REMIGIUSZ LEWANDOWSKI
ORCID: 0000-0001-7353-9742

DOI: 10.4467/20801335PBW.21.022.14299

Alternatywne narzędzia zdalnej identyfikacji

Przeobrażenia gospodarcze, w tym te wynikające z ograniczeń mających przeciwdziałać rozprzestrzenianiu się pandemii COVID-19, znacznie upowszechniły pracę realizowaną w trybie zdalnym i przyspieszyły cyfryzację gospodarki. Implikuje to jednak coraz większe zagrożenia wynikające z podatności procesów realizowanych w cyberprzestrzeni na różnego rodzaju ryzyko. W kontekście wspomnianych zjawisk szczególnie istotne są zagrożenia związane z tożsamością człowieka i możliwością kradzieży tej tożsamości, tj. bezprawnego wejścia w posiadanie danych osobowych określonej osoby i wykorzystywania ich wbrew jej woli lub poza jej wiedzą. Warto się zatem dogłębnie zastanowić nad adekwatnością środków zdalnej identyfikacji stosowanych obecnie i zasadnością proponowania nowych narzędzi w tym zakresie. Podjęcie refleksji naukowej na ten temat jest tym bardziej zasadne, że jednymi z najszybciej rozwijających się trendów technologicznych są sztuczna inteligencja (ang. *artificial intelligence*, AI) i algorytmizacja, które w coraz większym stopniu są wykorzystywane w działaniach gospodarczych, administracyjnych i dotyczących bezpieczeństwa. Rola AI nabiera szczególnego znaczenia w przypadku procesów związanych z zapewnieniem bezpieczeństwa tożsamości, w tym tych, w których wykorzystuje się algorytmy rozpoznawania twarzy. W niniejszym artykule omówiono problemy wynikające z obecnie stosowanych, klasycznych metod zdalnej identyfikacji tożsamości człowieka oraz przedstawiono propozycję alternatywnego podejścia, bazującego na wykorzystaniu cech biometrycznych i elektronicznego dowodu osobistego. Zastosowano strategię, której podstawą jest porównanie modelu zdalnej identyfikacji opartego na klasycznych metodach z proponowanym nowym modelem. Cechą tych modeli jest, z oczywistych względów, symplifikacja ujętych w nich zjawisk, co prowadzi do stworzenia prototypu rzeczywistości, przy maksymalnym odwzorowaniu tych właściwości, które są ważne z punktu widzenia analizy, oraz pominięciu tych, które są nieistotne[1].

[1] H.G. Adamkiewicz-Drwiłło, *Współczesna metodologia nauk ekonomicznych*, Toruń 2008, s. 172.

Pojęcie tożsamości

Bezpieczeństwo i komfort życia współczesnych społeczeństw zależą m.in. od poziomu rozwoju technologicznego. Jednym z ważniejszych aspektów bezpieczeństwa jest bezpieczeństwo tożsamości, czyli zapewnienie pewności, tj. jednoznacznej wiedzy, co do tożsamości danej osoby. Anglojęzycznym odpowiednikiem pojęcia „tożsamość" jest pojęcie „*identity*", słowo wywodzące się z łacińskiego *idem* oznaczającego „identyczność" oraz „ciągłość". *Merriam-Webster's Dictionary* wskazuje cztery główne znaczenia „*identity*"[2]. Są to: 1a) „wyróżniające cechy charakteru lub osobowość jednostki" albo 1b) „świadomość wspólnych cech określona przez psychologiczne identyfikowanie się"; 2) „stan bycia takim samym jak przedmiot opisu lub wskazania"; 3a) „identyczność istotnej lub wtórnej cechy w różnych warunkach" albo 3b)" identyczność we wszystkim, co składa się na obiektywną rzeczywistość przedmiotu"; 4) „równość dwóch wyrażeń, która zachodzi dla wszystkich wartości występujących w niej zmiennych"[3]. Z kolei *Słownik języka polskiego* PWN podaje pięć znaczeń terminu „tożsamość"[4]. Po pierwsze, oznacza on „identyczność". Jest to więc rozumienie analogiczne do drugiej i trzeciej definicji terminu „*identity*" ujętej w *Merriam-Webster's Dictionary*. Po drugie, jest to „świadomość siebie w odniesieniu do pojedynczego człowieka". Odpowiada to pierwszej definicji „*identity*". Po trzecie, są to „fakty, cechy i dane personalne pozwalające zidentyfikować jakąś osobę", co pozostaje bliskie pierwszej definicji anglojęzycznej ujętej w literze a. Po czwarte, jest to „w odniesieniu do społeczności: świadomość wspólnych cech i poczucie jedności", co odpowiada pierwszej definicji anglojęzycznej ujętej w literze b. Piąte znaczenie terminu „tożsamość" wymieniane przez SJP jest zgodne z objaśnieniem znaczenia „*identity*" podanym przez *Merriam-Webster's Dictionary* w punkcie 4.

W kontekście tematyki niniejszego artykułu istotne jest przede wszystkim ujęcie pojęcia tożsamości jako wiedzy o faktach, cechach i danych personalnych pozwalających zidentyfikować jakąś osobę. Mimo że jest to definicja słownikowa, a nie specjalistyczna i oparta na dogłębnych badaniach z dziedziny socjologii, nauk prawnych czy nauk o bezpieczeństwie, jest ona dość pojemna i kierunkowo prawidłowa, gdyż prowadzi do konkluzji, że tożsamość jest związana z potrzebą identyfikacji danej osoby, tj. zweryfikowania, czy jest ona tą, za którą się podaje, lub tą, za którą ją uważamy. Cechy biometryczne należą do szerszej kategorii danych personalnych i są jedną z podstaw identyfikacji lub weryfikacji tożsamości. Stanowią one część szerszego katalogu danych osobowych, które – zgodnie z rozporządzeniem PE i Rady UE nr 679 z 27 kwietnia 2016 r. – obejmują:

> (…) informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna

[2] https://www.merriam-webster.com/ [dostęp: 1 IX 2020].

[3] Wszystkie tłumaczenia w artykule pochodzą od autora (przyp. red.).

[4] https://sjp.pwn.pl/szukaj/tożsamość.html [dostęp: 1 IX 2020].

> to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[5].

Z kolei w rozporządzeniu PE i Rady UE nr 910 z 23 lipca 2014 r.[6] został sprecyzowany termin „identyfikacja elektroniczna". Zgodnie z art. 3 pkt 1 wspomnianego rozporządzenia oznacza on (…) *proces używania danych* w *postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną*. W Polskiej Normie PN-I-02000 „tożsamość" zdefiniowano natomiast jako (…) *element danych przypisany podmiotowi i wykorzystywany do jego identyfikowania*", a „identyfikowanie" jako (…) *proces zautomatyzowanego rozpoznania określonego użytkownika* w *systemie, możliwy do zrealizowania dzięki zastosowaniu unikalnych nazw*.

Katalog danych personalnych określony przepisami prawa jest otwarty i główną przesłanką jest to, czy dana informacja umożliwia pośrednie lub bezpośrednie zidentyfikowanie konkretnej osoby. W przypadku identyfikacji elektronicznej omawiane dane są zapisane w postaci elektronicznej i – co interesujące – ten katalog może się odnosić także do osób prawnych. Takie pojmowanie danych osobowych (w odniesieniu do osób fizycznych) jest w zasadzie spójne ze słownikowym rozumieniem tożsamości jako faktów, cech i danych personalnych pozwalających zidentyfikować jakąś osobę. Jest to jednak pojmowanie zbyt wąskie i nie obejmuje szczególnego atrybutu tożsamości, jakim jest jestestwo człowieka i to wszystko, co konstytuuje go jako jedną osobę, niepowtarzalną w wymiarze fizycznym i umysłowym. Jak wskazuje Olga Sakson-Obada, wymiar fizyczny jest istotny dla tożsamości, gdyż ciało każdego człowieka jest wyjątkowe, jedyne w swoim rodzaju i ma zestaw cech, jakich nie ma żadna inna istota ludzka[7]. Z kolei wymiar psychiczny ma, według Brunona Hołysta, ogromny wpływ na przebieg procesu stawania się sobą i obejmuje trzy najważniejsze poziomy: poziom przeszłości i pamięci, poziom teraźniejszości i tworzenia nowej wiedzy oraz poziom przyszłości – fantazji i wyobraźni[8].

---

[5] Art. 4 pkt 1) *Rozporządzenia 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. UE L 119 z 4 V 2016 r.).

[6] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE* (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

[7] O. Sakson-Obada, *Rozwój ja cielesnego w kontekście wczesnej relacji z opiekunem*, „Roczniki Psychologiczne" 2008, nr 2, s. 29–31.

[8] B. Hołyst, *Bezpieczeństwo jednostki*, Warszawa 2014, s. 236–237.

W literaturze socjologicznej wskazuje się, że tożsamość, w tym tożsamość pojedynczego człowieka, jest zjawiskiem dynamicznym i ulega zmianom pod wpływem interakcji społecznych[9]. Równocześnie jednak tożsamość, zwłaszcza w odniesieniu do grup społecznych, pozostaje czynnikiem zapewniającym trwałość, stabilizację oraz ciągłość[10]. Można przyjąć, że gdy mówi się o dynamice tożsamości człowieka, ma się na myśli nie tylko wymiar kulturowy i światopoglądowy, lecz także biologiczny, związany choćby z procesem starzenia. Z upływem czasu człowiek podlega zmianom. Czy zatem tożsamość człowieka jest zmienna i nietrwała? Jeśli tak, to „ten sam", wydawałoby się, człowiek w perspektywie czasu nie będzie „tym samym" człowiekiem, ale kimś zgoła innym. Jego jednostkowe cechy określające fizyczną, fizjologiczną, genetyczną tożsamość mogą przecież ulec zmianie. Nawet tak, zdawałoby się, trwałe w czasie cechy biometryczne człowieka, jak odcisk jego palca czy nawet DNA[11], mogą się – w sposób intencjonalny lub nieintencjonalny – zmienić. Jak zatem zdefiniować tę tożsamość, pod którą – pomimo zmian zachodzących w czasie – kryje się ten sam człowiek?

Obecnie literatura przedmiotu nie dostarcza wystarczająco satysfakcjonującej definicji pojęcia „tożsamość" w odniesieniu do jednostki. Socjologowie wiążą ją z procesem nadawania ludziom społecznej egzystencji[12]. Krzysztof Gorazdowski łączy tożsamość z kształtującym ją zdobywaniem przez całe życie wiedzy i umiejętności, poszerzaniem zasobów intelektualnych oraz rozbudowywaniem strategii radzenia sobie w różnych sytuacjach życiowych[13]. Wskazuje ponadto na podstawową funkcję tożsamości, którą jest identyfikowanie osoby lub grupy na podstawie wybranych cech[14]. Izabela Jankowska ogranicza pojmowanie tożsamości praktycznie do danych osobowych zawartych w dokumentach tożsamości[15]. Podobne, równie wąskie rozumienie prezentuje Kamil Sowirka[16]. Definicja tożsamości, którą posługuje się Katarzyna Cygan, jest z kolei podobna do tej zawartej w *Słowniku języka polskiego.* Jej zdaniem są to (…) *fakty, cechy, dane personalne pozwalające zidentyfikować jakąś osobę, ale także świadomość siebie*[17].

---

[9] Z. Mach, *Przedmowa*, w: T. Paleczny, *Socjologia tożsamości*, „Rejony Humanistyki" 2015, nr 1, s. 9.

[10] E. Ardener, *Tożsamość i utożsamienie*, w: *Sytuacja mniejszościowa i tożsamość*, Z. Mach, A. Paluch (red.), Kraków 1992, s. 21–42; Z. Bokszański, *Tożsamość, interakcja, grupa: tożsamość jednostki w perspektywie teorii socjologicznej*, Łódź 1989, s. 206–207.

[11] Za prace nad metodami modyfikacji genomu (CRISPR/Cas9) Nagrodę Nobla w dziedzinie chemii otrzymały w 2020 r. Emmanuelle M. Charpentier i Jennifer A. Doudna.

[12] P.L. Callero, *The sociology of Self*, „Annual Review of Sociology" 2003, nr 29, s. 115–133.

[13] K. Gorazdowski, *Kradzież tożsamości w sieci w ujęciu normatywno-opisowym*, „Studia Administracji i Bezpieczeństwa" 2017, nr 2, s. 91–92.

[14] Tamże, s. 92.

[15] I.M. Jankowska, *Ochrona dokumentów tożsamości w polskim prawie karnym*, „Studia Lubuskie" 2016, t. 12, s. 19.

[16] K. Sowirka, *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, nr 1, s. 65, 78.

[17] K. Cygan, *Czyn złośliwego podszywania się pod inną osobę*, „Studia Prawnoustrojowe" 2015, nr 29, s. 68.

Zasadne jest więc, zdaniem autora, zaproponowanie własnej definicji tożsamości człowieka. Stanowi ona całokształt wszystkich cech fizycznych, fizjologicznych, genetycznych i psychicznych oraz identyfikatorów w postaci imienia, nazwiska, jak również innych indywidualnie nadanych identyfikatorów, łącznie konstytuujących jego indywidualność i niepowtarzalność. Zgodnie z tą definicją to nie jeden czynnik ani nawet kilka czynników przesądza o tożsamości osoby, lecz ich całokształt. Jak wskazano wcześniej, cechy fizyczne, fizjologiczne oraz genetyczne człowieka mogą ulec zmianie. Dotyczy to również jego atrybutów psychicznych, w tym nawet – na skutek choroby – osobistych przekonań o własnej tożsamości. Te zmiany nie powodują jednak, że mamy do czynienia z nową tożsamością, nigdy nie odbywają się one bowiem *en bloc*. Zarówno naturalny proces starzenia, jak i choroby nie modyfikują wszystkich indywidualnych cech danego człowieka. Nawet celowa manipulacja tymi cechami, w tym interwencja medyczna, nie jest możliwa w stosunku do wszystkich cech konstytuujących indywidualność i niepowtarzalność danego człowieka. Stosunkowo łatwa natomiast może być próba dokonania zmiany identyfikatorów takich, jak imię i nazwisko czy numer PESEL lub innych indywidualnych identyfikatorów służących np. do uwiarygodniania się w systemach teleinformatycznych. To najczęściej spotykane przykłady kradzieży tożsamości, polegające na posłużeniu się cudzymi danymi osobowymi przez osobę nieupoważnioną i przybraniu cudzej tożsamości[18]. Jednak tego rodzaju zdarzenia stwarzają jedynie pozory nowej czy cudzej tożsamości. Przestępca przybierający cudze imię i nazwisko nie uzyskuje tożsamości prawowitego właściciela tych danych osobowych, nie jest bowiem w stanie przejąć całokształtu cech konstytuujących indywidualność i niepowtarzalność drugiego człowieka. Rację ma zatem Piotr Girdwoyń, który zwraca uwagę, że (…) *przypisywanie jakiejkolwiek cesze (lub zespołowi cech) obiektu identyfikowanego waloru unikalności nie wydaje się możliwe, gdyż zawsze jej rzadkość, stanowiąca podstawową przesłankę indywidualności, jest odnoszona w najlepszym wypadku jedynie do klasy wszystkich przebadanych obiektów danego rodzaju i nie musi mieć waloru uniwersalnego*[19]. Raz jeszcze należy więc podkreślić, że pewność co do tożsamości człowieka nie może być oparta wyłącznie na jednej czy kilku jego cechach lub identyfikatorach. Absolutną pewność może dać jedynie całokształt tych cech i identyfikatorów, chociaż w praktyce, z przyczyn pragmatycznych, mamy do czynienia z pewnością opartą na rachunku prawdopodobieństwa (o ile dane zjawisko jest możliwe do skwantyfikowania) lub zwykłym subiektywnym osądzie[20].

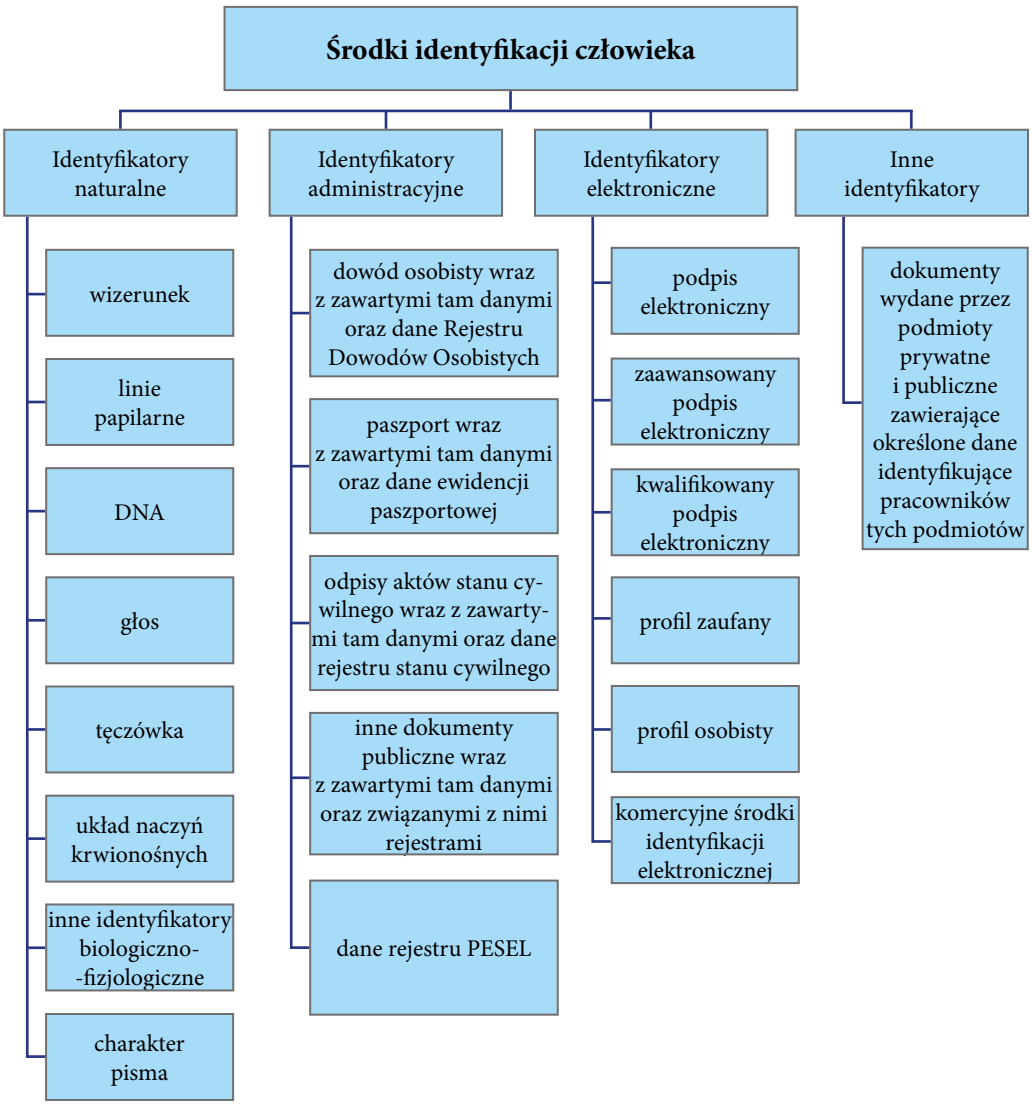
[18] A. Lach, *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3, s. 29.

[19] P. Girdwoyń, *Zarys kryminalistycznej taktyki obrony*, Kraków 2004, s. 223.

[20] J. Moszczyński, *Dylematy identyfikacji indywidualnej i grupowej*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, s. 184–185.

Zdalna identyfikacja

W praktyce do identyfikacji człowieka są wykorzystywane różne środki. Przedstawiono je na schemacie zamieszczonym poniżej.



Schemat. Klasyfikacja środków służących do identyfikacji człowieka.

Źródło: Opracowanie własne.

W przypadku środków identyfikacji elektronicznej należy wskazać podstawowe procesy, w których są one wykorzystywane. W literaturze przedmiotu najczęściej wymienia się cztery, tj.:

a) rejestrację,
b) weryfikację tożsamości i wydanie środków identyfikacji elektronicznej,
c) uwierzytelnienie,
d) autoryzację.

Powyższe procesy składają się na identyfikację zdalną. Etap rejestracji obejmuje deklarację tożsamości wraz z przekazaniem określonych atrybutów tożsamości, np. imienia i nazwiska (identyfikatorów administracyjnych) lub cech biometrycznych (identyfikatorów naturalnych) takich, jak wizerunek twarzy czy odciski palców. Najważniejszym zadaniem jest sprawdzenie, czy zadeklarowane dane rzeczywiście należą do osoby je przedstawiającej. Służy temu proces weryfikacji tożsamości, polegający na skonfrontowaniu deklarowanych danych z danymi ujętymi w wiarygodnych źródłach. Przykładowo, klasyczną metodą weryfikacji tożsamości jest porównanie deklarowanych danych osobowych z danymi w dowodzie osobistym oraz porównanie wizerunku twarzy osoby podlegającej weryfikacji z wizerunkiem widniejącym w jej dowodzie osobistym. Istotna w tym przypadku jest możliwość powiązania analizowanych danych osobowych z tożsamością fizyczną takiej osoby, stąd porównanie wizerunku twarzy jako cechy składającej się na tożsamość fizyczną. Możliwe jest wykorzystanie także innych niż dowód osobisty źródeł danych, z zastrzeżeniem jednak, że powinny one być wiarygodne i wymagać wykazania związku z tożsamością fizyczną (na etapie ich użycia w procesie weryfikacji lub na etapie ich wydania). Na podstawie pozytywnej weryfikacji tożsamości mogą zostać wydane środki identyfikacji elektronicznej, tj. materialne lub niematerialne jednostki zawierające dane identyfikujące osobę i używane do celów uwierzytelniania podczas usługi online. Powstaje w ten sposób tożsamość elektroniczna, która – poprzez użycie otrzymanych środków identyfikacji elektronicznej – może być wykorzystywana w cyberprzestrzeni, jednak każdorazowo będzie ona podlegać uwierzytelnieniu i autoryzacji. Należy przy tym podkreślić, że istnieją procesy identyfikacji elektronicznej, w których weryfikacja tożsamości nie następuje (są przyjmowane zadeklarowane dane osobowe), lub takie, w których weryfikacja ma bardzo uproszczoną formę, np. polega na przesłaniu pocztą elektroniczną skanu dowodu osobistego. Dotyczy to jednak sytuacji, w których poziom ryzyka wynikający z takich odstępstw jest akceptowalny.

Uwierzytelnienie oznacza weryfikację zadeklarowanej tożsamości elektronicznej, np. przez podanie właściwego hasła przypisanego do indywidualnego loginu osoby uprawnionej do korzystania z danego systemu lub zbioru danych czy też porównanie przekazywanych danych biometrycznych z danymi przyporządkowanymi do wskazanej tożsamości. Z kolei autoryzacja jest procesem potwierdzającym, czy użytkownik ma uprawnienie do wykonania określonej operacji (np. zlecenia transakcji przelewu) lub uprawnienie dostępu do określonego zasobu (np. pliku). Celem autoryzacji jest kontrola dostępu, a zatem następuje ona po uwierzytelnianiu. W art. 4 pkt 29 dyrektywy PE i Rady UE nr 2366 z 25 listopada 2015 r.[21] zdefiniowano jednak uwierzytelnienie

[21] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE,*

znacznie szerzej, jako (…) *procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika*.

Wskazane powyżej cztery procesy składają się na proces identyfikacji zdalnej, tj. sprawdzenie z odpowiednim poziomem ufności, czy dana osoba usiłująca dokonać określonej czynności w sposób zdalny jest osobą do tego uprawnioną, i pozyskanie informacji określających tożsamość tej osoby. Środki identyfikacji elektronicznej różnią się między sobą konstrukcją technologiczną i poziomem bezpieczeństwa. Powszechnie stosowane są środki identyfikacji polegające na indywidualnie przyporządkowanym do użytkownika loginie (i haśle), wydanym na podstawie samodzielnej rejestracji w określonym systemie informatycznym, z pominięciem etapu weryfikacji tożsamości. W kontaktach z podmiotami sektora publicznego środkiem identyfikacji elektronicznej szeroko stosowanym w Polsce jest profil zaufany. Znacznie rzadziej obywatele naszego kraju korzystający z usług tego sektora posługują się elektronicznym dowodem osobistym (profil osobisty). W sektorze komercyjnym klasycznymi środkami identyfikacji elektronicznej są elektroniczny podpis kwalifikowany oraz bankowe środki identyfikacji elektronicznej. Ponadto funkcjonuje wiele różnego rodzaju innych środków, których poziom bezpieczeństwa jest znacznie niższy.

Specyfika niektórych czynności realizowanych za pośrednictwem sieci wymaga uzyskania pewności co do tożsamości osoby, która je wykonuje. Dotyczy to zwłaszcza czynności prawnych (np. składanie oświadczeń woli), zatwierdzania określonych czynności w systemach teleinformatycznych organizacji i przeprowadzania transakcji finansowych w systemach bankowości internetowej lub mobilnej. Podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi zostały uregulowane w rozporządzeniu PE i Rady UE nr 910 z 23 lipca 2014 r.[22] Wybór określonego środka identyfikacji elektronicznej powinien być uzależniony od niezbędnego poziomu bezpieczeństwa dla danej czynności wymagającej uwierzytelnienia w cyberprzestrzeni. Poziom wymaganego bezpieczeństwa oznacza stopień, w jakim można mieć zaufanie do danego identyfikatora elektronicznego przy ustalaniu tożsamości osoby, która się nim posługuje. Poziom ten zależy zatem od stopnia zaufania do podawanej lub zgłaszanej tożsamości danej osoby zapewnianego przez ten identyfikator, przy uwzględnieniu określonych procesów (np. potwierdzanie i weryfikowanie tożsamości oraz uwierzytelnianie), działań zarządczych (np. działania jednostki wydającej identyfikator elektroniczny i procedury wydawania takich identyfikatorów) oraz stosowanych zabezpieczeń technicznych.

2009/110/ WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/ WE (Dz. Urz. UE L 337 z 23 XII 2015 r.).

[22] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE* (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

W przypadku notyfikowanego systemu identyfikacji elektronicznej istnieje wymóg określenia poziomu bezpieczeństwa środka identyfikacji elektronicznej wydanego w ramach tego systemu[23]. Niski poziom bezpieczeństwa odnosi się do środka, (…) *który zapewnia ograniczony stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest obniżenie ryzyka podszycia się lub modyfikacji tożsamości*[24]. Średni poziom bezpieczeństwa odnosi się do środka, (…) *który zapewnia średni stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest znaczne obniżenie ryzyka podszycia się lub modyfikacji tożsamości*[25]. Przykładem takiego środka jest profil zaufany. Wysoki poziom bezpieczeństwa odnosi się do środka, (…) *który zapewnia wyższy stopień zaufania względem podawanej lub zgłaszanej tożsamości danej osoby niż środek identyfikacji elektronicznej o średnim poziomie pewności i jest charakteryzowany w odniesieniu do technicznych specyfikacji, standardów i procedur powiązanych z nim, w tym zabezpieczeń technicznych, których celem jest zapobieganie podszyciu się lub modyfikacji tożsamości*[26]. Przykładami takich środków są profil osobisty oraz kwalifikowany podpis elektroniczny.

Szczegółowe, minimalne specyfikacje techniczne i procedury dotyczące poziomów zaufania w zakresie środków identyfikacji elektronicznej, zwłaszcza podpisu elektronicznego, zaawansowanego podpisu elektronicznego oraz kwalifikowanego podpisu elektronicznego, są określone w rozporządzeniu wykonawczym Komisji UE nr 1502 z 8 maja 2015 r.[27]

Weryfikacja tożsamości ma szczególne znaczenie, o czym już wspomniano, w sektorze bankowym. Zgodnie ze stanowiskiem Urzędu Komisji Nadzoru Finansowego (UKNF) z 5 czerwca 2019 r. w przypadku, gdy nie ma możliwości skorzystania z powyższych środków identyfikacji elektronicznej, bank powinien rozważyć zastosowanie wzmożonych środków bezpieczeństwa finansowego[28]. Obowiązkiem banku jest ustalenie, jakimi dokumentami, danymi oraz informacjami (tj. materiałami weryfikacyjnymi) należy się w takiej sytuacji posługiwać w celu weryfikacji tożsamości klienta, a także jakie

[23] Tamże, art. 8 ust. 1.

[24] Tamże, art. 8 ust. 2 lit. a.

[25] Tamże, art. 8 ust. 2 lit. b.

[26] Tamże, art. 8 ust. 2 lit. c.

[27] *Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 maja 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym* (Dz. Urz. UE L 235 z 9 IX 2015 r.).

[28] https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf [dostęp: 1 IX 2020].

sposoby uzyskiwania dostępu do materiałów weryfikacyjnych będą stosowane. Ponadto w celu zdalnej weryfikacji tożsamości klienta bank powinien rozważyć posłużenie się różnymi materiałami weryfikacyjnymi pochodzącymi z wiarygodnych i niezależnych źródeł. W przypadku weryfikacji tożsamości osoby fizycznej przynajmniej jeden z materiałów weryfikacyjnych powinien być dokumentem stwierdzającym tożsamość (dowód osobisty, paszport, karta pobytu). Innym tego rodzaju materiałem wskazanym przez UKNF jest dokument ze zdjęciem, np. prawo jazdy. Za uzupełniające dokumenty potwierdzające tożsamość klienta i adres jego pobytu można uznać np. rachunki za media. Dodatkowym środkiem bezpieczeństwa, którego stosowanie jest oczekiwane przez UKNF, jest zrealizowanie pierwszej transakcji za pomocą przelewu bankowego z rachunku klienta (prowadzonego w innej instytucji obowiązanej) na rzecz banku weryfikującego jego tożsamość. Z uwagi jednak na minimalny zakres danych osobowych zawartych w informacji o przelewie, powinny one służyć pomocniczo do weryfikacji tożsamości klienta.

Metodą dopuszczoną przez UKNF jest także wideoweryfikacja. W tym przypadku konieczne jest przeprowadzenie analizy ryzyka, z uwzględnieniem m.in. modelu funkcjonowania usługi, możliwych do zastosowania technologii i dostosowanych do nich mechanizmów kontrolnych zapewniających odpowiedni poziom bezpieczeństwa usługi, zwłaszcza mitygowanie różnych rodzajów ryzyka[29] związanych z prawidłową identyfikacją i weryfikacją klienta (np. ryzyka kradzieży tożsamości), w tym odnoszących się do wiarygodności materiałów weryfikacyjnych. Zgodnie ze stanowiskiem UKNF bank może uzyskiwać dostęp do materiałów weryfikacyjnych za pomocą wideorozmowy, podczas której pracownik banku ma możliwość bliższej obserwacji klienta i przedstawionych przez niego oryginałów dokumentów, a także upewnienia się, że materiały weryfikacyjne nie zostały sfałszowane, porównania fotografii w dokumencie tożsamości z osobą, z którą rozmawia, oraz sprawdzenia klienta w wiarygodnych bazach danych. Niezależnie od powyższego bank powinien wziąć pod uwagę czynniki behawioralne, które mogą wskazywać, że klient np. jest pod wpływem środków odurzających, nie działa samodzielnie bądź nie jest świadomy, że nawiązuje relację z bankiem.

Zgodnie z art. 79 dyrektywy PE i Rady UE nr 2366 w sprawie usług płatniczych w ramach rynku wewnętrznego[30] państwa członkowskie mają zapewnić stosowanie przez dostawcę usług płatniczych silnego uwierzytelniania klienta, w przypadku gdy płatnik: a) uzyskuje dostęp do swojego rachunku płatniczego w trybie online; b) inicjuje elektroniczną transakcję płatniczą; c) przeprowadza czynność za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć. W sytuacji inicjowania elektronicznych transakcji płatniczych państwa członkowskie są natomiast zobowiązane do tego, aby w odniesieniu do elektronicznych zdalnych

[29] Mitygowanie ryzyka – podejmowanie działań zmierzających do obniżenia poziomu ryzyka do akceptowalnego poziomu (przyp. red.).

[30] Dyrektywa została implementowana do polskiego prawa w ramach znowelizowanej *Ustawy* z *dnia 19 sierpnia 2011 r.* o *usługach płatniczych* (DzU z 2011 r. nr 199 poz. 1175, ze zm.), a omawiany przepis tej dyrektywy ujęto w art. 32i wspomnianej ustawy.

transakcji płatniczych dostawcy usług płatniczych stosowali silne uwierzytelnianie klienta, obejmujące elementy, które dynamicznie łączą transakcję z określoną kwotą i określonym odbiorcą. Przez silne uwierzytelnianie klienta należy rozumieć uwierzytelnianie z wykorzystaniem co najmniej dwóch elementów (niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych) należących do kategorii: wiedza (coś, co wie wyłącznie użytkownik), posiadanie (coś, co ma wyłącznie użytkownik) i cechy klienta (coś, czym jest użytkownik), które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających (art. 4 pkt 30 dyrektywy PE i Rady UE nr 2366).

Słabe strony zdalnej identyfikacji i związane z tym wyzwania

Podstawowym mankamentem współcześnie stosowanych środków identyfikacji elektronicznej jest to, że potwierdzają one jedynie fakt posiadania przez osobę identyfikującą się (uwierzytelniającą się lub autoryzującą określoną czynność) indywidualnych środków przypisanych uprawnionej osobie (loginów, haseł itd.). Wspomniane środki nie pozwalają bowiem na weryfikację, kto fizycznie się nimi posługuje. A zatem współczesna zdalna identyfikacja odbywa się na podstawie domniemania, że środki identyfikacji są zawsze w wyłącznym posiadaniu osób uprawnionych. Praktyka wskazuje natomiast, że jest możliwe przejęcie tego rodzaju danych pozwalających podszywać się pod inną osobę (kradzież tożsamości). Stosowane obecnie środki nie spełniają podstawowego celu uwierzytelnienia, którym jest weryfikacja tożsamości użytkownika usług, a jedynie weryfikują posiadanie przez użytkownika wymaganych indywidualnych danych. Ponieważ możliwe jest ich przejęcie przez przestępców, dlatego przy zdalnym dokonywaniu transakcji nie ma pewności, kto faktycznie dokonuje tych operacji. Wiadomo jedynie, że są one realizowane przez osobę dysponującą danymi uwierzytelniającymi, tj. indywidualnymi cechami zapewnianymi przez dostawcę usług użytkownikowi do celów uwierzytelnienia.

Należy zaznaczyć, że art. 66 dyrektywy PE i Rady UE nr 2366 dotyczący usług płatniczych realizowanych w ramach rynku wewnętrznego nakłada na dostawców usług inicjowania płatności obowiązek zapewnienia, aby indywidualne dane uwierzytelniające użytkownika usług płatniczych nie były – z wyjątkiem użytkownika i wydawcy takich indywidualnych danych uwierzytelniających – dostępne dla innych stron oraz by były przekazywane przez dostawcę świadczącego usługę inicjowania płatności za pośrednictwem bezpiecznych i wydajnych kanałów. Równocześnie, zgodnie z art. 69 wspomnianej dyrektywy, użytkownik usług płatniczych z chwilą otrzymania instrumentu płatniczego jest zobowiązany do podjęcia wszelkich racjonalnych kroków, aby chronić swoje indywidualne dane uwierzytelniające. Dostawca usług płatniczych wydający instrument płatniczy jest z kolei zobowiązany do upewnienia się, że indywidualne dane uwierzytelniające nie są dostępne dla stron innych niż użytkownik usług płatniczych, który jest uprawniony do używania tego instrumentu płatniczego (art. 70). Niemniej jednak te wymogi nie eliminują ryzyka przejęcia rzeczonych danych przez

przestępców. Przyczyną opisanych słabości zdalnej identyfikacji jest charakter weryfikowanych danych. Nawet po wdrożeniu procedur uwzględniających silne uwierzytelnienie banki najczęściej korzystają z cech należących wyłącznie do dwóch obszarów: coś, co wiem (np. hasło logowania) i coś, co posiadam (np. telefon komórkowy, na który przychodzą wiadomości SMS z kodami do autoryzacji, lub urządzenie mobilne, na którym jest zainstalowany program (token) wyświetlający kody do autoryzacji). Rzadko są uwzględniane cechy z obszaru: coś, czym jestem, tj. indywidualne cechy użytkownika, ograniczone w zasadzie do jego cech biometrycznych. Korzystanie z cech biometrycznych jest w omawianej sytuacji utrudnione, gdyż generuje wymóg dysponowania wzorcem, z którym należałoby porównywać weryfikowane dane. Z uwagi na wrażliwy charakter danych biometrycznych i społeczną niechęć do ich przekazywania nie są one przechowywane w bazach banków. W przypadkach stosowania biometrii w systemach bankowych (głównie w odniesieniu do aplikacji mobilnych) dane biometryczne (najczęściej odciski palców) nie są przechowywane w banku, lecz zapisane tylko i wyłącznie na karcie kryptograficznej, którą posiada użytkownik. Takie lokalne umieszczenie danych biometrycznych może wydawać się wygodne, lecz generuje ryzyko przejęcia tego wzorca przez przestępców i zastąpienia go danymi osoby nieuprawnionej, np. w celu uzyskania kontroli nad rachunkiem bankowym i wytransferowania z niego środków finansowych. Nie istnieje także krajowa baza danych biometrycznych wszystkich obywateli, która mogłaby służyć jako źródło omawianych wzorców.

Pewną alternatywną próbą wykorzystania biometrii w bankowości jest wspomniana już wideoweryfikacja, w ramach której pracownik banku w czasie rzeczywistym weryfikuje tożsamość klienta przez porównanie jego wizerunku z kamery z wizerunkiem widniejącym na fotografii dokumentu tożsamości okazanego także do kamery. Słabymi stronami tego rozwiązania są: stosunkowo długi czas weryfikacji (ograniczający stosowanie tej metody wyłącznie do nawiązywania relacji gospodarczych i wykluczający posługiwanie się nią w celu uwierzytelniania), trudność związana z poprawną zdalną weryfikacją autentyczności dowodu tożsamości (wyłącznie przez obraz z kamery), ograniczone zdolności pracowników banków w zakresie weryfikacji tożsamości na podstawie wizerunku. Omawianą metodę należy więc uznać za jedynie pozornie bezpieczną.

Nowy model zdalnej identyfikacji

Odpowiedzią na zdiagnozowane słabości stosowanych obecnie środków i metod identyfikacji elektronicznej może być przedstawiony w niniejszym artykule model bazujący na zdalnej identyfikacji za pomocą danych biometrycznych zapisanych w dokumencie tożsamości – elektronicznym dowodzie osobistym lub paszporcie. Zamysł tego rozwiązania opiera się na wykorzystaniu w procesie weryfikacji:

1) danej biometrycznej w postaci wizerunku twarzy pobieranego w czasie rzeczywistym w trakcie identyfikacji (uwierzytelniania lub autoryzacji) z kamery telefonu komórkowego lub komputera,

2) wzorca biometrycznego w postaci wizerunku twarzy zapisanego w mikroprocesorze dowodu osobistego[31] lub paszportu[32].

Proces weryfikacji tożsamości z zastosowaniem omawianego modelu obejmuje następujące kroki:

1. Pozyskanie dostępu aplikacji do mikroprocesora przez zdjęcie pola MRZ dokumentu.
2. Automatyczną weryfikację statusu dokumentu (certyfikatu na chipie CSCA/CVCA).
3. Automatyczny odczyt danych z mikroprocesora przy użyciu czytnika NFC wbudowanego w telefon lub laptop:
   – DG1: Wydawca dokumentu,
   – DG1: Numer dokumentu,
   – DG1: Data narodzin,
   – DG1: Płeć,
   – DG1: Data wygaśnięcia dokumentu,
   – DG1: Narodowość,
   – DG1: Imię i nazwisko posiadacza dokumentu,
   – DG2: Biometryczne zdjęcie twarzy posiadacza dokumentu.
4. Wykonanie fotografii twarzy przez użytkownika z techniczną pomocą aplikacji.
5. Weryfikację funkcji życiowych użytkownika (sprawdzenie wiarygodności danych uzyskanych dzięki działaniu wskazanemu w pkt 4, tzn. tego, czy przed telefonem lub laptopem jest faktycznie żywa osoba, czy też jest to podstawione zdjęcie lub obraz wideo).
6. Weryfikację tożsamości użytkownika na podstawie algorytmicznej analizy obrazów: wizerunku twarzy z mikroprocesora oraz wizerunku twarzy pobranej w czasie rzeczywistym z kamery.
7. Raportowanie wyniku weryfikacji: weryfikacja pozytywna lub weryfikacja negatywna.
8. Opcjonalną ponowną weryfikację tożsamości w przypadku negatywnego wyniku pierwszej weryfikacji lub wsparcie użytkownika w procesie weryfikacji przez zdalnego konsultanta.
9. Archiwizację procesu weryfikacji tożsamości w systemie bankowym.

Wyjątkowymi zaletami omawianego modelu są:

1) wykorzystanie zaufanego i powszechnego środka identyfikacji w postaci dowodu osobistego lub paszportu,

[31] Dowody osobiste wydawane obecnie w Polsce są wyposażone w mikroprocesory zawierające dane biometryczne. Od 2 sierpnia 2021 r. biometryczne dowody osobiste (z dwiema cechami) obowiązują na terenie całej UE.

[32] Wszystkie paszporty wydawane obecnie w kraju i na świecie są wyposażone w mikroprocesory zawierające dane biometryczne.

2) uniwersalny charakter wykorzystanego środka identyfikacji, tj. polskich i zagranicznych paszportów oraz dowodów osobistych,
3) wykorzystanie danych biometrycznych, dających wymaganą i obiektywną pewność co do wyniku weryfikacji tożsamości,
4) uzyskanie pewności co do autentyczności dowodu osobistego lub paszportu,
5) łatwość i szybkość procesu weryfikacji tożsamości, niewymagającego żadnego oprzyrządowania poza telefonem komórkowym lub laptopem z kamerą i czytnikiem NFC,
6) duża liczba różnego rodzaju zastosowań w sektorze bankowym i innych sektorach (pozyskiwanie nowych klientów, autoryzacja transakcji, uwierzytelnianie w kanałach zdalnych, identyfikacja w bankowości oddziałowej i inne),
7) niski poziom błędu.

Dzięki automatyzacji procesu oraz bazowaniu na danych zapisanych na mikroprocesorze w przedstawionym modelu zostaje wyeliminowany subiektywizm w ocenie autentyczności dokumentu oraz w ocenie zgodności wizerunku klienta z jego wizerunkiem w dowodzie tożsamości. W ten sposób można znacznie podnieść poziom bezpieczeństwa tożsamości i transakcji realizowanych w systemach bankowych oraz innego rodzaju transakcji wymagających pewności co do tożsamości wykonujących je osób. Poziom trafności modelu, tj. prawidłowe powiązanie wizerunku użytkownika w czasie rzeczywistym z jego zdjęciem z dowodu osobistego (lub paszportu), jest uzależniony od ustalonego przez bank minimalnego poziomu zgodności (pomiędzy zdjęciem „na żywo" a wzorcem wizerunku zapisanym na dokumencie) i wynika z zastosowanych bibliotek algorytmów rozpoznawania twarzy.

Bibliografia

Adamkiewicz-Drwiłło H.G., *Współczesna metodologia nauk ekonomicznych*, Toruń 2008, TNOiK.

Ardener E., *Tożsamość i utożsamienie*, w: *Sytuacja mniejszościowa i tożsamość*, Z. Mach, A. Paluch (red.), Kraków 1992, Wydawnictwo UJ, s. 21–42.

Bokszański Z., *Tożsamość, interakcja, grupa: tożsamość jednostki w perspektywie teorii socjologicznej*, Łódź 1989, Wydawnictwo UŁ.

Callero P.L., *The sociology of the Self*, „Annual Review of Sociology" 2003, nr 29, s. 115–133.

Cygan K., *Czyn złośliwego podszywania się pod inną osobę*, „Studia Prawnoustrojowe" 2015, nr 29, s. 59–79.

Girdwoyń P., *Zarys kryminalistycznej taktyki obrony*, Kraków 2004, Zakamycze.

Gorazdowski K., *Kradzież tożsamości w sieci w ujęciu normatywno-opisowym*, „Studia Administracji i Bezpieczeństwa" 2017, nr 2, s. 89–102.

Hołyst B., *Bezpieczeństwo jednostki*, Warszawa 2014, Wydawnictwo Naukowe PWN.

Jankowska I.M., *Ochrona dokumentów tożsamości w polskim prawie karnym*, „Studia Lubuskie" 2016, t. 12, s. 13–28.

Lach A., *Kradzież tożsamości*, „Prokuratura i Prawo" 2012, nr 3, s. 29–39.

Mach Z., *Przedmowa*, w: T. Paleczny, *Socjologia tożsamości*, „Rejony Humanistyki" 2015, nr 1, s. 7–16.

Moszczyński J., *Dylematy identyfikacji indywidualnej i grupowej*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, Volumina.pl.

Sakson-Obada O., *Rozwój ja cielesnego w kontekście wczesnej relacji z opiekunem*, „Roczniki Psychologiczne" 2008, nr 2, s. 27–44.

Sowirka K., *Przestępstwo „kradzieży tożsamości" w polskim prawie karnym*, „Ius Novum" 2013, nr 1, s. 64–80.

Źródła internetowe

https://www.merriam-webster.com/.

Stanowisko UKNF dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_dot_identyfikacji_klienta_i_weryfikacji_jego_tozsamosci_w_bankach_oraz_oddzialach_instytucji_kredytowych_w_oparciu_o_metode_wideoweryfikacji_66066.pdf.

Akty prawne

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. UE L 119 z 4 V 2016 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 VIII 2014 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23 XII 2015 r.).

Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 maja 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 9 IX 2015 r.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (DzU z 2011 r. nr 199 poz. 1175, ze zm.).

Abstrakt

W pracy przeanalizowano proces zdalnej identyfikacji w tej postaci, w jakiej jest on realizowany obecnie. Na tej podstawie zdiagnozowano najważniejsze słabe strony metod wykorzystywanych w tym procesie. W przypadku metod niebiometrycznych ich główną słabością jest ograniczenie ich stosowania do weryfikacji określonych danych uwierzytelniających posiadanych przez użytkownika (osobę weryfikującą się), a nie do weryfikacji tożsamości *per se*. Z kolei stosowane współcześnie metody biometryczne są czasochłonne i obarczone subiektywizmem w ocenie zgodności danych biometrycznych ze wzorcem. Alternatywę dla tych metod stanowi zaprezentowany w niniejszym artykule model, który jest oparty na w pełni zautomatyzowanej, zdalnej identyfikacji biometrycznej, wykorzystującej jako wzorzec dane biometryczne zawarte w dokumentach osobistych i paszportach. Model jest wolny od słabości i ograniczeń innych analizowanych biometrycznych i niebiometrycznych metod identyfikacji i charakteryzuje się bardzo niskim poziomem błędu.

Słowa kluczowe: biometria, identyfikacja, uwierzytelnienie, autoryzacja, tożsamość.

Alternative tools of remote identification and authentication

Abstract

The paper presents an analysis of the present-day process of remote identification. On this basis, the most important weaknesses of the methods were diagnosed. With regard to non-biometric methods, the main weakness and limitation is that they only verify

if the user (the person being verified) has appropriate credentials, and they do not verify the identity per se. On the other hand, the currently applied biometric methods are time-consuming and subjective in assessing the compliance of biometric data with the template. An alternative to these methods is a model, presented in this paper, which is based on fully automated, remote biometric identification using biometric data contained in IDs and passports as a template. The model is free from the weaknesses and limitations of other biometric and non-biometric identification methods analysed in this paper and has a very low error rate.

Keywords: biometrics, identification, authentication, authorization, identity.