dr Magdalena Tomaszewska-Michalak
Wydział Nauk Politycznych i Studiów Międzynarodowych,
Uniwersytet Warszawski
ORCID 0000-0001-5441-0396

PISMO RĘCZNE JAKO CECHA BIOMETRYCZNA. CZĘŚĆ II

Streszczenie
Pierwsza część artykułu dotyczy prawnych aspektów przetwarzania danych biometrycznych ze szczególnym uwzględnieniem identyfikatora w postaci podpisu biometrycznego. Autorka odwołuje się w tym zakresie do rozporządzenia RODO, wskazującego zasady gromadzenia i wykorzystywania danych osobowych. Część druga odnosi się do problemów technicznych, jakie mogą pojawić się w związku z przetwarzaniem danych biometrycznych, w tym do błędów związanych z działaniem systemów biometrycznych.

Słowa kluczowe: technologia biometryczna, pismo ręczne, podpis, przetwarzanie danych biometrycznych

Wstęp

Niniejsze opracowanie stanowi część drugą opracowania pt. *Pismo ręczne jako cecha biometryczna*[1]. W pierwszej części poruszone zostały zagadnienia wskazujące na przynależność pisma do behawioralnych cech biometrycznych oraz możliwość wykorzystania podpisu w charakterze identyfikatora biometrycznego. W niniejszym opracowaniu nacisk położony zostanie natomiast na aspekty prawne przetwarzania danych biometrycznych, a także na problemy, jakie mogą się pojawić w związku z automatyczną weryfikacją tożsamości/identyfikacją osoby na podstawie pisma[2].

---

[1] Zob. „Problemy Współczesnej Kryminalistyki" 2022, t. XXVI, s. 423–433.

[2] 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: Cen-

Prawne aspekty przetwarzania danych biometrycznych

Pierwszym zagadnieniem, które należy rozważyć w kontekście prawnych możliwości wykorzystania danych biometrycznych, w tym weryfikacji/identyfikacji na podstawie podpisu, są ogólne zasady przetwarzania wzorców biometrycznych. Warto zwrócić uwagę, że prawodawca unijny uznał w rozporządzeniu 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) (dalej jako RODO)[3] odrębność identyfikatorów biometrycznych, wyróżniając cechy biometryczne jako dodatkową kategorię danych. Jest to o tyle istotne, że dane biometryczne nie pojawiały się ani pod rządami dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[4] poprzedzającej RODO, ani w ramach uchylonej już polskiej ustawy o ochronie danych osobowych[5]. RODO określa 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" (art. 4 pkt 14 RODO). Jednocześnie dane biometryczne włączone zostały do katalogu danych szczególnych, których gromadzenie i wykorzystywanie możliwe jest jedynie w ściśle określonych sytuacjach (art. 9 RODO)[6]. Dodatkowo w odniesieniu do wskazanych danych

tralne Laboratorium Kryminalistyczne Policji, Instytut Kryminalistyki Polskiego Towarzystwa Kryminalistycznego Sp. z o.o. oraz JAS technologie Sp. z o.o.

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 (ogólne rozporządzenie o ochronie danych), Dz. Urz. 2016, L119.

4 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych; Dz. Urz. 1995, L281.

5 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997, nr 133, poz. 883.

6 Art. 9 RODO daje możliwość przetwarzania danych wrażliwych tylko we wskazanych sytuacjach, mianowicie jeżeli:

a) „osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem

RODO nakazuje przeprowadzenie oceny ryzyka ich przetwarzania pod kątem skutków, jakie takie działanie niesie dla praw lub wolności osób fizycznych (art. 35 RODO). W sytuacji gdy dopuszczone zostanie przetwarzanie danych biometrycznych, administrator bazy powinien przestrzegać zasad przetwarzania wzorców biometrycznych: rzetelności i przejrzystości, celowości oraz proporcjonalności/adekwatności. Zasady rzetelności i przejrzystości polegają na przetwarzaniu tylko takich danych, które są aktualne. W przypadku części identyfikatorów biometrycznych, w tym np. podpisu, należy pamiętać o konieczności odnawiania wzorca po upływie określonego czasu. Reguła rzetelności wiąże się również z obwarowaniem prowadzenia zbioru

państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) 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;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą".

danych obowiązkiem informacyjnym[7], a także określeniem czasu, po którym dane należy usunąć. Zasada celowości polega na możliwości wykorzystania danych tylko do celów, do których zostały zebrane. W przypadku danych biometrycznych będzie to oznaczało, że nie mogą one zostać przekazane innym podmiotom, np. do celów marketingowych. Taka zasada może mieć wpływ na zwiększenie zaufania do posługiwania się danymi biometrycznymi w różnych dziedzinach życia. Ostatnią z reguł zapisanych w RODO jest reguła proporcjonalności, która stanowi, że gromadzenie danych musi być adekwatne do założonego celu. W konsekwencji przetwarzanie nadmiernej ilości danych uznane zostanie za naruszenie opisywanej reguły. Przykładem ilustrującym sytuację nieproporcjonalności w przypadku danych biometrycznych było uznanie przez Naczelny Sąd Administracyjny przetwarzania identyfikatorów biometrycznych do celu kontroli czasu pracy[8]. NSA uznał bowiem, że w tej sytuacji ingerencja w prawo do prywatności pracownika jest zbyt daleko idąca w porównaniu z korzyściami, jakie niesie ze sobą w tym przypadku gromadzenie linii papilarnych. Do tej pory jednak nie pojawiły się orzeczenia wskazujące na sytuację, w której weryfikacja na podstawie podpisów biometrycznych stanowiłoby naruszenie zasady proporcjonalności. Podsumowując, nie ma obecnie przeciwskazań prawnych gromadzenia biometrycznych wzorców podpisów. Należy jednak w każdej sytuacji przetwarzania danych biometrycznych kierować się określonymi w przepisach zasadami dotyczącymi ochrony danych osobowych.

Brak zakazów nie idzie obecnie w parze z dostosowywaniem prawa (w tym przypadku głównie cywilnego) do możliwości wykorzystywania coraz bardziej popularnych w życiu codziennym urządzeń biometrycznych. W literaturze dostrzega się już ten problem, np. w odniesieniu do prawa spadkowego w kontekście możliwości wykorzystania biometrycznego podpisu w celu sporządzenia testamentu[9]. Jak wskazuje Katarzyna Sikora, prawo nie może nie uwzględniać postępującej cyfryzacji, zwłaszcza w sytuacji, gdy wykorzystanie nowoczesnej technologii pozwala skuteczniej uwierzytelnić testatora. Można by zatem rozważyć wprowadzenie możliwości sporządzenia testamentu w formie elektronicznej, podpisanego za pomocą biometrycznego identyfikatora spadkodawcy (np. podpisu). Wykorzystana

[7] Obowiązek informacyjny polega na konieczności poinformowania osoby, której dane są przetwarzane, o tym fakcie, a także wskazania drogi sprostowania lub usunięcia gromadzonych informacji.

[8] Por. np. Wyrok NSA I OSK 249/09.

[9] K. Sikora, *Technologie biometryczne sposobem uwspółcześnienia przepisów o formie testamentu holograficznego*, „Studia Prawnicze. Rozprawy i materiały" 2020, nr 2(27), s. 207–225.

do uwierzytelnienia cecha biometryczna może stanowić w tym przypadku dodatkowy element potwierdzający autentyczność dokumentu. Przykład ten pokazuje jedynie możliwości, jakie wiążą się z wykorzystywaniem technologii biometrycznej również w ramach sektora publicznego.

Technologiczne aspekty przetwarzania danych biometrycznych

Poza prawną dopuszczalnością przetwarzania danych biometrycznych konieczne jest również pochylenie się nad problemami natury technologicznej, które mogą wystąpić w związku z wdrażaniem nowoczesnych rozwiązań identyfikacji osoby lub weryfikacji jej tożsamości. Należy bowiem pamiętać, że skuteczność algorytmów nigdy nie jest stuprocentowa i że wykorzystanie urządzeń biometrycznych wiąże się z ryzykiem wystąpienia błędu. W zakresie technologii biometrycznej wyróżnia się trzy rodzaje błędów: FER, FAR oraz FRR. Pierwszy z wymienionych, zwany błędem rejestracji (FER – ang. *Failure to Enrol Rate*), polega na braku możliwości zarejestrowania wzorca biometrycznego. Może mieć to miejsce, gdy osoba nie posiada danej cechy (np. brak dłoni uniemożliwiający pobranie linii papilarnych) lub gdy jakość cechy nie pozwala na stworzenie z niej wzorca biometrycznego (np. choroby powodujące zanik linii papilarnych, a w konsekwencji niemożność stworzenia wzorca o odpowiedniej jakości, tak by dokonać rejestracji). W odniesieniu do podpisu omawiany błąd wystąpić może w związku z fizyczną ułomnością osoby (brak dłoni, zaawansowana choroba ręki niepozwalająca na złożenie podpisu) lub brakiem umiejętności złożenia podpisu (np. w przypadku analfabetyzmu). W razie wdrożenia systemu opartego na biometrycznym porównaniu podpisu wystąpienie FER powoduje zatem konieczność wprowadzenia tzw. procedur awaryjnych. Są to procedury, które pozwalają na uwierzytelnienie tożsamości osoby na podstawie innych cech niż biometryczne. Implementowanie procedur awaryjnych jest konieczne z punktu widzenia osób monitorujących porównanie tożsamości, gdyż daje jasne wytyczne zachowania w nietypowej sytuacji. Jest to równie korzystne dla użytkownika systemu, gdyż nie jest on dyskryminowany ze względu na brak możliwości pobrania od niego wzorca identyfikatora biometrycznego. Istotne jest również określenie, jak wiele prób rejestracji powinno się podjąć. Należy pamiętać, że uparte powtarzanie procesu rejestracji wzorca może mieć negatywne konsekwencje związane ze spadkiem zaufania użytkownika do systemu. Dodatkowo rejestracja wzorca „kompromisowego" może prowadzić w przyszłości do problemów podczas przeprowadzania uwierzytelniania biometrycznego. W sytuacji wystąpienia FER warto zidentyfikować również przyczynę braku możliwości rejestracji,

gdyż może mieć ona jedynie charakter czasowy (np. czasowe uszkodzenie ręki). W takim przypadku również warto wdrożyć procedury awaryjne, a obraz wzorca identyfikatora pobrać w późniejszym terminie.

W przypadku algorytmów biometrycznych wysoki odsetek FER ma poważne konsekwencje, gdyż może spowodować konieczność ponownego przemyślenia sensu gromadzenia danych biometrycznych ze względu na przymusowy dualizm procesu uwierzytelniania. Dodatkowo głównym celem wprowadzania rozwiązań opartych na biometrii jest podniesienie poziomu bezpieczeństwa danego systemu. Konsekwencją natomiast braku możliwości rejestracji osoby jest niemożność jest uwierzytelnienia na etapie porównania, co tym samym uniemożliwia realizację podstawowego założenia stojącego za wdrażaniem zabezpieczeń biometrycznych.

Pozostałe dwa błędy, które mogą wystąpić w związku z wykorzystaniem technologii biometrycznej, to: błąd fałszywego odrzucenia (FRR – ang. *Failure Rejection Rate*) oraz błąd fałszywej akceptacji (FAR – ang. *Failure Acceptance Rate*). Oba wskazane błędy pojawiają się już na etapie porównania cechy, a więc w sytuacji, gdy wzorzec identyfikatora znajduje się w systemie. Błąd FRR polega na uznaniu osoby faktycznie uprawnionej za nieupoważnioną do dostępu do określonego systemu. Wystąpienie błędu fałszywego odrzucenia może być kłopotliwe dla użytkownika, a jeśli będzie pojawiać się często, może prowadzić do braku akceptacji systemu oraz niechęci użytkownika wobec stosowania zabezpieczeń biometrycznych. W przypadku FER konieczne jest zastosowanie procedur awaryjnych, które powinny jasno określać reguły postępowania w sytuacji negatywnej weryfikacji tożsamości osoby. W procedurach tych należy przede wszystkim wskazać, kiedy powinno się uznać, że negatywny wynik porównania nie jest związany z próbą oszustwa, lecz stanowi błąd systemu. Następnie trzeba określić, jaka alternatywna metoda weryfikacji tożsamości osoby powinna być zastosowana w takim przypadku (np. wykorzystanie innej cechy biometrycznej czy okazanie dokumentu tożsamości). Drugi ze wskazanych błędów – fałszywej akceptacji – polega na nieprawidłowym działaniu urządzenia, które w wyniku porównania wskazuje na tożsamość cechy biometrycznej z wzorcem, podczas gdy nie jest to zgodne z rzeczywistością. FAR jest wyjątkowo niebezpiecznym błędem z perspektywy bezpieczeństwa systemu. Nieodpowiednia kontrola nad systemem może bowiem spowodować niewykrycie nieprawidłowej weryfikacji, a tym samym przyznanie uprawnień osobie nieupoważnionej. Należy zatem zawsze monitorować prawidłowe działanie urządzenia i mieć na uwadze możliwość popełnienia błędu przez algorytm.

Problemy związane z możliwością użycia pisma w charakterze cechy biometrycznej wykorzystywanej w procesie identyfikacji osoby/weryfikacji tożsamości

Każda cecha, która ma zostać wykorzystana w procesie porównania biometrycznego, powinna charakteryzować się określonymi właściwościami. Są to: powszechność występowania, niezmienność, unikatowość, możliwość pobrania, akceptowalność. Właściwości te zostały opisane szerzej w pierwszej części opracowania *Pismo ręczne jako cecha biometryczna*. W tym miejscu należy jedynie skupić się na tych elementach, które wydają się problematyczne w kontekście tworzenia wzorca biometrycznego podpisu. Będzie to zwłaszcza: unikatowość oraz niezmienność identyfikatora w postaci pisma (tabela 1).

Tab. 1. Właściwości pisma jako cechy biometrycznej

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

Źródło: M. Tomaszewska-Michalak, *Pismo ręczne jako cecha biometryczna. Część I*, „Problemy Współczesnej Kryminalistyki" 2022, t. XXVI, s. 427.

Pomimo iż w literaturze wskazuje się, że pismo charakteryzuje się indywidualnością osobniczą[10], można wymienić szereg czynników potencjalnie rzutujących na obraz kreślonych znaków[11]. Pierwszym jest niewątpliwie częstość pisania. Ponieważ pismo należy do cech behawioralnych, unikatowe dla osoby staje się ono w związku z powtarzaniem określonego zachowania. Im częściej składamy podpis, tym bardziej charakterystyczne są dla jego właściciela zarówno właściwości graficzne, jak i cechy dynamiczne (m.in. tempo i czas kreślenia). Brak konieczności ręcznego pisania/składania podpisów może prowadzić do niewykształcenia się w pełni cech indywidualizujących obraz pisma. Nie wyklucza to możliwości przeprowadzenia

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

[11] Por. np. M. Całkiewicz, *Kryminalistyczne badania patologicznego pisma ręcznego*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009.

biometrycznej weryfikacji osoby piszącej, może jednak znacząco utrudnić ten proces. Drugim problemem, który może stanąć na drodze prawidłowego uwierzytelniania na podstawie podpisu, jest wykorzystywanie różnych wzorów podpisów. W takim przypadku urządzenie biometryczne nie będzie mogło zostać użyte. Istotne z perspektywy zaburzenia działania urządzenia mogą być również zmiany wyglądu obrazu pisma związane z wiekiem osoby. Wiąże się to nieodłącznie z częściową zmiennością obrazu pisma. Urządzenie biometryczne nie będzie bowiem w stanie prawidłowo porównać podpisu złożonego przez dziecko dopiero uczące się pisać z podpisem osoby dorosłej, której grafizm uważa się już za wyrobiony. Nie tylko jednak młody wiek może stać na przeszkodzie przeprowadzeniu skutecznego porównania biometrycznego. Obraz podpisu osoby starszej również może różnić się od wzorca, który zarejestrowany został kilkanaście lat wcześniej. Może to wynikać np. z mniejszej sprawności pisania lub z chorób ujawniających się najczęściej u osób starszych, takich jak np. parkinsonizm. Choroby czy uszkodzenia ręki mogą również mieć wpływ na obraz pisma. Wszystkie wskazane wyżej czynniki należy brać pod uwagę w przypadku wdrażania systemu biometrycznego opartego na uwierzytelnianiu na podstawie podpisu. Zdając sobie bowiem sprawę z potencjalnych problemów związanych z wykorzystaniem omawianego identyfikatora, można wprowadzać odpowiednie procedury minimalizujące ryzyko nieprawidłowego działania algorytmu. Przede wszystkim po upływie określonego czasu należy odnawiać wzorzec biometryczny podpisu. Jeśli osoba zwyczajowo wykorzystuje więcej niż jedną formę podpisu, można w systemie utworzyć np. dwa wzorce. Takie rozwiązanie będzie wygodne dla użytkownika i pozwoli uniknąć negatywnej weryfikacji tożsamości. Dodatkowo, biorąc pod uwagę rożne scenariusze (np. chorobę, uszkodzenie ręki), należy wprowadzić procedury awaryjne pozwalające na weryfikację osoby bez konieczności składania podpisu. Przewidywanie potencjalnych problemów związanych z uwierzytelnianiem biometrycznym na podstawie wzoru podpisu pozwala na lepsze przygotowanie się na sytuacje nietypowe, a tym samym na zachowanie odpowiedniego poziomu bezpieczeństwa systemu nawet w przypadku konieczności stosowania procedury alternatywnej do porównania biometrycznego. Duże znaczenie ma tu również wygoda użytkownika, która wpływać może na akceptację rozwiązań biometrycznych.

Podsumowanie

Celem opracowania było odniesienie się do problematycznych kwestii związanych z wykorzystaniem technologii biometrycznej opartej na uwie-

rzytelnianiu osoby na podstawie pisma, ze szczególnym uwzględnieniem podpisu. W pierwszej części opracowania poruszone zostały prawne aspekty przetwarzania danych biometrycznych. Analiza wykazała, że w obecnym ustawodawstwie brak jest jednoznacznych przeciwwskazań do wdrażania zabezpieczeń opartych na identyfikatorach biometrycznych. W niektórych aktach prawnych pojawia się nawet bezpośrednie odwołanie do cech biometrycznych (por. RODO), co oznacza, że prawodawca unijny dostrzega, iż urządzenia biometryczne stają się coraz popularniejsze w życiu codziennym. Jednocześnie wrażliwość wskazanych danych powoduje, że możliwość ich przetwarzania obwarowywana jest określonymi zasadami. Zauważenie istnienia danych biometrycznych nie skłoniło jednak polskiego prawodawcy do wprowadzenia zmian ułatwiających włączenie biometrycznego uwierzytelniania na podstawie podpisu do czynności z zakresu prawa cywilnego. Nie przeszkadza to jednak wykorzystywaniu go w sektorze prywatnym, w tym zwłaszcza finansowym.

Druga część opracowania dotyczyła błędów algorytmów, jakie mogą pojawić się w procesie uwierzytelnia podpisu. Należy pamiętać, że każde urządzenie popełnić może błąd, a prawidłowe monitorowanie działania systemu może pozwolić na skuteczne zniwelowanie skutków jego wystąpienia.

W ramach ostatniej części opracowania podjęto próbę przeanalizowania problemów, jakie związane są z wykorzystaniem podpisu w procesie biometrycznego uwierzytelniania tożsamości. Prawidłowe funkcjonowanie systemu biometrycznego wiąże się bowiem nie tylko z nadzorowaniem efektywnego działania algorytmu, ale również ze zidentyfikowaniem czynników, które mogą mieć wpływ na różne etapy procesu uwierzytelniania. Prawidłowa diagnoza w tym zakresie pozwala na świadome wprowadzanie ulepszeń do systemu biometrycznego.

Niniejszy artykuł stanowi drugą część opracowania *Pismo ręczne jako cecha biometryczna*. Obie części pozwalają na pełniejsze zrozumienie problemu wykorzystania pisma w charakterze identyfikatora biometrycznego stosowanego w procesie identyfikacji osoby lub weryfikacji jej tożsamości.

Bibliografia

Literatura

Całkiewicz M., *Kryminalistyczne badania patologicznego pisma ręcznego*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009.

Cieśla R., *Współczesne wyzwania wobec badań dokumentów*, Uniwersytet Wrocławski. Wydawnictwo, 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.
Goc M., *Badania podpisów w kryminalistycznej ekspertyzie pismoznawczej – wybrane zagadnienia metodyczne*, „Problemy Kryminalistyki" 2009, nr 263.
Mendyk-Krajewska T., *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, „Roczniki SGH" 2019, nr 54.
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 i orzecznictwo

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. 1995, L281.
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), Dz. Urz. 2016, L119.
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997, nr 133, poz. 883.
Wyrok NSA I OSK 249/09.