

dr Magdalena Tomaszewska-Michalak

Wydział Nauk Politycznych i Studiów Międzynarodowych, Uniwersytet Warszawski, Warszawa

ORCID: 0000-0001-5441-0396

PISMO RĘCZNE JAKO CECHA BIOMETRYCZNA CZEŚĆ I

Streszczenie

Celem opracowania jest określenie przynależności pisma ręcznego do cech biometrycznych. W pierwszej części autorka odnosi się do podstawowych zagadnień związanych z możliwością wykorzystania cech jednostki w procesie identyfikacji osoby lub weryfikacji jej tożsamości. W tym celu przybliża historię wdrażania urządzeń biometrycznych oraz podaje przykłady dziedzin, w których obecnie stosuje się metodę rozpoznania osoby na podstawie jej indywidualnych cech. W drugiej części opracowania autorka skupia się na wykorzystaniu podpisu w procesie biometrycznej identyfikacji/weryfikacji tożsamości.

Słowa kluczowe: technologia biometryczna, pismo ręczne, podpis, weryfikacja, identyfikacja

Wstęp

Celem niniejszego opracowania jest określenie przynależności pisma ręcznego do cech o charakterze biometrycznym. Opracowanie podzielone zostało na trzy części. Pierwsza przybliża pojęcia związane z technologią biometryczną oraz wskazuje na właściwości, które pozwalają zaliczyć pismo do kategorii identyfikatorów biometrycznych. W drugiej omówiony został krótko kontekst historyczny związany z rozwojem technologii biometrycznej oraz zalety, które wpływają na coraz powszechniejszy wybór urządzeń biometrycznych jako środka do wzmocnienia bezpieczeństwa. W części tej wskazano również przykładowe obszary, w których wdrażana jest technologia biometryczna. Trzecia część natomiast odwołuje się do możliwości wykorzystania podpisu w charakterze identyfikatora biometrycznego. W tej części wskazane zostały właściwości, jakie daje analiza pomiaru biometrycznego podpisu dla określenia jego autentyczności. Niniejsze opracowanie stanowi pierwszą część analizy dotyczącej wykorzystania pisma ręcznego w charakterze cechy biometrycznej.

Technologia biometryczna w kontekście pisma

Aby określić przynależność pisma ręcznego do cech o charakterze biometrycznym, należy przede wszystkim zacząć od wyjaśnienia pojęcia *biometria*. Zgodnie z definicją słownikową *biometria* jest nauką o badaniu zmienności cech wśród populacji organizmów żywych. Wskazany pomiar odbywa się z wykorzystaniem metod statystyki matematycznej¹. Jako taka biometria wykorzystywana jest od lat, również w kryminalistyce jako narzędzie wspomagające potwierdzenie tożsamości sprawcy zdarzenia. Na założeniu różnorodności właściwości cech ludzkiego ciała opierały się bowiem pierwsze systemy identyfikacyjne współczesnej kryminalistyki, takie jak *bertillonage*² czy daktyloskopia³. Od połowy XX wieku termin biometria zaczął jednak nabierać nowego znaczenia. Stało się to za sprawą rozwoju technologicznego, który pozwolił na automatyzację, a co za tym idzie znaczne przyspieszenie procesu porównywania cech jednostki. Technologię biometryczną można zatem zdefiniować jako technologię wykorzystywaną w celu automatycznej identyfikacji osoby lub weryfikacji jej tożsamości bazującą na porównaniu biologiczno-fizycznych lub behawioralnych cech osoby. Warto pokrótce przybliżyć poszczególne elementy wskazanej definicji. Automatyzm procesu porównania polega na wykorzystaniu odpowiednich algorytmów do identyfikacji/weryfikacji. W ramach systemów w pełni automatycznych oznacza to wyłączenie czynnika ludzkiego i zdanie się jedynie na dokładność algorytmu. W odniesieniu do kryminalistycznych metod uwierzytelniania tożsamości lub identyfikacji osoby biometria często stanowi jedynie pierwszy krok w procesie identyfikacji/weryfikacji. Po wstępnym stwierdzeniu przez urządzenie podobieństwa porównywanych cech to specjaliści podejmują w tym względzie ostateczną decyzję. Przykładem takiego rozwiązania jest system AFIS wspomagający pracę ekspertów policyjnych w zakresie daktyloskopii⁴.

Kolejnym wartym wytłumaczenia pojęciem związanym z technologią biometryczną jest różnica pomiędzy identyfikacją a weryfikacją. Identyfikacja osoby polega na porównaniu prezentowanej cechy (np. linii papilarnych) ze zbiorem cech przechowywanych w bazie danych. Celem porównania jest ujawnienie tożsamości osoby. Na takiej zasadzie działają tzw. *watch lists*, których zadaniem jest ujawnianie tożsamości osób niepożądanych czy poszukiwanych (np. w ramach kontroli na granicy). Podobnym działaniem charakteryzuje się wspomniany wcześniej system AFIS. Weryfikacja tożsamości polega natomiast na porównaniu prezentowanej cechy z wzorcem tejże cechy zapisanym wcześniej na określonym nośniku. Jest to zatem jedynie potwierdzenie, że osoba deklarująca swoją tożsamość jest faktycznie uprawniona do korzystania z systemu (np. w przypadku pobierania gotówki z bankomatu). Różnica pomiędzy weryfikacją a identyfikacją została obrazowo przedstawiona na Ryc. 1.

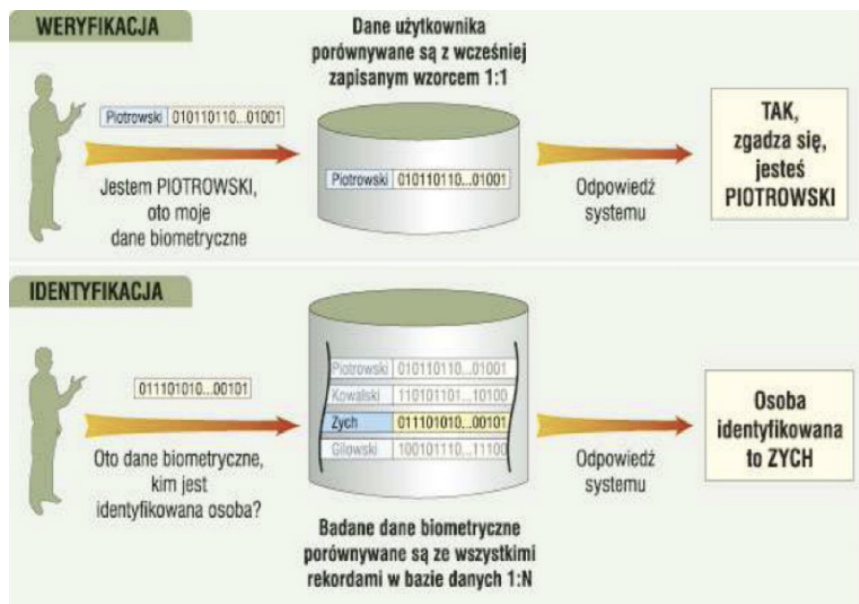
¹ <https://sjp.pwn.pl/>, dostęp 16.06.2021.

² A. Bertillon, *Identification anthropométrique*, Imprimerie Administrative, Melun 1893.

³ C. Grzeszyk, *Daktyloskopia*, Wydawnictwo Naukowe PWN, Warszawa 1992.

⁴ J. Moszczyński, *Z historii polskiej daktyloskopii*, „Studia Prawnoustrojowe” 2014, nr 26.

Ryc. 1. Identyfikacja osoby a weryfikacja tożsamości



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

Kolejnym ważnym punktem koniecznym do pełnego zrozumienia istoty funkcjonowania technologii biometrycznej jest wyjaśnienie, jakie właściwości muszą spełniać cechy jednostki wykorzystywane w procesie identyfikacji/weryfikacji. Porównanie biometryczne bazować może na cechach biologiczno-fizycznych, które związane są z ludzkim organizmem. Jednostka nie ma zatem wpływu na ich kształtowanie się. Obecnie najczęściej wykorzystywanymi cechami biologiczno-fizycznymi są linie papilarne, tęczęwka oka i geometria twarzy. Cechy behawioralne natomiast kształtują się w wyniku powtarzania określonego zachowania, które w konsekwencji prowadzi do zindywidualizowania się danej właściwości. Do tego typu cech zaliczyć można sposób poruszania się czy dynamikę uderzeń w klawiaturę. Wskazane kryteria cechy behawioralnej spełnia również sposób pisania, a przede wszystkim charakterystyka kreślenia podpisu. Niezależnie od rodzaju cechy wykorzystanie technologii biometrycznej zakłada, że powinny się one charakteryzować określonymi właściwościami. Pierwszą z nich jest uniwersalność, która oznacza, że dana cecha musi występować powszechnie w badanej społeczności. Niespełnienie wskazanej przesłanki powoduje, że wykorzystanie biometrii staje się nieskuteczne, gdyż część społeczeństwa nie będzie mogła zostać poddana porównaniu biometrycznemu, a tym samym zaistnieje konieczność poszukiwania alternatywnych metod weryfikacji/identyfikacji. W tym miejscu należy jednakże podkreślić, że uniwersalności nie przeczy sytuacja, w której jedynie niewielki odsetek społeczeństwa nie ma określonej cechy. Może to nastąpić

np. w przypadku wystąpienia choroby czy innych niepożądanych zdarzeń (np. choroby powodujące zanikanie linii papilarnych czy uszkodzenie tęczówki oka). Kolejnym wymaganiem co do właściwości wykorzystywanych cech jest ich unikatowość. Za celem stosowania biometrii stoi bowiem możliwość rozróżnienia jednostek między sobą, co możliwe jest jedynie w sytuacji, gdy porównywane cechy charakteryzują się indywidualnością osobniczą. Trzecią z właściwości, na którą zwraca się uwagę, jest względna niezmienność cechy w czasie. Im bowiem większą stałością wykazuje się dana cecha, tym dłużej jest ona przydatna w procesie identyfikacji/weryfikacji. W przypadku gdy cecha ulega zmianom związanym z upływem czasu, należy pamiętać o konieczności wprowadzenia procedury odnawiania wzorca (np. geometria twarzy). Może to dotyczyć również podpisu. Aby cecha mogła zostać wykorzystana w ramach porównania biometrycznego, musi istnieć również możliwość jej szybkiego i bezinwazyjnego pobrania. Istotne jest też, aby cecha była akceptowalna, co oznacza, że podejście społeczności, która będzie wykorzystywała daną właściwość w procesie identyfikacji/weryfikacji, powinno zostać wcześniej przeanalizowane pod kątem możliwości wdrożenia urządzeń biometrycznych określonego typu. Przykładem braku akceptowalności cechy jest konieczność odsłonięcia twarzy w celu przeprowadzenia porównania biometrycznego w kraju, w którym względy religijne nakazują zasłanianie twarzy.

Pamiętać należy, że nie każda cecha biometryczna (tzw. identyfikator biometryczny) spełnia wszystkie wymienione kryteria (np. obraz twarzy może ulegać zmianom wraz z upływem czasu). Znając jednak właściwości identyfikatora, można starać się niwelować problemy związane z jego biometrycznym wykorzystaniem (np. odnawianie wzorca twarzy po upływie określonego czasu).

Rozpatrując wymienione właściwości w kontekście pisma, a w szczególności podpisu osoby, stwierdzić należy, że z pewnymi zastrzeżeniami spełnia ono większość kryteriów stawianych identyfikatorowi biometrycznemu. Przede wszystkim ma bowiem charakter uniwersalny. Zdecydowana większość społeczeństwa potrafi złożyć podpis. W literaturze wskazuje się, że pismo nosi znamiona indywidualizacji osobniczej⁵. Stwierdzenie to odnosi się w szczególności do podpisu jednostki. Należy jednakże zaznaczyć, że podpis jest cechą behawioralną, co oznacza, że istnieje wiele czynników mogących wpłynąć na jego obraz. Zależy on bowiem od częstości pisania, a więc od stopnia wyrobienia pisma. Trzeba również pamiętać, że pismo może się zmieniać z uwagi na wiek osoby piszącej czy wystąpienie choroby. Powinno to zatem zostać wzięte pod uwagę podczas tworzenia wzorca biometrycznego na podstawie obrazu pisma. Nie na natomiast wątpliwości, że pobranie próbki pisma do badań biometrycznych wymaga co prawda współpracy jednostki, ale ma przy tym charakter bezinwazyjny. Wydaje się również, że z uwagi na przyzwyczajenie do podpisywania licznych dokumentów wdrożenie urządzeń biometrycznych opierających

⁵ A. Feluś, *Podpisy – studium z pismoznawstwa*, Uniwersytet Śląski, Katowice 1987; Z. Czeczot, *Badania identyfikacyjne pisma ręcznego*, Wydawnictwo Zakładu Kryminalistyki KG MO, Warszawa 1972.

się na porównaniu pisma (zwłaszcza podpisów) nie stanowi problemu w kontekście akceptowalności społecznej takiego rozwiązania.

Tab. 1. Właściwości pisma jako cechy biometrycznej

Właściwość identyfikatora biometrycznego	Identyfikator w postaci pisma (podpisu)
Uniwersalność	Tak
Unikalność	Częściowo tak
Niezmienność	Częściowo tak
Możliwość pobrania	Tak
Akceptowalność	Tak

Źródło: opracowanie własne.

Możliwości wykorzystania technologii biometrycznej opartej na piśmie

Mimo iż współczesna kryminalistyka wykorzystywała indywidualne cechy jednostki do potwierdzenia tożsamości sprawy już w XIX wieku, rozwój porównania biometrycznego związany był w dużej mierze z możliwościami technologicznymi, którym zaczęto się przyglądać w połowie XX wieku⁶. Najbardziej intensywnie jednak biometria zaczęła rozwijać się po zamachach na World Trade Center oraz Pentagon z 11 września 2001 r.⁷ Po tym wydarzeniu administracja Stanów Zjednoczonych zaczęła poszukiwać efektywniejszych możliwości kontroli tożsamości osób wkraczających na terytorium USA. W tym kontekście kierunek biometryczny wskazany został przez tzw. Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)⁸. Patriot Act zakładał opracowanie standardu technologicznego, który pozwoliłby w szybki i skuteczny sposób identyfikować cudzoziemca/weryfikować jego tożsamość w momencie np. ubiegania się o wizę wjazdową na terytorium Stanów Zjednoczonych. Początek XXI wieku to również czas, gdy możliwością wykorzystania biometrii zainteresowała się Unia Europejska. W charakterze przykładu można wspomnieć o wdrożeniu w 2004 r. rozporządzenia nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie⁹. Przez ostatnie lata rynek zabezpieczeń biometrycznych stale rośnie, co wskazuje na popularność wykorzystywania identyfikatorów biometrycznych w różnych dziedzinach życia. Jedynie w ramach przykładu wskazać można

⁶ M. Tomaszewska-Michalak, *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warszawa 2015.

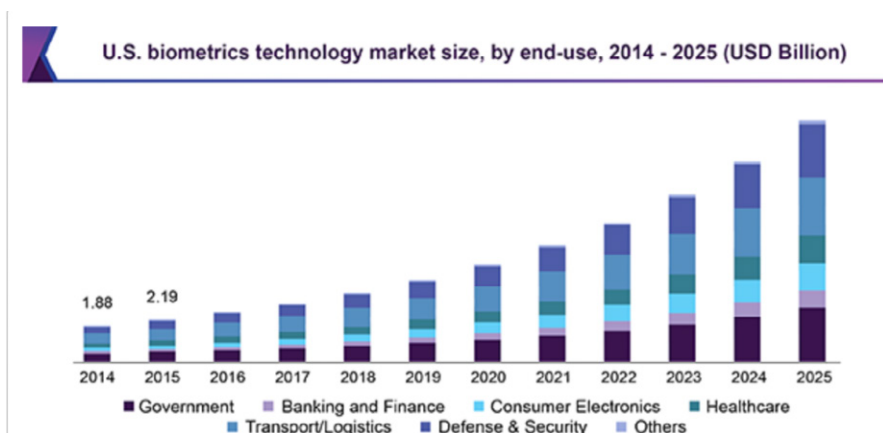
⁷ K. Gates, *Identifying the 9/11 'faces of terror'. The promise and problem of facial recognition technology*, „Cultural Studies” 2006, t. 20 (4–5), s. 417–440.

⁸ Public Law Pub.L. 107-56.

⁹ Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, Dz. Urz. L. 385.

wzrost znaczenia rynku technologii biometrycznych we wspomnianych już Stanach Zjednoczonych (Ryc. 2).

Ryc. 2. Rynek technologii biometrycznych w Stanach Zjednoczonych z podziałem na obszary wykorzystania



Źródło: <https://www.grandviewresearch.com>, dostęp 30.09.2022.

Poza możliwościami, jakie uzyskała biometria w związku z ogólnym rozwojem technologicznym na przestrzeni ostatnich 20 lat, o popularności wykorzystania identyfikatorów zdecydowały zalety, jakie niesie ze sobą porównanie biometryczne. Pierwszą i podstawową jest szybkość procesu weryfikacji/identyfikacji, zwłaszcza w porównaniu z wykonywaniem tych czynności w sposób tradycyjny (np. przez urzędnika czy funkcjonariusza). Obecnie porównanie biometryczne może trwać mniej niż sekundę, co znacznie usprawnia otrzymanie uprawnień przez jednostkę. W parze z szybkością idzie również dokładność pomiaru. Porównanie biometryczne ma nad tradycyjną weryfikacją/identyfikacją tę przewagę, że zbadany jest odsetek błędów popełnianych przez algorytmy wykorzystywane w pracy konkretnego urzędnika. Dodatkowo biometria może zastąpić inne metody weryfikacji uprawnień jednostki. Tradycyjne środki zabezpieczeń oparte są na filozofii „coś, co wiem” lub „coś, co posiadam”. Do pierwszej kategorii zaliczyć można hasła czy numery PIN, do drugiej natomiast tokeny czy karty. Biometria należy natomiast do trzeciej grupy zabezpieczeń – „coś, czym jestem”. Wykorzystanie identyfikatorów może zatem być wygodne dla użytkownika, który nie jest w takim przypadku zmuszony do zapamiętania hasła czy posiadania przy sobie np. karty z kodami¹⁰. Dodatkowo w przypadku

¹⁰ Zalety biometrii zostały w tym przypadku dostrzeżone np. przez prawodawcę unijnego, który w dyrektywie 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniającej dyrektywę: 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylającej dyrektywę 97/5/WE (Payment

identyfikatorów biometrycznych nie istnieje ryzyko, że zostaną one wykradzione osobie uprawnionej. Zwiększa to bezpieczeństwo prawidłowego określenia osoby uprawnionej, gdyż identyfikator bezwzględnie połączony jest z tożsamością osoby. Obecnie identyfikatory biometryczne mają liczne zastosowania i używane są m.in.:

- jako element zabezpieczenia dokumentu. Przykładem może być wydawany w państwach członkowskich Unii Europejskiej paszport zawierający zdjęcie biometryczne oraz chip z zakodowanym wzorem linii papilarnych;

- do weryfikacji tożsamości/identyfikacji osób poszukiwanych/sprawców przestępstw. Polski system AFIS czy europejski system SIS II można włączyć do wskazanej kategorii;

- do weryfikacji tożsamości klienta instytucji finansowej w celu uzyskania uprawnień do wykonania transakcji. Za przykład mogą tu posłużyć bankomaty biometryczne czy weryfikacja tożsamości jednostki oparta na systemie rozpoznawania twarzy;

- w celu podnoszenia poziomu bezpieczeństwa imprez masowych. Przykładem może być weryfikacja biometryczna osób próbujących dostać się do wioski olimpijskiej;

- jako zabezpieczenie przedmiotów użytku codziennego, takich jak telefony czy komputery;

- jako środek chroniący przed wejściem na określony teren osoby nieposiadającej do tego uprawnień (np. instalacja klamek zabezpieczonych biometrycznie).

Wskazany zbiór stanowi tylko przykład zastosowania biometrii. Obrazuje on jednak wszechstronność tej technologii i możliwość implementacji algorytmów porównawczych w wielu dziedzinach życia. Odnośnie do wykorzystania podpisu w charakterze identyfikatora biometrycznego wydaje się, że ta cecha sprawdzi się w miejscach, w których już obecnie stosowany jest tradycyjny podpis w celu weryfikacji tożsamości, przykładem są tu zatem wszelkie transakcje przeprowadzane w oddziałach banku czy za pomocą karty płatniczej. Podobne miejsce dla podpisu biometrycznego można również znaleźć w dokumentach.

Cel zastosowania identyfikatora biometrycznego w postaci podpisu

Najbardziej unikatowym elementem pisma jest podpis. Im częściej jest on kreślony, tym bardziej automatyczny staje się to proces, co tym samym włącza go do grupy behawioralnych identyfikatorów biometrycznych. Podpis stanowi ważny element potwierdzający tożsamość danej osoby. O jego wadze świadczy konieczność składania go na wszelkich dokumentach niosących za sobą skutki prawne, takich jak

Services Directive) wskazał na konieczność wprowadzenia w sektorze finansowym mechanizmu tzw. silnego uwierzytelnienia klienta, które oznacza uwierzytelnianie oparte na zastosowaniu co najmniej dwóch elementów należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co posiada wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających (art. 4 pkt 30).

np.: umowy, dokumenty finansowe czy testament. Chociaż zgodnie z policyjnymi statystykami liczba przestępstw z art. 270 k.k. (fałszerstwo dokumentu)¹¹ sukcesywnie spada, to cały czas pozostaje ona na dość wysokim poziomie¹².

Tab. 2. Statystyka przestępstwa z art. 270 k.k.

Rok	Liczba postępowań wszczętych	Liczba przestępstw stwierdzonych
2020	9350	17 546
2019	11 910	19 880
2018	12 667	22 474
2017	13 667	23 690
2016	15 129	28 324
2015	16 707	26 988
2014	16 652	30 392
2013	17 579	30 331
2012	17 148	29 588
2011	15 888	36 025

Źródło: opracowanie własne.

Jak wskazuje się w literaturze, można wyróżnić wiele rodzajów fałszowania podpisów. Są to między innymi:

- fałszerstwo w wyniku przekopiowania podpisu,
- fałszerstwo poprzez tzw. naśladownictwo intelektualne, z którym mamy do czynienia, gdy fałszerz nie zna obrazu autentycznego podpisu,
- fałszerstwo powstałe w wyniku naśladowania znanego fałszerzowi podpisu autentycznego,

¹¹ „Art. 270 k.k. § 1. Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto wypełnia blankiet, zaopatrzone cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo takiego dokumentu używa.

§ 2 a. W przypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 3. Kto czyni przygotowania do przestępstwa określonego w § 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”.

¹² Należy jednakże zwrócić uwagę, że art. 270 k.k. dotyczy generalnie przestępstwa podrobienia lub przerobienia dokumentu, a nie jedynie interesującego ze względu na to opracowanie przestępstwa fałszowania podpisu.

- autofalszerstwo, którego celem jest zamaskowanie własnego pisma, tak aby w późniejszym czasie podważyć autentyczność złożonego podpisu¹³.

Tradycyjną metodą badania autentyczności podpisu jest skorzystanie z pomocy biegłego z zakresu badań dokumentów. Bardzo pomocne jednak byłyby wprowadzenie tam, gdzie to możliwe, formy składania podpisu na specjalnym tablecie służącym do weryfikacji biometrycznej. W tym przypadku bowiem poza tradycyjną metodą graficzno-porównawczą, wykorzystywaną przez ekspertów w ramach analizy podpisu, istnieje również możliwość weryfikacji dodatkowych cech związanych z kreśleniem podpisu¹⁴. Pierwszą z nich jest czas jego składania. Zbyt długi czas kreślenia podpisu porównawczego może świadczyć o jego nieautentyczności i próbie przekopiowania bądź odwzorowania podpisu osoby. Dynamika pisania jest jedną z właściwości, której fałszerz nie może się nauczyć jedynie przez patrzenie na obraz graficzny podpisu. Drugą zaletą tabletu używanego do biometrycznego porównywania podpisów jest zapisywanie przez urządzenie informacji na temat rozkładu nacisku na urządzenie podczas pisania. Wspomaga to eksperta w tradycyjnych badaniach, gdyż nienaturalny dla wzorca danej osoby rozkład nacisku może oznaczać próbę sfałszowania podpisu. Trzecią cechą, na którą warto zwrócić uwagę, jest mierzenie przez urządzenia kątów położenia rysika, jak również rejestrowanie odrywania rysika od powierzchni tabletu. Wspomniane możliwości algorytmów biometrycznych w przypadku podpisu dają duże możliwości w zakresie wychwytywania potencjalnych fałszerstw podpisów. Oczywiście aby można było przeprowadzić weryfikację biometryczną podpisu, jego wzorzec musi zostać wcześniej zapisany w systemie. Nie da się bowiem dokonać biometrycznej weryfikacji pod kątem wskazanych wyżej właściwości podpisu złożonego w sposób tradycyjny. Przypadkiem, w którym wspomniane właściwości (dynamika, nacisk, kąt przyłożenia pióra) mogą okazać się niewystarczające do odkrycia próby oszustwa, jest wspomniane wcześniej autofalszerstwo. W takiej jednak sytuacji klasyczna ekspertyza pismoznawcza powinna wykazać próbę maskowania pisma poprzez ujawnienie cech nawykowych w podpisie. Wydaje się, że po spełnieniu odpowiednich warunków algorytmy biometryczne mogłyby być wykorzystywane do weryfikacji nie tylko autentyczności podpisów, lecz także innych kreślonych zapisów. Pamiętać jednak należy, że najczęściej to właśnie w podpisie ujawnia się największy automatyzm kreślenia, dlatego też naturalnie to ten element pisma staje się podstawą tworzenia wzorca biometrycznego.

Podsumowanie

Celem opracowania było ukazanie możliwości wykorzystania pisma w charakterze identyfikatora biometrycznego. Biorąc pod uwagę przytoczoną wyżej definicję technologii biometrycznej, można stwierdzić, że pismo należy do behawioralnych

¹³ M. Goc, *Badania podpisów w kryminalistycznej ekspertyzie pismoznawczej – wybrane zagadnienia metodyczne*, „Problemy Kryminalistyki” 2009, nr 263, s. 19–27.

¹⁴ A. Czajka, A. Pacut, *Biometria podpisu odręcznego*, w: P. Zając, S. Kwaśniowski (red.), *Automatyczna identyfikacja w systemach logistycznych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004, s. 244–260.

cech biometrycznych, które kształtują się i indywidualizują proporcjonalnie do częstotliwości pisania. Obecnie istniejące na rynku tablety, ograniczające się do porównania podpisu jednostki, mogą wspomóc eksperta z zakresu badań pisma w procesie ustalania autentyczności nakreślonego zapisu.

W opracowaniu nie zostały poruszone kwestie prawne związane z możliwością przetwarzania danych biometrycznych ani problemy, jakie mogą się pojawić w związku z wykorzystaniem algorytmów do weryfikacji osoby na podstawie złożonego podpisu. Z uwagi na istotę wskazanych zagadnień staną się one tematem drugiej części opracowania.

Bibliografia

Literatura

- Bertillon A., *Identification anthropométrique*, Imprimerie Administrative, Melun 1893.
- Cieśla R., *Współczesne wyzwania wobec badań dokumentów*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2021.
- Czajka A., Pacut A., *Biometria podpisu odręcznego*, w: P. Zając, S. Kwaśniowski (red.), *Automatyczna identyfikacja w systemach logistycznych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.
- Czeczot Z., *Badania identyfikacyjne pisma ręcznego*, Wydawnictwo Zakładu Kryminalistyki KG MO, Warszawa 1972.
- Feluś A., *Podpisy – studium z pismoznawstwa*, Uniwersytet Śląski, Katowice 1987.
- Gates K., *Identifying the 9/11 ‘faces of terror’. The promise and problem of facial recognition technology*, „Cultural Studies” 2006, t. 20 (4–5).
- Goc M., *Badania podpisów w kryminalistycznej ekspertyzie pismoznawczej – wybrane zagadnienia metodyczne*, „Problemy Kryminalistyki” 2009, nr 263.
- Grzeszyk C., *Daktyloskopia*, Wydawnictwo Naukowe PWN, Warszawa 1992.
- Mendyk-Krajewska T., *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, „Roczniki SGH” 2019, nr 54.
- Moszczyński J., *Z historii polskiej daktyloskopii*, „Studia Prawnoustrojowe” 2014, nr 26.
- Sikora K., *Technologie biometryczne sposobem uwspółcześnienia przepisów o formie testamentu holograficznego*, „Studia Prawnicze. Rozprawy i Materiały” 2020, nr 2 (27).
- Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warszawa 2015.

Źródła prawa

- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997 Nr 88, poz. 553 ze zm.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law Pub.L. 107-56.
- Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, Dz. Urz. L. 385.
- Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniającej dyrektywę: 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylającej dyrektywę 97/5/WE (Payment Services Directive).

Źródła internetowe

<https://sjp.pwn.pl/>

<https://statystyka.policja.pl>

Konflikt interesów

Brak

Źródło finansowania

Publikacja opracowana w ramach projektu nr DOB-SZAFIR/06/A/042/01/2020 pt. „Inteligentny system do identyfikacji fałszerstwa cech biometrycznych pisma ręcznego”, finansowanego ze środków NCBR, realizowanego w Programie pn. Rozwój nowoczesnych, przełomowych technologii służących bezpieczeństwu i obronności państwa” pk. „SZAFIR” z Konkursu nr 1/SZAFIR/2020. Projekt realizowany w latach 2021–2024 przez konsorcjum w składzie: Centralne Laboratorium Kryminalistyczne Policji, Instytut Kryminalistyki Polskiego Towarzystwa Kryminalistycznego Sp. z o.o. oraz JAS Technologie Sp. z o.o.