BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2021
Nr 2 (XLIII)

DOI: 10.48269/2451-0718-btip-2021-2-007
Data wpłynięcia: 20.03.2021
Data akceptacji: 14.08.2021

Paweł Wilkowski

mgr, funkcjonariusz policji, specjalista w Wydziale dw. z Przestępczością Gospodarczą Komendy Miejskiej Policji w Olsztynie
https://orcid.org/0000-0001-6994-3099

Bezpieczeństwo Rzeczypospolitej Polskiej w kontekście dynamicznego rozwoju technologii biometrycznych. Część I

Wprowadzenie

W związku z dostrzeżoną w nauce luką dotyczącą możliwych zagrożeń dla bezpieczeństwa narodowego, wynikających ze stosowania zabezpieczeń opartych na technologiach biometrycznych, autor przeprowadził badania, których rezultatem będzie kompleksowa analiza stanu bezpieczeństwa Rzeczypospolitej Polskiej w kontekście niekontrolowanej retencji danych biometrycznych. Badania wstępne pozwoliły zidentyfikować szereg problemów badawczych, które dotychczas nie były objęte zainteresowaniem naukowców.

W celu usystematyzowania informacji o dostępnych technologiach biometrycznych przeanalizowana została dostępna literatura przedmiotu, w tym publikacje dostępne w Internecie, a uzyskane w ten sposób treści zestawiono następnie z wiedzą praktyczną oraz aspektami życia codziennego, na które owa literatura zdaje się zupełnie nie zwracać uwagi. Przeprowadzone badania tworzą grunt pod dalsze działania w obszarze zagrożeń bezpieczeństwa narodowego wynikających ze stosowania technologii biometrycznych. Niniejszy, podzielony na dwie części, artykuł stanowi część pracy badawczej autora obejmującej zwięzły opis stosowanych obecnie technologii biometrycznych. W sposób syntetyczny przedstawiono poziom aktualnej wiedzy z owego zakresu oraz przewidywane kierunki rozwoju biometrii w najbliższej przyszłości. Niniejsza publikacja jest zatem jedynie wstępem do dalszych rozważań w kwestii zagrożeń dla bezpieczeństwa narodowego, zastanej sytuacji prawnej, przy

aktualnym rozwoju technologicznym. Zatem przez wzgląd na kompleksowość i interdyscyplinarną naturę omawianego zagadnienia niezbędne jest skupienie się na poszczególnych jego aspektach, aby finalnie, w ujęciu holistycznym, rozstrzygnąć wpływ omawianych technologii na poziom bezpieczeństwa narodowego. Kluczem do zrozumienia tej korelacji jest wstępna prezentacja najpopularniejszych systemów biometrycznych i ich zwięzła charakterystyka.

Definicje biometrii i danych biometrycznych

Biometria to nauka, która zajmuje się analizą indywidualnych cech osobniczych charakteryzujących i definiujących każdy żywy organizm. Z semantycznego punktu widzenia słowo „biometria" wywodzi się z greki, gdzie *bios* to życie, zaś *metrum* oznacza mierzyć[1]. Zasadne jest zatem stwierdzenie, że jej istotą jest dążenie do stworzenia pakietu danych, na podstawie którego możliwa będzie identyfikacja wskazanej jednostki.

Według międzynarodowej normy z dziedziny technologii informatycznych ISO/IEC 2382:2015 pojęcie biometrii zdefiniowane zostało jako użycie specyficznych atrybutów odzwierciedlających unikalne cechy osoby w celu potwierdzenia jej tożsamości. Webopedia, techniczny słownik on-line dla studentów i nauczycieli, definiuje pojęcie „dane biometryczne" jako ogólne określenie dowolnych danych komputerowych wytworzonych w procesie przetwarzania biometrycznego. Obejmuje to zatem dane dotyczące próbki biometrycznej, modelu biometrycznego, wybranych cech charakterystycznych, wartości podobieństwa, wszystkie dane weryfikacyjne i identyfikacyjne, takie jak imię i nazwisko, oraz dane demograficzne[2]. Definicja zawarta w art. 4 pkt 14 unijnego rozporządzenia o ochronie danych osobowych – RODO – definiuje dane biometryczne jako „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne"[3].

W podobny sposób biometrię definiuje amerykańskie Federalne Biuro Śledcze (FBI), które regularnie aktualizuje literaturę dla swoich pracowników, pozwalając im tym samym na nadążanie za stale zmieniającym się światem i sprostanie wyzwaniom stawianym przez wymagającą służbę w obronie bezpieczeństwa narodowego. Według ekspertów rzeczonej agencji biometria oznacza zespół mierzalnych (anatomicznych i fizjologicznych) lub behawioralnych cech umożliwiających identyfikację jednostki[4].

---

1 K. Krassowski, I. Sołtyszewski, *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252, s. 39.

2 V. Beal, *Biometric Data* [hasło], 1.04.2008, Webopedia.com, https://www.webopedia.com/TERM/B/biometric_data.html [dostęp: 26.04.2020].

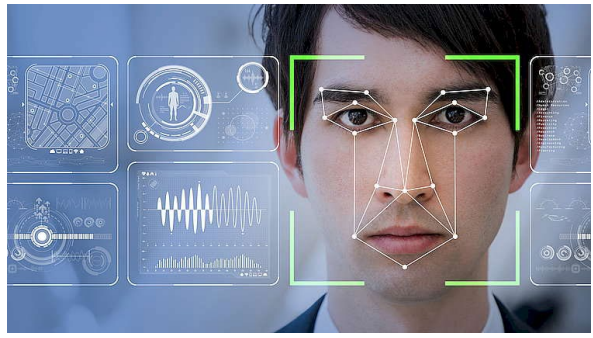
3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L/119 z 4.05.2016.

4 FBI, *Fingerprints and Other Biometrics*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics [dostęp: 27.04.2020].

Każdy człowiek posiada szereg cech pozwalających na jego identyfikację, których niepowtarzalność i stopień złożoności zezwalają na przyjęcie założenia, że cechy te umożliwiają wskazanie na ich podstawie konkretnej jednostki z niemal stuprocentową precyzją. Dlatego też często definiuje się biometrię jako „naukę badającą metodami statystycznymi prawidłowości zmian w obrębie populacji, wykonującą pomiary wielkości, ciężaru i kształtu istot żywych"[5].

Posługiwanie się przez podmioty komercyjne, jak i przez instytucje rządowe bazami danych zawierającymi unikatowe cechy ludzkiego organizmu w procesie identyfikacji czy weryfikacji, wydaje się założeniem słusznym, mającym na celu usprawnienie ich funkcjonowania. Przynajmniej taka narracja towarzyszy działaniom podejmowanym przez podmioty umocowane do pozyskiwania danych biometrycznych, które w mniejszym lub większym stopniu dotyczą życia statystycznego obywatela. Jednak bez względu na nierozerwalnie związane z omawianym zagadnieniem kontrowersje, idea wykorzystania biometrii staje się coraz powszechniejsza, co implikuje liczne nieporozumienia. Przykładem nagminnego stosowania biometrii są bardzo popularne skanery analizujące rysy twarzy (rys. 1).

Rysunek 1. Schemat prezentujący algorytm analizujący geometrię twarzy



Źródło: aleBank.pl, https://alebank.pl [dostęp: 11.07.2020].

Wysoki poziom złożoności zagadnienia sprawia, że może być ono przedstawione w skrajnie odmiennym świetle, w zależności od wrażenia jakie ma zostać wywarte na odbiorcy. Należy przy tym zwrócić uwagę na fakt, że taka możliwość manipulowania emocjami społecznymi pozwala na wykorzystanie tego zjawiska do własnych celów. Zatem niezwykle istotne jest przedstawienie omawianej materii w sposób możliwie najbardziej obiektywny, bazując na dowiedzionych faktach, prowadzonych badaniach, odcinając się zaś od niesprawdzonych źródeł, których motywacje i zaangażowanie może być kwestionowane.

Mając powyższe na uwadze, niezmiernie istotne jest ustanowienie szczegółowych przepisów prawa definiujących poszczególne elementy rozpoznawanej płaszczyzny. W nawiązaniu do uprzednio przytoczonego zapisu rozporządzenia o ochronie danych osobowych, należy dodać, że aby możliwe było zaliczenie rozpatrywanych

[5] *Biometria* [hasło], ekologia.pl, https://www.ekologia.pl/wiedza/slowniki/leksykon-ekologii-i-ochrony-srodowiska/biometria [dostęp: 2.05.2020].

danych do danych biometrycznych, konieczne jest spełnienie przez nie jednocześnie wszystkich opisanych powyżej warunków. Winny one zatem wynikać ze specjalnego przetwarzania technicznego, dotyczyć zdefiniowanych cech osoby fizycznej oraz umożliwiać albo potwierdzać jednoznaczną identyfikację danej osoby. W przypadku gdy chociaż jeden z tych warunków nie zostanie spełniony, oznaczać to będzie, że przetwarzana dana osobowa nie może być postrzegana jako dana biometryczna[6].

Najczęściej przytaczaną i, jak się wydaje, najbardziej trafiającą do świadomości przeciętnego odbiorcy jest definicja *Słownika Języka Polskiego*, według której biometria to „nauka zajmująca się badaniem prawidłowości kierujących zmiennością cech populacji organizmów żywych, posługująca się metodami statystyki matematycznej" lub też, w najprostszym ujęciu, jest to „technika dokonywania pomiarów istot żywych"[7].

Rodzaje systemów biometrycznych

Identyfikacja jednostki w oparciu o jej charakterystyczne cechy nie jest pomysłem nowym. Dążenia do opracowania systemu pozwalającego na takie działania sięgają początków ludzkości. Najstarsze źródła pisane odnoszą się do rozpoznawania przez naszych przodków przyjaciół lub wrogów w oparciu o ich wizerunek. Przyjęte wówczas metody sprawdzały się w małych społecznościach, jednak wraz z rozwojem aglomeracji i wzrostem liczby ludności stawały się one coraz bardziej zawodne. Brak technicznych możliwości do gromadzenia pozyskiwanych informacji i zawodność pamięci ludzkiej sprawiły, że już w okresie starożytnym cywilizacje Dalekiego Wschodu podjęły próby stworzenia systemu pozwalającego na weryfikację tożsamości za pomocą innych narzędzi, które miały być skuteczniejsze niż samo rozpoznawanie twarzy.

Analizując historię rozwoju biometrii natrafiamy na przypadki wykorzystania wzorów linii papilarnych znajdujących się na ludzkim ciele. Odbitki kciuków znajdywano na glinianych tablicach i ceramicznych naczyniach pochodzących ze starożytnego Babilonu, datowanych na ok. 2000 lat (rys. 2) p.n.e.[8]

Odbitki linii papilarnych pozostawiano na glinianych tabliczkach, aby zalegalizować podejmowane przez siebie kroki prawne. Najczęściej dotyczyło to transakcji handlowych, ale zdarzało się, że również decyzje wydawane przez organy administracyjne były sygnowane w taki sposób. Podobne praktyki stosowano chociażby w Chinach, gdzie zdawano sobie sprawę ze zindywidualizowanych właściwości organizmu[9].

---

6 LexDigital, *Dane biometryczne. Ochrona szczególnej kategorii danych*, 11.06.2018, https://lexdigital.pl/dane-biometryczne-ochrona-szczegolnej-kategorii-danych [dostęp: 2.05.2020].

7 *Biometria* [hasło], [w:] *Słownik Języka Polskiego*, PWN, https://sjp.pwn.pl/slowniki/biometria.html [dostęp: 2.05.2020].

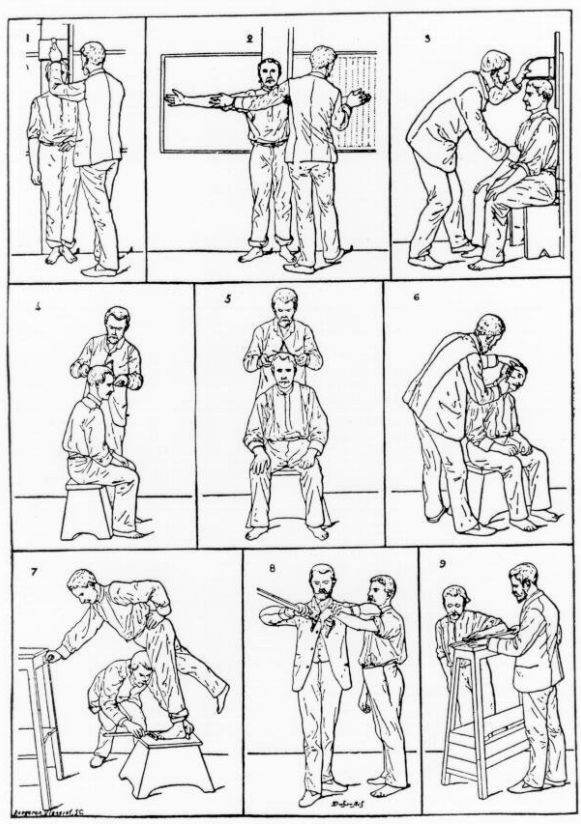
8 D. Powęda, *Biometria – rewolucja czy ewolucja?*, „Nowoczesny Bank Spółdzielczy" 2015, nr 9, s. 110–115, https://test.alebank.pl/wp-content/uploads/2015/09/nbs.2015.09.110-115.pdf [dostęp: 2.05.2020].

9 *Daktylopskopia* [hasło], kryminalistyka.fr.pl/, http://www.kryminalistyka.fr.pl/crime_daktyloskopia.php [dostęp: 2.05.2020].

Rysunek 2. Gliniane tabliczki, których powstanie datuje się na ok. 2000 lat p.n.e., z odwzorowanymi liniami papilarnymi

Źródło: E. Saeed, J. Konopińska, Z. Mariak, K. Saeed, *Zastosowanie wzorca tęczówki i siatkówki oka w procedurach identyfikacji człowieka i wpływ chorób na zaburzenie tego wzorca*, „Klinika Oczna" 2017, t. 19, nr 2, s. 121, DOI: 10.5114/ko.2017.71783.

Rysunek 3. Zestaw pomiarów antropometrycznych wg Alphonse'a Bertillona



Źródło: *Alphonse Bertillon*, Sprawy detektywa Murdocha, 24.07.2010, http://detektywmurdoch.blogspot.com/2010/07/alphonse-bertillon.html [dostęp: 19.07.2020].

Francuski uczony Alphonse Bertillon w XIX w. opracował autorski system identyfikacyjny. *Bertillonage* to system antropometryczny oparty na analizie korelacji odległości poszczególnych części ludzkiego ciała[10] (rys. 3). W toku badań uczonemu udało się dowieść, że wyniki pomiarów różnią się w zależności od badanego obiektu, co w konsekwencji pozwalało mu na tworzenie kartotek osób podejrzewanych o popełnienie przestępstwa. Służyły one następnie francuskim organom ścigania, w szeregach których znajdowali się wyszkoleni odpowiednio funkcjonariusze, posiłkujący się tymi danymi w toku prowadzonych przez siebie postępowań.

Milowym krokiem w rozwoju biometrii było wykorzystanie na szeroką skalę odbitek linii papilarnych. Choć, jak już wykazano, technika ta znana była od tysięcy lat, to dopiero w XIX w. udoskonalono i upowszechniono ją w stopniu pozwalającym na jej wykorzystanie w codziennym życiu[11]. Henry Faulds zdefiniował i dokonał charakterystyki trzech podstawowych typów układów linii papilarnych występujących na ludzkich palcach. Równolegle William Herschel udowodnił, że linie te ułożone są u każdego człowieka w sposób nieco inny, co oznacza, że są indywidualne i niepowtarzalne. Pogląd ten funkcjonował w przestrzeni naukowej przez kilkadziesiąt lat, aż do chwili, gdy możliwości techniczne pozwoliły na szczegółową analizę milionów pobranych wzorów linii papilarnych, co w konsekwencji rzuciło nieco inne światło na ich niepowtarzalność.

W 1892 r. Francis Galton, uchodzący za twórcę daktyloskopii jako takiej, zebrał i usystematyzował całość ówczesnej wiedzy. Z owoców jego badań korzystają do dnia dzisiejszego organy ścigania większości państw[12]. Z biegiem lat również sądy zaakceptowały uzyskiwany w ten sposób w toku prowadzonych postępowań przygotowawczych materiał dowodowy. Fakt ten stanowił podwalinę pod dynamiczną ewolucję urządzeń wykorzystujących identyfikację właściciela poprzez weryfikację zapisanego w pamięci wzoru linii papilarnych[13].

Czytniki linii papilarnych stały się nie tylko popularne, ale i mobilne, co umożliwiło ich masowe użycie w wielu typach urządzeń stosowanych każdego dnia przez miliony użytkowników (rys. 4).

Inną formą badania biometrycznego jest badanie geometrii dłoni. Polega ono na uzyskaniu szeregu wielkości poprzez zmierzenie odległości pomiędzy poszczególnymi punktami, uprzednio naniesionymi na tę część ciała. Specjalnie umiejscowiona kamera wykonuje zdjęcie znajdującej się w ściśle określonej pozycji dłoni, po czym porównuje je z innymi fotografiami znajdującymi się w bazie danych.

Pionierskie badanie tego typu wykonał w 1985 r. David Sidlauskas i niemal od razu zdobyło ono uznanie światowych ekspertów. Okazało się, że stosowana wówczas geometria 2D, oraz rozwinięta na przestrzeni kolejnych lat geometria 3D, jest na tyle unikatowa i spełnia niezbędne kryteria danych biometrycznych, że

---

[10] A. Bertillon, *Identification anthropométrique: Instructions signalétiques, Imprimerie administrative*, Imprimerie Administrative, Melun 1893, s. 12.

[11] *Zasada 3N Francisa Galtona*, 25.02.2018, minnie-kryminalistka.pl, https://minnie-kryminalistka.pl/zasada-3n-francisa-galtona [dostęp: 16.04.2020].

[12] Cz. Grzeszyk, *Daktyloskopia*, Wydawnictwo Naukowe PWN, Warszawa 1992, s. 9.

[13] K. Janicki, *Kryminalistyka w historii. Metody detektywistyczne w Polsce*, „Newsweek", 29.04.2017, https://www.newsweek.pl/wiedza/historia/kryminalistyka-w-historii-metody-detektywistyczne-w-polsce/rnt4cyq [dostęp: 12.04.2020].

w niedługim czasie zaczęła ona być wykorzystywana w systemach bezpieczeństwa wielu podmiotów[14].

Wśród licznych zalet tej metody wymienić można niską inwazyjność, szybkość wykonania badania i duży poziom wiarygodności. Największą jej wadą jest natomiast fakt, że wymiary dłoni, jak i wszelkie inne parametry ją opisujące zmieniają się na przestrzeni czasu, co powoduje, że bazy danych są aktualne tylko w odstępie relatywnie niedługiego czasu[15]. Metoda ta jest stosowana najczęściej w czytnikach zabezpieczających dostęp do lokacji o strategicznym znaczeniu (rys. 5).

Rysunek 4. Przykład ultramobilnego zastosowania czytnika linii papilarnych w pamięci przenośnej USB

Źródło: J. Brzeziński, *Nowa pamięć USB 3.0 flash firmy Lexar wykorzystuje linie papilarne do zabezpieczenia zdjęć*, InterFoto, 23.10.2018, http://blog.interfoto.eu/2018/10/23/nowa-pamiec-usb-3-0-flash-firmy-lexar-wykorzystuje-linie-papilarne-do-zabezpieczenia-zdjec [dostęp: 19.08.2020].

Rysunek 5. Czytnik geometrii dłoni najnowszej generacji Handkey II firmy Recognition Systems Inc.

Źródło: AutoID Polska, Produkty. HandKey II, https://www.autoid.pl/produkty/automatyczna-identyfikacja-osob/czytniki-geometrii-dloni/188-handkey-ii [dostęp: 21.10.2020].

[14] Homeland Security, Biometrics, http://www.biometrics.gov/Documents/handgeometry.pdf [dostęp: 18.04.2020].

[15] T. Kulas, *Rodzaje technologii biometrycznych*, „MIT Sloan Management Review", https://mitsmr.pl/trendy/cyberbezpieczenstwo/rodzaje-technologii-biometrycznych [dostęp: 25.04.2020].

Równie zaawansowane rozwiązania zastosowano w skanerach układu naczyń krwionośnych. Zasada ich działania polega na wykorzystaniu, w celu identyfikacji lub weryfikacji, systemu naczyń krwionośnych i detekcji występujących różnic osobniczych – głównie wielkości i umiejscowienia naczyń krwionośnych, które znacząco różnią się u każdego człowieka.

Czytnik naczyń krwionośnych wyposażony jest w emiter światła podczerwonego, który umożliwia ujawnienie układu żył, po czym utrwala go na zdjęciu[16] (rys. 6). Jest ono następnie analizowane pod kątem ewentualnej zbieżności z innymi znajdującymi się w bazie danych obrazami.

Rysunek 6. Jeden z wielu rodzajów czytników układu naczyń krwionośnych

Źródło: *Biometria naczyniowa – skanery układu naczyń krionośnych słoni w systemach biometrycznych*, WebsterSystem™. Blog – Nowoczesne Technologie, 26.08.2011, https://blog.weber-systems.pl/biometria-naczyniowa [dostęp: 23.09.2020].

Technologia ta znalazła spore grono zwolenników, co wynika z jej niepodważalnych zalet w postaci braku możliwości podrobienia analizowanej struktury oraz faktu, że przedmiotowa analiza pozwala na pozyskanie dodatkowych, niezwiązanych z weryfikacją informacji, takich jak żywotność badanego obiektu, poprzez obliczenie przepływu krwi w jednostce czasu[17].

---

[16] P. Niedziejko, I. Krysowaty, *Biometria – Charakterystyka danych człowieka (cz. 2)*, „Zabezpieczenia", 12.10.2006, https://www.zabezpieczenia.com.pl/biometria/biometria-charakterystyka-danych-cz%C5%82owieka-cz-2 [dostęp: 15.10.2020].

[17] Ł. Michalik, Fujitsu PalmSecure – układ krwionośny w roli osobistego klucza, gadzetomania.pl, https://gadzetomania.pl/57049,fujitsu-palmsecure-uklad-krwionosny-w-roli-osobistego-klucza [dostęp: 17.04.2020].

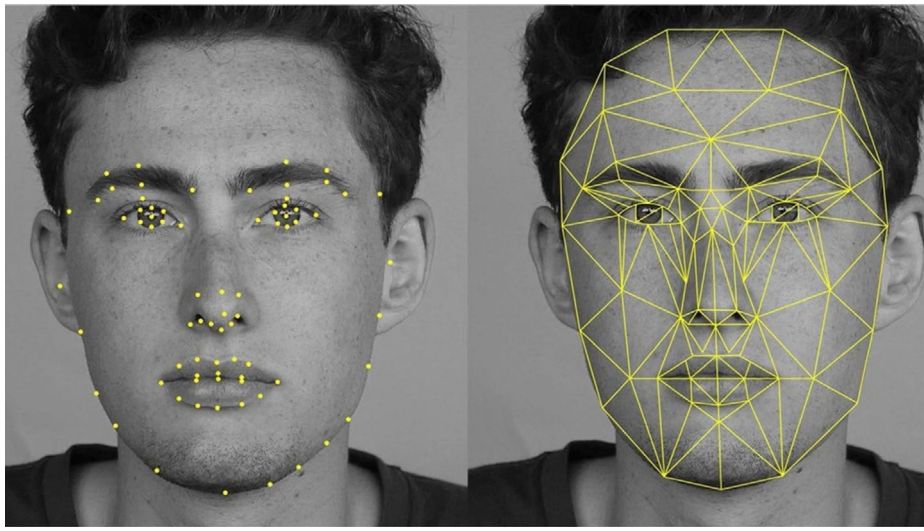
Istotną kwestią jest ponadto trwałość analizowanego czynnika. Układ naczyń krwionośnych nie zmienia się z wiekiem; wyniku badania nie zafałszuje także powierzchowna rana czy opuchlizna[18]. Przez wzgląd na powyższe oraz, dodatkowo, relatywnie niewielki koszt zastosowania tej technologii w różnego rodzaju urządzeniach wymagających niejednokrotnie wielostopniowego uwierzytelnienia, wiele podmiotów zdecydowało się na jej zastosowanie w oferowanych przez siebie produktach.

W Polsce już od wielu lat czytniki układu naczyń krwionośnych są stosowane w bankomatach, stanowiąc zabezpieczenie główne lub uzupełniające w przypadku jednoczesnego korzystania przez firmy nimi zarządzające z innych systemów bezpieczeństwa[19].

Najstarszym znanym ludzkości sposobem identyfikacji jest rozpoznawanie twarzy. O ile proces ten wydaje się prosty i w miarę skuteczny, o tyle na jego wydajność wpłynąć może wiele czynników i okoliczności, na które identyfikujący nie ma wpływu wcale lub jest on znacząco ograniczony.

Skanery dedykowane do analizy geometrii twarzy wykorzystywane są jako zabezpieczenie dostępu do istotnych lokacji, także w miejscach użytku publicznego, takich jak lotniska czy ulice miast (rys. 7).

Rysunek 7. Analiza geometrii twarzy z wykorzystaniem skanera



Źródło: J. Markiewicz, *Rozpoznawanie twarzy na zdjęciach – jak to się dzieje?*, android.com.pl, 5.08.2019, https://android.com.pl/aplikacje/250525-rozpoznawanie-twarzy-na-zdjeciach [dostęp: 23.09.2020].

---

[18] M. Tomaszewska-Michalak, *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warszawa 2015, s. 20.

[19] *Biometria w bankowości. Tak korzystają z niej Polacy*, money.pl, 2.02.2013, https://www.money.pl/gospodarka/wiadomosci/artykul/biometria;w;bankowosci;tak;korzystaja;z;niej;polacy,199,0,1244359.html [dostęp: 21.03.2020].

Czynnikiem komplikującym rozpoznanie jednostki po jej twarzy jest wysoki stopień zmian mogących mieć miejsce w zależności od upływu czasu lub, chociażby, od subiektywnie postrzeganych warunków wpływających na percepcję obserwatora, niezależnie od tego czy jest to żywa osoba czy też urządzenie do tego zaprojektowane[20].

Nie sposób ponadto nie zwrócić uwagi na aspekt zawodności pamięci ludzkiej, co w zestawieniu z upływającym czasem (który okazuje się być kluczowym faktorem w przypadku niemal każdej metody identyfikacyjnej) znacząco zwiększa ryzyko pomyłki[21]. Mając na uwadze powyższe, już w latach 60. XX w. zaprojektowano i wykonano pierwsze urządzenia skanujące. Były one z początku wysoce niedoskonałe, ale z biegiem czasu procesy identyfikacyjne w ich wykonaniu stały się względnie dokładne.

W dużym uproszczeniu można przyjąć, że biometryczne skanowanie twarzy bazuje na technologii badającej geometrię przestrzenną głowy i naniesionej na nią siatki punktów charakterystycznych. Jest metodą całkowicie nieinwazyjną, która może być stosowana nawet ze znacznej odległości. Z punktu widzenia systemów bezpieczeństwa publicznego jest to zaleta, natomiast w kontekście zabezpieczeń biznesowych – raczej wada. Do wad zaliczana jest także stosunkowo duża podatność na manipulację, nawet w przypadku skanowania trójwymiarowego głowy[22].

Pomimo ewidentnych niedoskonałości, skanowanie twarzy w celach identyfikacji zostało względnie dobrze przyjęte przez stronę społeczną. Jest to metoda mało inwazyjna, o istnieniu której większość ludzi nie do końca zdaje sobie sprawę, a jednocześnie dość szeroko stosowana, choćby poprzez wprowadzenie zdjęć biometrycznych do dokumentów[23].

Z czasem technologia posunęła się na tyle, że kolejne sposoby pozyskiwania danych biometrycznych stawały się dalece bardziej wysublimowane. Wizje sztabów specjalistów pracujących nad coraz to bardziej zaawansowanymi technicznie projektami były śmielsze, zahaczając z czasem o przestrzeń zarezerwowaną jeszcze kilkanaście lat temu dla autorów powieści z gatunku *science-fiction*.

Jednym z przykładów nieskończonej inwencji naukowców jest niewątpliwie pomysł identyfikacji i weryfikacji ludzi na podstawie ich oczu. Metoda ta bazuje na badaniu i analizie dwóch parametrów. Jedną z nich jest możliwość pomiaru wzoru tęczówki kolorowej części oka (rys. 8). Wzory tęczówki różnią się między poszczególnymi ludźmi (nawet bliźniętami jednojajowymi), a nawet między lewym i prawym okiem. To skuteczna, dobrze dopracowana metoda, więc wykorzystuje się ją zarówno do identyfikacji, jak i weryfikacji osób. Ma jednak pewne ograniczenia: urządzenia do pomiaru są dość kosztowne, a sam proces badania spotyka się z niechęcią badanych osób[24].

---

20 *Biometria. Wykład 2. Cechy biometryczne: twarz*, Wydział Fizyki i Informatyki Stosowanej AGH–Małopolska Chmura Edukacyjna, http://home.agh.edu.pl/~jsw/MCE/Face.pdf [dostęp: 24.04.2020].

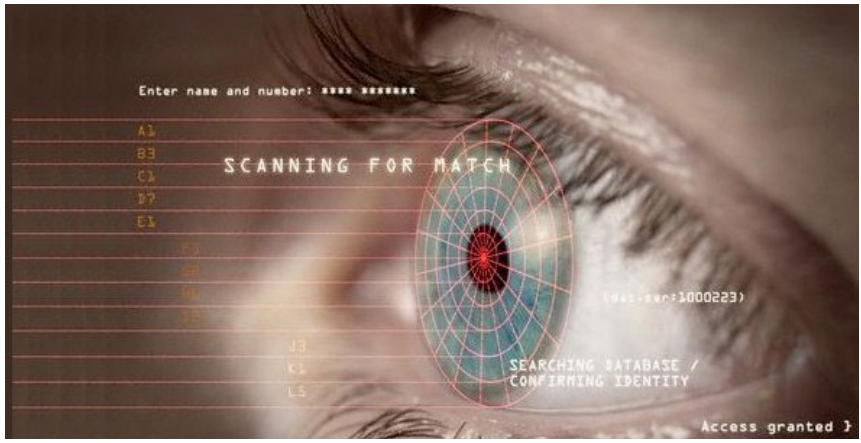
21 M. Usidus, *Biometria współcześnie. Czy te oczy mogą kłamać?*, „Młody Technik", https://mlodytechnik.pl/technika/29045-biometria-wspolczesnie-czy-te-oczy-moga-klamac [dostęp: 16.06.2020].

22 T. Kulas, *op. cit.*

23 *Analiza biometryczna pokaże reakcje klientów*, cc.news.pl, 20.11.2017, https://ccnews.pl/2017/11/20/analiza-biometryczna-pokaze-reakcje-klientow [dostęp: 25.04.2020].

24 A. Bełcik, *Transakcję zatwierdzi tęczówka oka*, „Puls Biznesu", 23.01.2018, https://www.pb.pl/transakcje-zatwierdzi-teczowka-oka-903857 [dostęp: 29.04.2020].

Rysunek 8. Pozyskiwanie danych poprzez analizę tęczówki oka



Źródło: D. Kucharski, *Skaner tęczówki oka to przyszłość dla smartfonów Samsunga*, gsmManiaK.pl, 4.08.2016, https://www.gsmmaniak.pl/571248/samsung-skaner-teczowki-sredniakow [dostęp: 25.09.2020].

Największą zaletą stosowania tego parametru jest fakt, że tęczówka oka kształtuje się podczas życia płodowego i nie zmienia się aż do śmierci. Do samego procesu identyfikacji, który jest nieinwazyjny i szybki, nie trzeba nawet zdejmować szkieł kontaktowych czy okularów. Eksperci uznają, że skanowanie tęczówki oka jest jedną z najbezpieczniejszych i najbardziej wiarygodnych metod pozyskiwania danych biometrycznych[25].

Metodą drugą, niejako zbliżoną do zdejmowania skanu tęczówki, jest skanowanie siatkówki oka, która jest jego wewnętrznym elementem, jednocześnie wrażliwym na bodźce zewnętrzne, takie jak chociażby światło i jego natężenie[26].

Sam pomiar polega na skierowaniu na tę część oka strumienia światła celem wykonania zdjęcia unikalnej dla każdego człowieka struktury naczyń krwionośnych umiejscowionych na jego dnie, a następnie na analizie uzyskanego w ten sposób wzoru i porównaniu go do zbiorów podobnych, znajdujących się w bazach danych zainteresowanych instytucji[27].

Innym sposobem identyfikacji jednostki na podstawie unikatowych parametrów jej organizmu jest analiza struktury opuszka palca (rys. 9). Metoda ta, często błędnie utożsamiana z analizą odbitki linii papilarnych, została wynaleziona i opatentowana przez małą firmę PosID, specjalizującą się w rozwoju identyfikacji termalnej (*Thermal-ID*).

Technika ta polega na skanowaniu wiązką promieni podczerwonych, dzięki

---

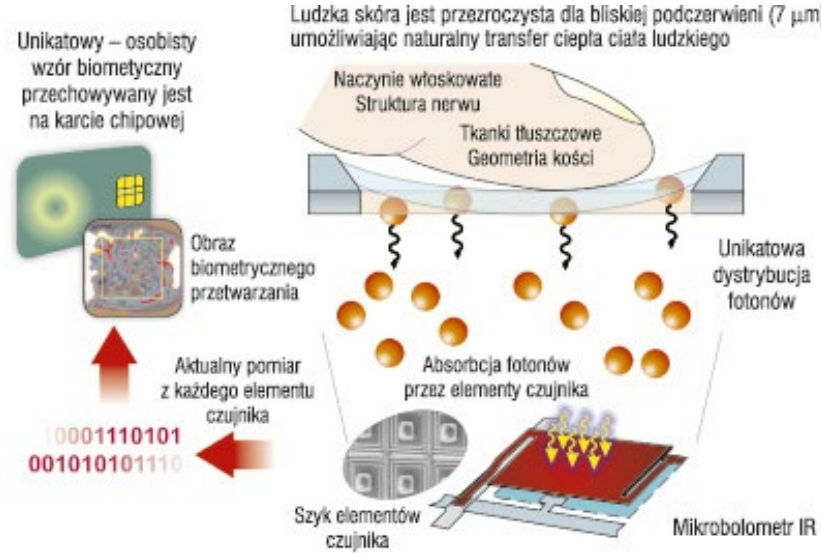
[25] M. Piotrowski, *Biometr w firmie*, „Computerworld", 7.12.2012, https://www.computerworld.pl/news/Biometria-w-firmie,387406.html [dostęp: 30.04.2020].

[26] https://www.doctormed.pl/info/okulistyka/siatkowka-lac-retina [dostęp: 13.03.2020].

[27] E. Saeed, J. Konopińska, Z. Mariak, K. Saeed, *Zastosowanie wzorca tęczówki i siatkówki oka w procedurach identyfikacji człowieka i wpływ chorób na zaburzenie tego wzorca*, „Klinika Oczna" 2017, t. 19, nr 2, s. 120–126, DOI: 10.5114/ko.2017.71783.

czemu uzyskuje się unikatowy obraz wewnętrznej struktury opuszka palca, co eliminuje wiele ograniczeń oraz możliwość oszustw przy rozpoznawaniu odcisku palca w biometrycznym uwierzytelnianiu[28]. W przypadku odcisku palca może np. dojść do jego niewielkiego mechanicznego uszkodzenia lub chociażby zabrudzenia, co skutkować będzie brakiem możliwości identyfikacji jednostki.

Rysunek 9. Proces weryfikacji tożsamości poprzez analizę struktury opuszka palca



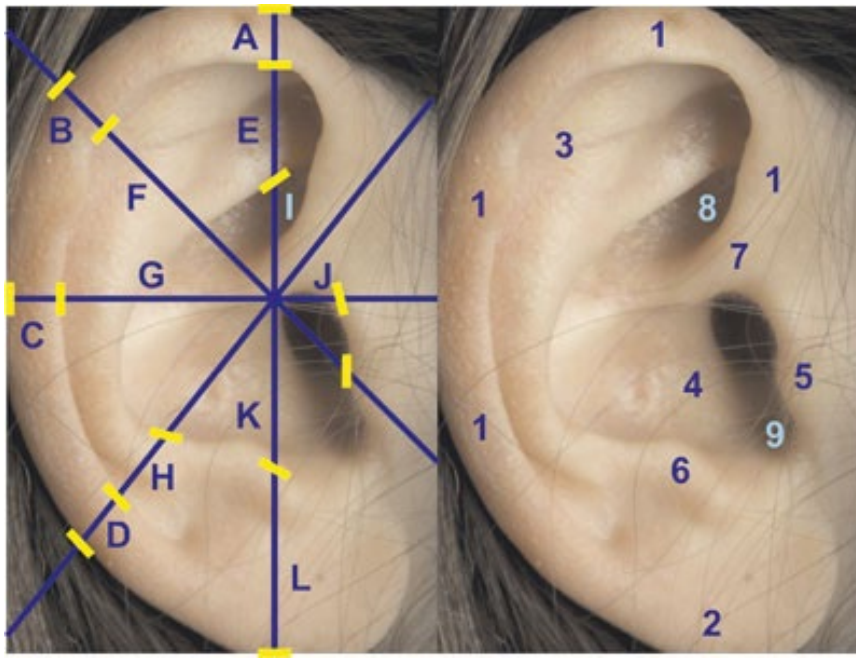
Źródło: P. Niedziejko, I. Krysowaty, *Biometria – Charakterystyka danych człowieka (cz. 2)*, „Zabezpieczenia", 12.10.2006, https://www.zabezpieczenia.com.pl/biometria/biometria-charakterystyka-danych-cz%C5%82owieka-cz-2 [dostęp: 15.10.2020].

Omawiany proces nie polega w tym przypadku na stwierdzeniu zgodności wizualnej i optycznym dopasowywaniu wzorca, co ma miejsce w przypadku większości technik biometrycznego uwierzytelniania. Zamiast tego technika PosID odwzorowuje na „mapie" poziomy energetyczne emanujące od osobnika bezpośrednio na czujnik podczerwieni i dokonuje porównania wcześniej zarejestrowanej, przechowywanej w bazie danych mapy energii, z mapą uzyskaną w procesie uwierzytelniania. Według dostępnych danych weryfikacja odbywa się w czasie nie dłuższym niż trzy sekundy. Biometryczna technologia PosID jest bezinwazyjna i eliminuje praktycznie ryzyko kradzieży tożsamości[29].

[28] P. Niedziejko, I. Krysowaty, *op. cit*.

[29] Optel, *Odczytywanie struktury linii papilarnych za pomocą kamery ultradźwiękowej*, http://www.optel.eu/article/polska/art.html [dostęp: 23.07.2020].

Rysunek 10. Niepowtarzalność struktury ucha



Źródło: P. Niedziejko, I. Krysowaty, *op. cit.*

Kolejnym sposobem identyfikowania ludzi jest analiza struktury ucha (rys. 10). Zagadnienie to budziło zainteresowanie już sto lat temu. Na łamach literatury przedmiotu toczy się nieustannie dyskusja dotycząca tego, czy rzeczywiście uszy są wystarczająco niepowtarzalne albo dość specyficzne, aby być przedmiotem cennym w kontekście pozyskiwania danych biometrycznych. Aplikacje wykorzystujące algorytmy bazujące na rozpoznaniu unikatowych cech ucha nie są jeszcze powszechnie stosowane, ale budzą rosnące zainteresowanie wśród osób zajmujących się wieloma dziedzinami życia[30]. Poza służbami odpowiadającymi za szeroko pojęte bezpieczeństwo, algorytmy te wykorzystują np. historycy, którzy na podstawie wizerunków postaci historycznych starają się ustalić potencjalne więzy pomiędzy członkami rodów, czy też dążą do identyfikacji poszczególnych osób.

W 1989 r. Alfred Iannarelli w swojej najbardziej znanej publikacji dotyczącej identyfikowania ucha pt. *Ear Identification. Forensic Identification Series* wykazał, że wśród ponad 10 tys. przebadanych przez niego uszu wszystkie były różne, a więc pozwalały na identyfikację osoby bez wątpliwości, co do ewentualnych pomyłek w toku przeprowadzonej analizy. Okazało się, że nawet bliźnięta jednojajowe mają cechy fizjologiczne ucha podobne, ale nie identyczne[31].

[30] M. Usidus, *op. cit*.

[31] M. Rahman, R. Islam, N.I. Bhuiyan, B. Ahmed, A. Islam, *Person Identification Using Ear Biometrics*, „The International Journal of the Computer, the Internet and Management" 2007, vol. 15, s. 1–8, https://www.semanticscholar.org/paper/Person-Identification-Using-Ear-Biometrics-Rahman-Islam/403f3d3e47343aa5322b6886e8a9b9ebd4b67a04?p2df [dostęp: 13.07.2020].

Bardzo dobrze rokują na przyszłość systemy wykorzystujące pomiary obrazu termalnego ucha. Są to rozwiązania, które pozwalają uniknąć problemów związanych z koniecznością odpowiedniej ekspozycji ucha podczas procesu identyfikacji. Istnieje również metoda akustycznego rozpoznawania ucha. Pomiar akustycznych właściwości może być dokonany stosunkowo łatwo i ekonomicznie.

Udowodniono, że zachodzi znaczna różnica pomiędzy własnościami akustycznymi uszu różnych osobników. Dlatego też tego rodzaju rozpoznawanie ucha i uzyskiwanie wzorca biometrycznego może zastąpić kod PIN m.in. w telefonach komórkowych, albo umożliwić automatyczną personalizację słuchawek i innego wyposażenia akustycznego. Dodatkowa korzyść płynąca z tej metody to utrudnienie ewentualnej kradzieży wzorca biometrycznego[32].

Biometria głosowa opiera się na wyjątkowości i niepowtarzalności ludzkiego głosu. Wykorzystuje zarówno cechy fizyczne, jak i behawioralne mowy: akcent, szybkość mówienia czy sposób wysławiania się, dzięki czemu umożliwia weryfikację tożsamości osoby mimo np. chorób gardła czy hałasu z otoczenia. *Voiceprint* to matematyczny model wzorca głosu, który tworzony jest na podstawie nagrania, odpowiednio opisujący jego parametry[33].

Autoryzacja głosem jest stosowana w przypadku wielu podmiotów, zarówno komercyjnych, jak i tych wchodzących w szeroko pojęte struktury bezpieczeństwa państwa. W Polsce Krajowa Informacja Podatkowa zamierzała identyfikować dzwoniących podatników za pomocą głosu, jednak uruchomienie tego projektu zostało wstrzymane ze względu na zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych (GIODO)[34]. Kwestie prawne stanowią jednak oddzielny obszar rozważań o technologiach biometrycznych.

Tymczasem firma Unico Software opracowała system biometrycznego rozpoznawania i weryfikacji głosu – VoicePass. W pracach pomagali naukowcy z Akademii Górniczo-Hutniczej w Krakowie. System pozwala przyporządkować do głosu jednego człowieka kilka tysięcy atrybutów, dzięki czemu głos ten może zostać rozpoznany nawet wtedy, kiedy np. nieco zmieni się w wyniku choroby[35].

Podsumowanie

Zagadnienie biometrii w kontekście bezpieczeństwa państwa otwiera niewątpliwie zupełnie nową przestrzeń do dyskusji. Przestrzeń ta była dotychczas marginalizowana, a jej omówienie i zrozumienie jest niezbędne do zapewnienia kompleksowo postrzeganej zdolności obronnej Rzeczypospolitej Polskiej. W tym właśnie zakresie przeprowadzone badania są niezwykle wartościowe.

---

[32] R. Anderson, *Inżynieria zabezpieczeń*, tłum. P. Carlson, WNT, Warszawa 2005.

[33] *Rozpoznawanie mówcy na podstawie głosu najważniejszym trendem na rynku biometrii*, ccnews.pl, 8.11.2017, https://ccnews.pl/2017/11/08/rozpoznawanie-mowcy-na-podstawie-glosu-najwazniejszym-trendem-na-rynku-biometrii [dostęp: 16.06.2020].

[34] T. Jurczak, *Biometria: Analiza głosu oznacza koniec haseł i PIN-ów*, „Dziennik Gazeta Prawna", 9.03.2016, https://serwisy.gazetaprawna.pl/poradnik-konsumenta/artykuly/926561,analiza-glosu-biometria-giodo-ochrona-danych.html#icwcv=15 [dostęp: 15.07.2020].

[35] R. Fabisiak, *Biometria pełną gębą*, „Puls Biznesu", 28.05.2014, https://www.pb.pl/biometria-pelna-geba-757018 [dostęp: 28.05.2020].

Omówione w tej części zagadnienia stanowią zatem swego rodzaju wstęp do dalszych rozważań, które jawią się jako próba odpowiedzi na pytania o bezkrytyczne podejście do szerokiego stosowania niedostatecznie poznanych technologii. Sama ich natura nie jest bezpośrednio związana z aspektami technicznymi, jednak – przez wzgląd na interdyscyplinarność oraz wielopłaszczyznowość zagadnienia – aspekty te należało objaśnić, co pozwoliło również zobrazować wpływ dynamiki rozwoju i ewolucji technologii biometrycznych na poziom bezpieczeństwa w kontekście braku możliwości przeprowadzenia wystarczająco wyczerpującej analizy zagrożeń wynikających z takiego stanu rzeczy[36].

Część druga artykułu stanowić będzie omówienie kolejnych aktualnie wykorzystywanych technologii biometrycznych.

Bibliografia

aleBank.pl, https://alebank.pl [dostęp: 11.07.2020].

Alphonse Bertillon, Sprawy detektywa Murdocha*,* 24.07.2010, http://detektywmurdoch.blogspot.com/2010/07/alphonse-bertillon.html [dostęp: 19.07.2020].

Analiza biometryczna pokaże reakcje klientów, cc.news.pl, 20.11.2017, https://ccnews.pl/2017/11/20/analiza-biometryczna-pokaze-reakcje-klientow [dostęp: 25.04.2020].

Anderson R., *Inżynieria zabezpieczeń*, tłum. P. Carlson, WNT, Warszawa 2005.

AutoID Polska*, Produkty*. HandKey II, https://www.autoid.pl/produkty/automatyczna-identyfikacja-osob/czytniki-geometrii-dloni/188-handkey-ii [dostęp: 21.10.2020].

Beal V., *Biometric Data* [hasło], 1.04.2008, Webopedia.com, https://www.webopedia.com/TERM/B/biometric_data.html [dostęp: 26.04.2020].

Bełcik A., *Transakcję zatwierdzi tęczówka oka*, „Puls Biznesu", 23.01.2018, https://www.pb.pl/transakcje-zatwierdzi-teczowka-oka-903857 [dostęp: 29.04.2020].

Bertillon A., *Identification anthropométrique: Instructions signalétiques*, Imprimerie administrative, Melun 1893.

Biometria [hasło], [w:] *Słownik Języka Polskiego*, PWN, https://sjp.pwn.pl/slowniki/biometria.html [dostęp: 2.05.2020].

Biometria [hasło], ekologia.pl, https://www.ekologia.pl/wiedza/slowniki/leksykon-ekologii-i-ochrony-srodowiska/biometria [dostęp: 2.05.2020].

Biometria naczyniowa – skanery układu naczyń krionośnych słoni w systemach biometrycznych, WebsterSystem™. Blog – Nowoczesne Technologie, 26.08.2011, https://blog.weber-systems.pl/biometria-naczyniowa [dostęp: 23.09.2020].

Biometria w bankowości. Tak korzystają z niej Polacy, money.pl, 2.02.2013, https://www.money.pl/gospodarka/wiadomosci/artykul/biometria;w;bankowosci;tak;korzystaja;z;niej;polacy,199,0,1244359.html [dostęp: 21.03.2020].

Biometria. Wykład 2. Cechy biometryczne: twarz, Wydział Fizyki i Informatyki Stosowanej AGH–Małopolska Chmura Edukacyjna, http://home.agh.edu.pl/~jsw/MCE/Face.pdf [dostęp: 24.04.2020].

[36] W. Bolanowski., *Co jest szansą dla (masowej) biometrii w bankach?*, PRNews.pl, 9.02.2015, https://prnews.pl/co-jest-szansa-dla-masowej-biometrii-w-bankach-13107 [dostęp: 18.08.2020].

Bolanowski W., *Co jest szansą dla (masowej) biometrii w bankach?*, PRNews.pl, 9.02.2015, https://prnews.pl/co-jest-szansa-dla-masowej-biometrii-w-bankach-13107 [dostęp: 18.08.2020].

Brzeziński J., *Nowa pamięć USB 3.0 flash firmy Lexar wykorzystuje linie papilarne do zabezpieczenia zdjęć, InterFoto*, 23.10.2018, http://blog.interfoto.eu/2018/10/23/nowa-pamiec-usb-3-0-flash-firmy-lexar-wykorzystuje-linie-papilarne-do-zabezpieczenia-zdjec [dostęp: 19.08.2020].

Daktylopskopia [hasło], kryminalistyka.fr.pl, http://www.kryminalistyka.fr.pl/crime_daktyloskopia.php [dostęp: 2.05.2020].

Fabisiak R., *Biometria pełną gębą*, „Puls Biznesu", 28.05.2014, https://www.pb.pl/biometria-pelna-geba-757018 [dostęp: 28.05.2020].

FBI, *Fingerprints and Other Biometrics*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics [dostęp: 27.04.2020].

Grzeszyk Cz., *Daktyloskopia*, Wydawnictwo Naukowe PWN, Warszawa 1992.

Homeland Security, Biometrics, http://www.biometrics.gov/Documents/handgeometry.pdf [dostęp: 18.04.2020].

https://www.doctormed.pl/info/okulistyka/siatkowka-lac-retina [dostęp: 13.03.2020].

Janicki K., *Kryminalistyka w historii. Metody detektywistyczne w Polsce*, „Newsweek", 29.04.2017, https://www.newsweek.pl/wiedza/historia/kryminalistyka-w-historii-metody-detektywistyczne-w-polsce/rnt4cyq [dostęp: 12.04.2020].

Jurczak T., *Biometria: Analiza głosu oznacza koniec haseł i PIN-ów*, „Dziennik Gazeta Prawna", 9.03.2016, https://serwisy.gazetaprawna.pl/poradnik-konsumenta/artykuly/926561,analiza-glosu-biometria-giodo-ochrona-danych.html#icwcv=15 [dostęp: 15.07.2020].

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

Kucharski D., *Skaner tęczówki oka to przyszłość dla smartfonów Samsunga*, gsmManiaK.pl, 4.08.2016, https://www.gsmmaniak.pl/571248/samsung-skaner-teczowki-sredniakow [dostęp: 25.09.2020].

Kulas T., *Rodzaje technologii biometrycznych*, „MIT Sloan Management Review", https://mitsmr.pl/trendy/cyberbezpieczenstwo/rodzaje-technologii-biometrycznych [dostęp: 25.04.2020].

LexDigital, *Dane biometryczne. Ochrona szczególnej kategorii danych*, 11.06.2018, https://lexdigital.pl/dane-biometryczne-ochrona-szczegolnej-kategorii-danych [dostęp: 2.05.2020].

Markiewicz J., *Rozpoznawanie twarzy na zdjęciach – jak to się dzieje?*, android.com.pl, 5.08.2019, https://android.com.pl/aplikacje/250525-rozpoznawanie-twarzy-na-zdjeciach [dostęp: 23.09.2020].

Michalik Ł., *Fujitsu PalmSecure – układ krwionośny w roli osobistego klucza*, gadzetomania.pl, https://gadzetomania.pl/57049,fujitsu-palmsecure-uklad-krwionosny-w-roli-osobistego-klucza [dostęp: 17.04.2020].

Niedziejko P., Krysowaty I., *Biometria – Charakterystyka danych człowieka (cz. 2)*, „Zabezpieczenia", 12.10.2006, https://www.zabezpieczenia.com.pl/biometria/biometria-charakterystyka-danych-cz%C5%82owieka-cz-2 [dostęp: 15.10.2020].

Optel, *Odczytywanie struktury linii papilarnych za pomocą kamery ultradźwiękowej*, http://www.optel.eu/article/polska/art.html [dostęp: 23.07.2020].

Piotrowski M., *Biometr w firmie*, „Computerworld", 7.12.2012, https://www.computerworld.pl/news/Biometria-w-firmie,387406.html [dostęp: 30.04.2020].

Powęda D., *Biometria – rewolucja czy ewolucja?*, „Nowoczesny Bank Spółdzielczy" 2015, nr 9, https://test.alebank.pl/wp-content/uploads/2015/09/nbs.2015.09.110-115.pdf [dostęp: 2.05.2020].

Rahman M., Islam R., Bhuiyan N.I., Ahmed B., Islam A., *Person Identification Using Ear Biometrics*, „The International Journal of the Computer, the Internet and Management" 2007, vol. 15, https://www.semanticscholar.org/paper/Person-Identification-Using-Ear-Biometrics-Rahman-Islam/403f3d3e47343aa5322b6886e8a9b9ebd4b67a04?p2df [dostęp: 13.07.2020].

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, Dz. Urz. UE L/119 z 4.05.2016.

Rozpoznawanie mówcy na podstawie głosu najważniejszym trendem na rynku biometrii, ccnews.pl, 8.11.2017, https://ccnews.pl/2017/11/08/rozpoznawanie-mowcy-na-podstawie-glosu-najwazniejszym-trendem-na-rynku-biometrii [dostęp: 16.06.2020].

Saeed E., Konopińska J., Mariak Z., Saeed K., *Zastosowanie wzorca tęczówki i siatkówki oka w procedurach identyfikacji człowieka i wpływ chorób na zaburzenie tego wzorca*, „Klinika Oczna" 2017, t. 19, nr 2, DOI: 10.5114/ko.2017.71783.

Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warszawa 2015.

Usidus M., *Biometria współcześnie. Czy te oczy mogą kłamać?*, „Młody Technik", https://mlodytechnik.pl/technika/29045-biometria-wspolczesnie-czy-te-oczy-moga-klamac [dostęp: 16.06.2020].

Zasada 3N Francisa Galtona, 25.02.2018, minnie-kryminalistka.pl, https://minnie-kryminalistka.pl/zasada-3n-francisa-galtona [dostęp: 16.04.2020].

Bezpieczeństwo Rzeczypospolitej Polskiej w kontekście dynamicznego rozwoju technologii biometrycznych. Część I

Streszczenie

Artykuł stanowi wstęp do dyskusji ukierunkowanej na znalezienie odpowiedzi na pytanie o bezpieczeństwo Rzeczypospolitej Polskiej w kontekście zagrożeń płynących z wykorzystywania najnowszych osiągnięć techniki, ze szczególnym naciskiem na technologie biometryczne, które niepostrzeżenie stały się integralną częścią życia większości ludzi. Zachęca on do zgłębienia problemów społecznej świadomości oraz niebezpieczeństw kryjących się w niekontrolowanej retencji, przechowywaniu i wykorzystywaniu danych biometrycznych przez wiele transgranicznych podmiotów komercyjnych oraz przez służby specjalne państw. Rozważania te w szerszej perspektywie pozwolą na wypełnienie luki w literaturze przedmiotu, która niezwykle szczątkowo traktuje o danych biometrycznych. Jeśli już zagadnienie to jest omawiane, to poruszane są zwykle aspekty techniczne, z pominięciem kluczowej kwestii, jaką jest niedostatecznie wnikliwa ocena zagrożenia i brak rozwagi w podejmowaniu strategicznych decyzji kształtujących zdolności obronne państwa w reakcji na potencjalną ingerencję wrogów, tak zewnętrznych, jaki i wewnętrznych, w strategiczne zasoby danych. Istotne jest zatem rozstrzygnięcie, czy

Rzeczpospolita Polska znajduje się w stanie permanentnego zagrożenia informatycznego mającego podłoże w niezrozumieniu zagrożeń i specyfiki omawianej technologii, a także braku wyobraźni osób i podmiotów powołanych do stania na straży bezpieczeństwa narodowego, czy też jest to jedynie problem natury teoretycznej. Przez wzgląd na znaczny zakres materiału, artykuł podzielony został na dwie części, które razem pozwolą na przedstawienie zagadnienia w sposób spójny i wyczerpujący.
Słowa kluczowe: biometria, dane biometryczne, systemy biometryczne, identyfikacja jednostki, antropometria, autoryzacja, biometria behawioralna, bezpieczeństwo narodowe

Security of the Republic of Poland in the Context of the Dynamic Development of Biometric Technologies Abstract

The article is an introduction to a discussion aimed at finding the answer to the question about the security of the Republic of Poland in the context of the threats posed by the use of the latest technological achievements, with particular emphasis on biometric technologies, which have imperceptibly become an integral part of most people's lives. The article encourages the exploration of the problems of public awareness and the dangers of uncontrolled retention, storage and use of biometric data by many cross-border commercial entities and by secret services of various countries. These considerations, in a broader perspective, will allow to fill the gap in the literature on the subject, which is extremely rudimentary about biometric data. Whenever these issues are brought up, technical aspects are usually discussed, with the omission of the key issue, which is a lack of sufficient thoroughness in the assessment of the threat and lack of caution in making strategic decisions shaping the state's defense capabilities in response to potential interference by enemies, both external and internal, in the strategic data resources. Therefore, it is important to decide whether the Republic of Poland is in a state of permanent IT threat arising from the unique characteristics of the technology in question and a misunderstanding of the threats as well as the lack of imagination of people and entities appointed to guard national security, or whether it is only a theoretical problem. Due to the considerable scope of the material, the article has been divided into two parts which together allow for a consistent and comprehensive presentation of the issue.
Key words: biometrics, biometric data, biometric systems, individual identification, anthropometry, authorization, behavioral biometrics, national security

Sicherheit der Republik Polen im Zusammenhang mit der Entwicklung von biometrischen Technologien. Teil 1 Zusammenfassung

Der Artikel ist eine Einleitung zur Diskussion, die darauf ausgerichtet ist, um die Frage nach der Sicherheit der Republik Polen im Zusammenhang mit den Bedrohungen, die bei der Anwendung von neuesten technischen Errungenschaften entstehen, unter besonderer Berücksichtigung von biometrischen Technologien, die unbemerkt zum integralen Teil des Lebens der Mehrheit von Menschen sind, zu beantworten. Durch den Artikel wird man zur Vertiefung der Problemen des Sozialbewusstseins und der, in unkontrollierter Speicherung, Aufbewahrung und Nutzung der biometrischen Daten von vielen grenzüberschreitenden kommerziellen Einrichtungen und Spezialkräften aus anderen Staaten, vorhandenen Gefahren angespornt. Diese Überlegungen erlauben in

der weiteren Perspektive Lücken in der Fachliteratur, die sehr sparsam von den biometrischen Daten handelt, zu füllen. Wenn schon dieses Problem besprochen wird, dann werden gewöhnlich technische Aspekte berührt. Der Kernpunkt des Problems wird übersprungen. Es geht hier um eine nichtausreichend tiefgründige Beurteilung der Bedrohung und um eine Rücksichtslosigkeit beim Treffen von strategischen Entscheidungen, die einen Einfluss auf Verteidigungsfähigkeiten des Staates als eine Reaktion auf einen potentiellen Eingriff vom inneren und äußeren Feind auf strategische Datenressourcen, haben. Wichtig ist also eine Entscheidung zu treffen: befindet sich die Republik Polen in einem ständigen Zustand der Informationsbedrohung, dessen Ursache am Miβverstehen des Problems der Bedrohung und der Besonderheit besprochener Technologie, und auch am Mangel an Vorstellungskraft der für Schutz des nationalen Sicherheitszustandes zuständigen Personen und Einrichtungen liegt oder ist das nur das Problem theoretischer Natur. Auf Grund eines erheblichen Materialumfangs des Artikels, ist er in zwei Teile aufgeteilt, die uns ermöglichen dieses Problem kohärent und ausführlich darzustellen.
Schlüßelwörter: Biometrie, biometrische Daten, biometrische Systeme, Individualindentifizierung, Anthropometrie, Autorisierung, Verhaltensbiometrie, nationale Sicherheit

Безопасность Республики Польша в контексте динамичного развития биометрических технологий. Часть I
Резюме

В статье даётся вступление к дискуссии, направленной на поиск ответа на вопрос о безопасности Республики Польша в контексте угроз, появляющихся в результате использования самых новых достижений техники, а особенно биометрических технологий, которые незаметно стали интегральной частью жизни большинства людей. Статья побуждает к изучению проблем общественного сознания, а также опасности, кроющейся в неконтролируемом сохранении, хранении и использовании биометрических данных многими трансграничными коммерческими субъектами, а также спецслужбами государств. Эти решения в более широкой перспективе позволят заполнить пробелы в соответствующей литературе, в которой пишут о биометрических данных слишком отрывочно. Если их вообще обсуждают, то только технические аспекты, исключая ключевой вопрос, которым является недостаточно внимательная оценка угрозы и неосмотрительность в принятии стратегических решений, формирующих обороноспособность государства в реакции на потенциальное вмешательство врагов, как внешних, так и внутренних, в стратегические базы данных. Существенным является, следовательно, решение, находится ли Республика Польша в состоянии перманентной информационной угрозы, основанной на непонимании угрозы и специфики описываемой технологии, а также недостатка воображения у людей и субъектов, призванных стоять на страже национальной безопасности, или это попросту проблема теории. В связи со значительным объёмом материала статья разделена на части, которые совместно позволяют представить вопрос связно и исчерпывающе.
Ключевые слова: биометрия, биометрические данные, биометрические системы, идентификация личности, антропометрия, авторизация, поведенческая биометрия, национальная безопасность