany również do identyfikacji obywateli w wyborach powszechnych[11]. W przyszło-

[7] B. Hołyst, J. Pomykała, *Biometria w systemach uwierzytelniania*…, s. 420–421.

[8] E. Jakielaszek, *Mechanizmy kształtujące zarządzanie tożsamością*, „Człowiek i Dokumenty" 2017, nr 44, s. 58.

[9] Podczas identyfikacji pobrane dane biometryczne porównuje się ze zbiorem danych zawartych w określonej bazie.

[10] E. Harinda, E. Ntagwirumugara, *Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities*, „Journal of Information Security" 2015, nr 6, s. 93–100.

[11] W. Gutfeter, A. Pacut., *Człowiek w systemie biometrycznym*, w: M. Tomaszewska-Michalak,

ści przewiduje się szerokie zastosowanie biometrii w obrocie prawnym, w tym także w zakresie składania podpisu elektronicznego[12].

Jednak zastosowania biometrii na znacznie szerszą skalę należy upatrywać w dwóch zasadniczych sferach, tj. w bankowości i w systemach kontroli dostępu opartych na kartach mikroprocesorowych.

2. Biometria w bankowości

Biometria w bankowości pojawiła się już ponad dekadę temu. W 2004 r. kolumbijski Bancafe Bank udostępnił ok. 400 bankomatów biometrycznych wykorzystujących odcisk palca. W tym samym roku w Japonii rozpoczęto udostępnianie bankomatów wykorzystujących biometrię naczyń krwionośnych (m.in. Mizuho Bank, Japan Post Bank, Bank of Kyoto, Resona Bank, Bank of Yokohama). Z kolei biometria tęczówki oka znalazła po raz pierwszy zastosowanie w bankowości w Jordanii (Cairo Amman Bank) – na potrzeby bankomatów oraz oddziałów banku, a w dalszej kolejności – w bankowości internetowej.

W Polsce historia biometrii w bankowości rozpoczęła się w 2010 r. – Bank Polskiej Spółdzielczości oraz Podkarpacki Bank Spółdzielczy zastosowały biometrię odcisku palca (rys. 3). W późniejszym okresie rozwiązania biometryczne zaczęły być oferowane przez inne banki, np. przez Bank BPH czy Getin Bank. Obecnie najbardziej atrakcyjne wydaje się jednak zastosowanie biometrii w bankowości mobilnej oraz w ramach fizycznych oddziałów.

Rys. 3. Biometryczny bankomat Banku Polskiej Spółdzielczości.

Źródło: http://prnews.pl/hydepark/bank-bps-rezygnuje-z-biometrii-6551894.html [dostęp: 10 XII 2016].

T. Tomaszewski, *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, Warszawa 2015, s. 80.

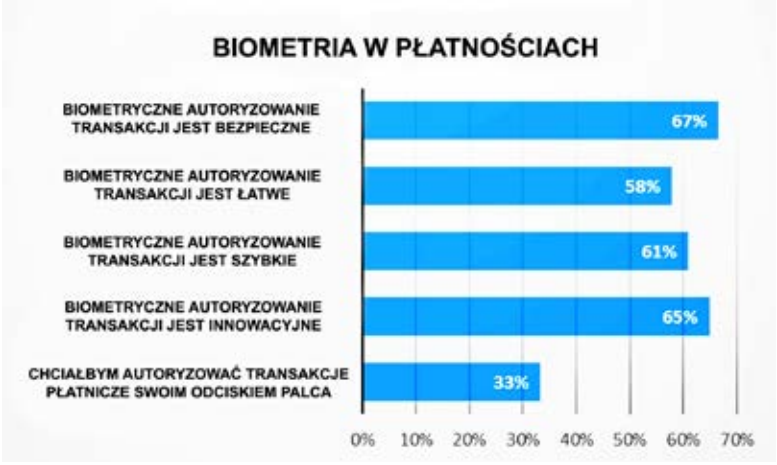
[12] T. Dziedzic, *Biometryczny podpis elektroniczny*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, s. 93–102.

Nieliczne banki w Polsce zaoferowały już możliwość weryfikacji tożsamości z użyciem danych biometrycznych na smartfonach. Tego rodzaju aplikacje mobilne są oferowane przez Millennium Bank, Meritum Bank, ING Bank Śląski, Euro Bank czy Citi Bank Handlowy (rys. 4). Niestety, z wyjątkiem Banku Millennium omawiane rozwiązanie jest możliwe tylko na urządzeniach firmy Apple (czytnik Touch ID). Są to jednak rozwiązania wyspowe, bardziej przypominające gadżety dla klientów wymagających nowinek technologicznych. W bankowości biometria nie zagościła jeszcze na dobre. Stąd branża z zaciekawieniem czeka na wyniki ogłoszonego w zeszłym roku przez Bank PKO BP projektu biometrycznego, który ma kompleksowo objąć wszystkie kanały dostępowe banku[13].

Rys. 4. Aplikacja mobilna Citi Banku Handlowego.
Źródło: https://www.online.citibank.pl/landing/citimobile/index.htm [dostęp: 10 XII 2016].

Badania ankietowe przeprowadzone w Polsce we wrześniu 2016 r. przez MasterCard dowodzą, że Polacy są entuzjastami zastosowania biometrii w bankowości. Jak wynika z rys. 5 dominująca część polskich obywateli uważa autoryzację płatności dokonywaną przy zastosowaniu rozwiązań biometrycznych za innowacyjną, prostą i bezpieczną. Jedna trzecia ankietowanych jest z kolei skłonna do wykorzystania swojego odcisku palca jako metody autoryzacji transakcji płatniczej.

[13] http://wyborcza.biz/biznes/1,147879,18140726,PKO_BP_chce_wdrozyc_kompleksowy_system_biometry-cznej.html (uprzejma prośba o weryfikację zapisu) [dostęp: 10 XII 2016].



Rys. 5. Wyniki badań ankietowych dotyczące zastosowania biometrii w bankowości.
Źródło: Opracowanie własne na podstawie: http://newsroom.mastercard.com/eu/pl/press-releases/badanie-mastercard-polscy-konsumenci-oczekuja-wiecej-cyfrowych-uslug/ [dostęp: 10 XII 2016].

Coraz więcej polskich banków prowadzi prace nad wdrożeniem systemów biometrycznych jako skutecznej kontroli tożsamości klientów, niosącej za sobą podniesienie bezpieczeństwa świadczonych usług[14]. Wydaje się, że jest to trend nieodwracalny.

3. Biometria w systemach kontroli dostępu

Systemy kontroli dostępu oparte na kartach mikroprocesorowych to drugi zasadniczy obszar wykorzystania biometrii w innych celach niż weryfikacja tożsamości z wykorzystaniem dokumentów publicznych. Tego typu systemy są stosowane praktycznie we wszystkich średnich i dużych przedsiębiorstwach oraz w urzędach administracji publicznej. Ich rola sprowadza się do zablokowania dostępu – zwykle przez zamknięcie bramki lub śluzy – do określonych pomieszczeń osobom nieuprawnionym. Niestety, w większości przypadków taka kontrola ma charakter iluzoryczny. Sprowadza się bowiem do weryfikacji, czy karta, którą posługuje się dana osoba, jest ważna i czy umożliwia dostęp do konkretnego pomieszczenia. Nie następuje natomiast sprawdzenie, czy osoba, która posługuje się danymi, jest tą osobą, której uprawnienia dostępowe są przypisane do danej karty. W przypadku braku kontroli tożsamości osób wchodzących do danych pomieszczeń (co jest standardem w odniesieniu do pracowników, którzy korzystają jedynie z identyfikatorów – kart dostępu) relatywnie łatwe jest wtargnięcie do określonych pomieszczeń (lub na określony teren) osób nieuprawnionych. Wystarczy do tego kradzież identyfikatora (karty dostępowej) osoby uprawnionej i wykorzystanie uprawnień dostępowych tej osoby. Czy kradzież identyfikatora

[14] M. Tomaszewska, *Technologia biometryczna w Polsce*, w: *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, B. Hołyst (red.), Warszawa 2014, s. 738–739.

jest trudna? Odpowiedzi na to pytanie powinien udzielić sobie każdy z nas, analizując, jakie środki bezpieczeństwa przedsiębierze, aby chronić kartę dostępową przed kradzieżą. Nie są to środki szczególnie zaawansowane i dające rękojmię zapewnienia bezpieczeństwa.

Zagrożenia związane z nieuprawnionym użyciem kart dostępowych są szczególnie istotne w przypadku podmiotów gospodarczych ważnych z punktu widzenia bezpieczeństwa państwa oraz w przypadku niektórych instytucji publicznych. Zidentyfikowanie tego rodzaju przedsiębiorstw, zarówno prywatnych, jak i kontrolowanych kapitałowo przez Skarb Państwa, nie jest trudne. Można tego dokonać przez analizę sektorową i wyodrębnienie tych dziedzin gospodarki, które pełnią funkcje strategiczne z punktu widzenia bezpieczeństwa narodowego. W wąskim zakresie są to[15]:

1) wytwarzanie energii elektrycznej i zaopatrywanie w ten surowiec,
2) wydobycie, przesył, dystrybucja i magazynowanie paliw gazowych,
3) wytwarzanie, przesył i magazynowanie paliw płynnych,
4) telekomunikacja,
5) bankowość,
6) produkcja dokumentów i banknotów,
7) przemysł zbrojeniowy.

W szerszym ujęciu zaś dziedziny gospodarki złożone z przedsiębiorstw, w odniesieniu do których kontrola dostępu – z punktu widzenia bezpieczeństwa narodowego – ma znaczenie zasadnicze, obejmują ponadto, oprócz wyżej wskazanych, wydobycie węgla kamiennego i przemysł chemiczny[16]. W ramach tych sektorów występują następujące podmioty gospodarcze kontrolowane przez Skarb Państwa: Polska Grupa Energetyczna S.A., Tauron S.A., Energa S.A., Enea S.A., Polskie Sieci Elektroenergetyczne S.A., Polskie Górnictwo Naftowe i Gazownictwo S.A., Gaz-System S.A., Polski Koncern Naftowy Orlen S.A., Lotos S.A., Przedsiębiorstwo Eksploatacji Rurociągów Naftowych „Przyjaźń" S.A., PKO Bank Polski S.A., Bank Ochrony Środowiska S.A., Bank Gospodarstwa Krajowego, Polska Wytwórnia Papierów Wartościowych S.A., Polska Grupa Zbrojeniowa S.A., Kompania Węglowa S.A., Jastrzębska Spółka Węglowa S.A., Katowicki Holding Węglowy S.A. oraz Grupa Azoty S.A. Niektórzy badacze wskazują dodatkowo takie sektory, jak transport lotniczy, kolejowy oraz morski, a także media.

Ponadto przepisy prawa określają także inne podmioty gospodarcze istotne z punktu widzenia państwa i bezpieczeństwa narodowego. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[17] nakłada obowiązek ochrony obiektów, instalacji lub urządzeń infrastruktury krytycznej (IK) przez ich właścicieli oraz posiadaczy samoistnych i zależnych. Przedsiębiorstwa będące właścicielami i posiadaczami infra-

[15] R. Lewandowski, *Bezpieczeństwo narodowe a strategiczne sektory gospodarki i regulacyjna rola państwa*, w: *Wymiary zarządzania ryzykiem w obrocie gospodarczym*, K. Raczkowski, S. Wojciechowska-Filipek (red.), Warszawa 2016, s. 380–381.

[16] Tamże, s. 376.

[17] Dz.U. z 2007 r. nr 89 poz. 590, ze zm.

struktury krytycznej są wyszczególnione w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład IK. Ten wykaz jest niejawny. Z kolei inną grupę przedsiębiorstw definiuje *Rozporządzenie Rady Ministrów z 3 dnia listopada 2015 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym*[18]. Wymienia on 185 podmiotów. Natomiast *Rozporządzenie Rady Ministrów z dnia 22 października 2010 r. w sprawie określenia przedsiębiorstw państwowych oraz jednoosobowych spółek Skarbu Państwa o szczególnym znaczeniu dla gospodarki państwa*[19] obejmuje obecnie 12 podmiotów gospodarczych.

Należy założyć, że realną ochroną dostępu do własnych pomieszczeń i terenów powinny być zainteresowane także przedsiębiorstwa, które nie pełnią strategicznych funkcji z punktu widzenia bezpieczeństwa narodowego. W tym przypadku może chodzić o ochronę interesu prywatnego i ochronę przed działaniami szpiegowskimi ze strony konkurencji. Tę realną ochronę dla wszystkich wymagających tego podmiotów zapewnia jednoznaczne powiązanie pracownika z wydaną dla niego kartą dostępową (z określonymi uprawnieniami dostępu). To powiązanie tworzy biometria i zawarcie określonych danych biometrycznych pracownika na jego karcie dostępowej (identyfikatorze). Tradycyjne metody kontroli dostępu nie zdają egzaminu w sytuacji obecnych zagrożeń[20].

W odniesieniu do instytucji publicznych biometria znajduje zastosowanie w przypadku ochrony niektórych wydzielonych pomieszczeń, ale nie jest to rozwiązanie stosowane na szeroką skalę. Ciekawą inicjatywę w tym zakresie planuje Ministerstwo Cyfryzacji, które rozważa wprowadzenie biometrycznej kontroli dostępu nie tylko do pomieszczeń wydzielonych, lecz także do całych gmachów użytkowanych przez resort[21]. Jeśli te plany wejdą w życie, będą niezwykle interesującym i cennym testem efektywności i praktyczności tej metody kontroli dostępu i zapewnienia bezpieczeństwa fizycznego.

Przez wprowadzenie mechanizmu weryfikującego, czy osoba posługująca się daną kartą dostępową jest osobą, dla której ta karta została wydana, w pełni można wyeliminować ryzyko wejścia na teren określonej firmy czy instytucji osoby, która używa cudzej karty dostępowej. To w istotny sposób podnosi poziom bezpieczeństwa, szczególnie, gdy dotyczy przedsiębiorstw oraz instytucji o znaczeniu strategicznym dla bezpieczeństwa narodowego. W dobie globalnego terroryzmu tego rodzaju środki bezpieczeństwa powinny mieć charakter standardowy w odniesieniu do tej grupy podmiotów.

Omawiając zagadnienie biometrii, nie sposób pominąć problemu ochrony danych osobowych. Artykuł 1 Ustawy z 29 dnia sierpnia 1997 r. o ochronie danych osobowych[22] mówi, że każdy ma prawo do ochrony własnych danych osobowych (ust. 1),

[18] Dz.U. z 2015 r. poz. 1871, ze zm.

[19] Dz.U. z 2010 r. nr 212 poz. 1387, ze zm.

[20] A.K. Jain, A. Kumar, *Biometrics of Next Generation: An Overview*, w: *The Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini, D. Tzovaras (red.), London 2012, s. 49–50.

[21] http://www.money.pl/gospodarka/wiadomosci/artykul/dowod-strezynska-biometria-pwpw mdokumenty,177,0,2234801.html [dostęp: 18 IV 2017].

[22] Tekst jednolity: Dz.U. z 2016 r. poz. 922.

a przetwarzanie takich danych może nastąpić ze względu na dobro publiczne, dobro osoby, której one dotyczą, lub ze względu na dobro osób trzecich – w zakresie i trybie określonym ustawą (ust. 2). Ponadto zgodnie z art. 23 ust. 1 cytowanej ustawy przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
2) jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
4) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne do realizacji przez administratorów danych albo odbiorców danych prawnie usprawiedliwionych celów, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Równolegle problem wykorzystywania danych osobowych w relacjach pracodawca – pracobiorca reguluje art. 22 kodeksu pracy. Dane, których pracodawca może żądać, to imię (imiona) i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie oraz przebieg dotychczasowego zatrudnienia. Pracodawca może żądać także numeru PESEL oraz innych informacji, w tym imion i nazwisk oraz dat urodzenia dzieci, jeżeli od ich podania zależy korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Innych danych pracodawca może żądać jedynie wówczas, gdy ich udostępnienie nakazują odrębne przepisy, a w zakresie nieuregulowanym w powyższym przepisie stosuje się przepisy o ochronie danych osobowych, a więc zwłaszcza do cytowanego wcześniej art. 23 ustawy o ochronie danych osobowych.

Przepisy prawa nie regulują zatem precyzyjnie wykorzystywania przez pracodawcę danych biometrycznych pracowników w związku z koniecznością zapewnienia bezpieczeństwa. Można co prawda domniemywać, że pobieranie danych biometrycznych od pracowników i ich przetwarzanie jest przewidziane w przesłance art. 23 ust. 1 pkt 5, tzn. jeśli jest to niezbędne do realizacji prawnie usprawiedliwionych celów przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Zapewnienie bezpieczeństwa należy uznać za prawnie usprawiedliwiony cel realizowany przez administratora danych (biometrycznych). Wydaje się jednak, że to zagadnienie wymaga doprecyzowania w przepisach prawa.

Należy także zważyć, że dotychczas Generalny Inspektor Danych Osobowych (GIODO) prezentował sceptyczne podejście do wykorzystania danych biometrycznych w relacjach pomiędzy pracodawcą a pracownikiem (np. w zakresie kontroli dostępu): *A zatem jedyną podstawą do gromadzenia odcisków linii papilarnych może być przepis prawa. Skoro jednak nie ma regulacji zezwalających pracodawcom na żądanie*

od podwładnych danych biometrycznych, jak linii papilarnych, obrazu tęczówki oka czy kodu DNA, to ich gromadzenie jest zabronione[23]. Tego rodzaju podejście GIODO do biometrii nie wydaje się przystawać do współczesnych zagrożeń, w tym także zagrożeń terrorystycznych. Grupa Robocza Art. 29[24] uznała w dokumencie roboczym z 1 sierpnia 2003 r. dotyczącym biometrii, że:

> (…) dla celów kontroli dostępu (identyfikacja/weryfikacja) systemy biometryczne związane z cechami fizycznymi nie pozostawiającymi śladów (np. kształt dłoni, ale już nie odcisk palca) lub systemy biometryczne związane z cechami fizycznymi, które pozostawiają ślady, ale nie są oparte o zapisywanie tych danych i ich posiadanie przez osoby inne, aniżeli osoba, której te dane dotyczą (innymi słowy dane nie są zapisywane w urządzeniu kontroli dostępu lub centralnej bazie danych), tworzą mniejsze ryzyko naruszenia ochrony podstawowych praw i wolności człowieka[25].

Do takich mniej ryzykownych rozwiązań należą właśnie systemy dostępowe oparte na danych biometrycznych zapisywanych na kartach (identyfikatorach) dostępowych użytkowanych przez pracowników. Wydaje się zatem, że jest otwarta furtka do wdrożenia zaprezentowanych rozwiązań.

Niemniej jednak prawodawstwo Unii Europejskiej jest ukierunkowane na ścisłą ochronę danych biometrycznych. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*[26] wprowadza w art. 9 ust. 1 generalny zakaz przetwarzania m.in. danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Równocześnie to rozporządzenie wskazało szereg warunków, w których ów zakaz nie obowiązuje. Warto zwrócić uwagę zwłaszcza na to, że omawiany zakaz nie obowiązuje m.in. w przypadku, gdy:

1) została udzielona zgoda na przetwarzanie tych danych przez osobę, której to dotyczy (chyba że prawo krajowe lub UE przewiduje, że takiego zakazu uchylić nie można);
2) przetwarzanie jest niezbędne do wykonywania obowiązków i szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa

[23] http://www.giodo.gov.pl/348/id_art/3358/j/pl/ [dostęp: 10 XII 2016].

[24] Organ konsultacyjny składający się z przedstawicieli organów ochrony danych osobowych obywateli państw członkowskich Unii Europejskiej. Rolą Grupy Roboczej Art. 29 jest czuwanie nad stosowaniem przez państwa członkowskie *Dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony danych osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (Dz. Urz. L 281 z 23 XI 1995 r., s. 31–50.

[25] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf [dostęp: 10 XII 2016].

[26] Dz.Urz. UE L 119 z 4 V 2016 r., s. 1.

pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem UE lub prawem krajowym, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych oraz interesów osoby, której dane dotyczą;

3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa UE lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych oraz przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Powyższe przepisy rozporządzenia nie wykluczają zatem możliwości stosowania biometrii w celach związanych z bezpieczeństwem, zwłaszcza w zakresie fizycznej kontroli dostępu lub dostępu do systemów teleinformatycznych (np. w bankowości internetowej), nawet w przypadku braku zgody osoby zainteresowanej, której dane biometryczne mają być przedmiotem przetwarzania. W takim jednak przypadku jest konieczna szczegółowa regulacja prawna. Należy także podkreślić, że zgodnie z art. 9 ust. 4 tego rozporządzenia państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania m.in. danych biometrycznych. Ustawodawca unijny pozostawił zatem dość duży zakres swobody w kształtowaniu zasad przetwarzania danych biometrycznych.

Wnioski

Biometria staje się coraz bardziej powszechnym instrumentem poprawy bezpieczeństwa. Szczególne cechy tej metody identyfikacji sprawiają, że z powodzeniem może ona znaleźć zastosowanie już nie tylko w dokumentach emitowanych przez państwo, lecz także w środowisku gospodarczym, obejmującym choćby banki czy przedsiębiorstwa o znaczeniu strategicznym dla bezpieczeństwa państwa. Analiza implementacji rozwiązań biometrycznych w Polsce prowadzi do wniosku, że poza wybranymi kategoriami dokumentów publicznych nie mają one powszechnego charakteru. Na szerszą skalę są stosowane przez niektóre banki jako instrument uwierzytelniania klienta w systemach bankowości elektronicznej. Z kolei jako narzędzie kontroli dostępu fizycznego biometria pozostaje technologią stosowaną w małym zakresie, pomimo istnienia obiektywnych przesłanek wskazujących na taką potrzebę, zwłaszcza w przedsiębiorstwach będących właścicielami lub posiadaczami infrastruktury krytycznej. Świadczy to o konieczności ciągłego podnoszenia wiedzy na temat zagrożeń wymierzonych w funkcjonowanie najważniejszych podmiotów gospodarczych w naszym kraju. Równocześnie u przedsiębiorców powinna rosnąć świadomość dostępnych technologii i rozwiązań, które powyższe zagrożenia mogą minimalizować.

Ważne jest również to, aby za coraz częstszym stosowaniem biometrii nadążały przepisy prawa, w tym przede wszystkim dotyczące ochrony danych osobowych. Powinny one z jednej strony zapewniać możliwość podnoszenia poziomu bezpieczeństwa podmiotów gospodarczych i urzędów przez stosowanie systemów biometrycznych, a z drugiej – ustanawiać minimalne standardy bezpieczeństwa w zakresie przechowywania danych biometrycznych i ich przetwarzania. Te standardy powinny chronić dane biometryczne przed utratą poufności, dostępności, integralności oraz rozliczalności[27], a zwłaszcza przed atakami na systemy biometryczne.

Bibliografia:

1. Dziedzic T., *Biometryczny podpis elektroniczny*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, Wolumina.pl Daniel Krzanowski.
2. Gutfeter W., Pacut A.*, Człowiek w systemie biometrycznym*, w: M. Tomaszewska-Michalak, T. Tomaszewski, *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, Warszawa 2015, SAWPiA UW.
3. Harinda E., Ntagwirumugara E., *Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities*, „Journal of Information Security" 2015, nr 6.
4. Hołyst B. , Pomykała J., *Biometria w systemach uwierzytelniania*, „Biuletyn WAT" 2011, t. 60, nr 4.
5. Jain A.K., Kumar A., *Biometrics of Next Generation: An Overview*, w: *The Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini, D. Tzovaras (red.), Springer, Dordrecht, Heidelberg, Nowy York, Londyn 2012.
6. Jakielaszek E., *Mechanizmy kształtujące zarządzanie tożsamością*, „Człowiek i Dokumenty" 2017, nr 44.
7. Krawczyk W., *Bezpieczeństwo teleinformatyczne kryminalistycznych baz danych odcisków palców (AFIS) oraz DNA*, w: *Nowe techniki badań kryminalistycznych a bezpieczeństwo informacji*, B. Hołyst, J. Pomykała, P. Potejko (red.), Warszawa 2014, PWN.
8. Lewandowski R., *Bezpieczeństwo narodowe a strategiczne sektory gospodarki i regulacyjna rola państwa*, w: *Wymiary zarządzania ryzykiem w obrocie gospodarczym*, K. Raczkowski, S. Wojciechowska-Filipek (red.), CeDeWu, Warszawa 2016.

[27] W. Krawczyk*, Bezpieczeństwo teleinformatyczne kryminalistycznych baz danych odcisków palców (AFIS) oraz DNA*, w: *Nowe techniki badań kryminalistycznych a bezpieczeństwo* informacji, B. Hołyst, J. Pomykała, P. Potejko (red.), Warszawa 2014, s. 181.

9. Prabhakar S., Pankat S., Jain A.K., *Biometric Recognition: Security and Privacy Concern*, „IEEE Transactions on Security & Privacy" 2003, nr 1.
10. Stoltz M., *Electronic Driver's Licences: Driving Towards the Future*, „ID & Secure Documents News" [online] 2016, t. 4, https://www.reconnaissance.net/secure-document-news/issues/may-2016/ [dostęp: 10 XII 2016].
11. Tomaszewska M., *Technologia biometryczna w Polsce*, w: *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, B. Hołyst (red.), Warszawa 2014, Wydawnictwo Naukowe PWN.

Abstrakt

Artykuł przedstawia analizę nowych zastosowań biometrii w obszarze bezpieczeństwa. Są dwa najważniejsze zastosowania tej metody. Po pierwsze, poza jej wykorzystaniem w dokumentach, takich jak dowody osobiste czy paszporty, biometria może być z powodzeniem stosowana jako narzędzie fizycznej kontroli dostępu w przedsiębiorstwach o znaczeniu strategicznym w systemie bezpieczeństwa publicznego. Po drugie, może znaleźć zastosowanie w bankowości elektronicznej – jako instrument identyfikacji klienta i autoryzacji transakcji. W obu przypadkach wykorzystanie biometrii w sposób znaczący zwiększa poziom zabezpieczeń w porównaniu do alternatywnych, tradycyjnych narzędzi. Jednakże jej powszechne zastosowanie wymaga regulacji prawnych, które z jednej strony pozwoliłyby organizacjom publicznym i prywatnym korzystać z tej metody jako instrumentu zapewniającego bezpieczeństwo, a z drugiej – ustanawiałyby minimalne standardy ochrony danych biometrycznych.

Słowa kluczowe: biometria, kontrola dostępu, bankowość.