Iwona Iskierka

Przetwarzanie danych biometrycznych w usługach elektronicznych = Processing of Biometric Data in Electronic Services

Dydaktyka Informatyki 13, 47-54

2018

Dydaktyka Informatyki 13(2018)
ISSN 2083-3156; e-ISSN 2543-9847
DOI: 10.15584/di.2018.13.7
http://www.di.univ.rzeszow.pl

Uniwersytet Rzeszowski

Iwona ISKIERKA

Dr inż., Politechnika Częstochowska, Wydział Elektryczny, Instytut Informatyki,
ul. Armii Krajowej 17, 42-200 Częstochowa; e-mail: iwona.iskierka@el.pcz.czest.pl

PRZETWARZANIE DANYCH BIOMETRYCZNYCH W USŁUGACH ELEKTRONICZNYCH[1]

PROCESSING OF BIOMETRIC DATA IN ELECTRONIC SERVICES

Słowa kluczowe: usługi elektroniczne, dane osobowe, przetwarzanie danych.
Keywords: electronic services, personal data, data processing.

Streszczenie

W pracy dokonano przeglądu podstawowych zagadnień dotyczących usług zaufania publicznego w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, projektowanych rozwiązań w obszarze ochrony danych osobowych oraz omówiono zagadnienia związane z bezpiecznym korzystaniem z technologii biometrycznych. Zwrócono uwagę na zagrożenia teleinformatyczne, konieczność budowania świadomości społeczeństwa w zakresie bezpieczeństwa danych i ich znaczenia zarówno w pracy zawodowej, jak i w codziennym życiu. Omówiono status prawny technologii biometrycznych z uwzględnieniem aktualnych aktów prawnych. Omówiono pojęcie danych biometrycznych oraz zagadnienia dotyczące przetwarzania danych osobowych, w tym danych biometrycznych.

Abstract

The paper reviews the basic issues concerning public trust services in relation to electronic transactions in the internal market, the proposed solutions in the area of personal data protection and issues related to the safe use of biometric technologies. Attention is paid to ICT threats, the need to build public awareness of the security of data and their significance in both professional work and everyday life. The legal status of biometric technologies has been discussed taking into account current legal acts. Discussed is the concept of biometric data and issues related to the processing of personal data, including biometric data.

[1] Stan prawny na dzień 31 stycznia 2018 r.

Wstęp

Regulacje prawne dotyczące danych osobowych obejmują wiele aktów prawnych[2]. Od roku 1997 prawo dotyczące danych osobowych było nowelizowane w ograniczonym zakresie i w wielu aspektach przestało gwarantować dostateczną ochronę w dobie nowoczesnych technologii XXI wieku. W dniu 13 września 2017 r. Ministerstwo Cyfryzacji przekazało do konsultacji publicznych projekt nowej ustawy o ochronie danych osobowych. Konsultacje trwały do 13 października 2017 r. i miały na celu zebranie możliwie najszerszego spektrum opinii dotyczących projektowanych rozwiązań w obszarze ochrony danych osobowych[3]. Opracowanie projektu nowej ustawy o ochronie danych osobowych wynika także z konieczności zapewnienia stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE)[4]. Każde z państw członkowskich zobowiązane jest do jego wdrożenia do 25 maja 2018 r., a w Polsce za to wdrożenie odpowiada Ministerstwo Cyfryzacji.

Projektowane przepisy ustanawiają nowy organ państwowy – Prezesa Urzędu Ochrony Danych Osobowych, który zaopatrzony zostanie w instrumenty zapewniające jego otwartość na wszelkie konsultacje z przedsiębiorcami oraz obywatelami. Po raz pierwszy projektowane przepisy określać będą także zasady przetwarzania danych biometrycznych zarówno w obszarze zatrudnienia jak i w sektorze bankowym oraz ubezpieczeniowym.

Cyberzagrożenia w świetle aktualnych analiz z dziedziny bezpieczeństwa

KPMG, która jest międzynarodową siecią firm audytorsko-doradczych, zatrudniając obecnie 189 000 osób w 152 krajach na całym świecie, przedstawiła w styczniu 2018 r. raport „Barometr cyberbezpieczeństwa", którego celem było zdiagnozowanie bieżących trendów w polskich przedsiębiorstwach w zakresie ochrony przed cyberprzestępczością[5]. Do badania zaproszono ponad 100 małych, średnich i dużych polskich firm, które były reprezentowane przez osoby

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2016 r., poz. 922); rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., nr 229, poz. 1536); rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r., nr 225, poz. 1350).

[3] https://www.gov.pl/cyfryzacja/konsultacje-spoleczne-projektu-przepisow-wdrazajacych--ogolne-rozporzadzenie-o-ochronie-danych-rodo- (dostęp: 20.01.2018 r.).

[4] http://giodo.gov.pl/1520147/id_art/9278/j/pl (dostęp: 20.01.2018 r.).

[5] https://home.kpmg.com/pl/pl/home/about.html (dostęp: 20.01.2018 r.).

odpowiedzialne za zapewnienie bezpieczeństwa informacji. Przeanalizowano skalę cyberataków na firmy w Polsce, zwracając uwagę na fakt, iż wśród firm działających w Polsce przynajmniej jeden cyberincydent w 2017 r. odnotowało 82% przedsiębiorstw. Wzrost liczby cyberataków w 2017 r. odnotowało 37% firm, natomiast spadek liczby cyberataków 5% firm.

Wśród najgroźniejszych cyberzagrożeń dla firm wymienia się: zaawansowane ukierunkowane ataki (tzw. *Advanced Persistent Threat*), wycieki danych za pośrednictwem złośliwego oprogramowania (malware), kradzież danych przez pracowników, ogólne kampanie ransomware, wyłudzanie danych uwierzytelniających (phishing), ataki wykorzystujące błędy w aplikacjach, wyciek danych w wyniku kradzieży lub zgubienia nośników lub urządzeń mobilnych, ataki na sieci bezprzewodowe, podsłuchiwanie ruchu i ataki Man-in-the-Middle, włamania do urządzeń mobilnych, kradzież danych na skutek naruszenia bezpieczeństwa fizycznego, ataki typu odmowa usługi.

W opinii ekspertów w roku 2018 w obszarze bezpieczeństwa IT będzie kształtowało się około 15 trendów dotyczących prognoz bezpieczeństwa IT[6].

Pierwszy z nich obejmuje zintensyfikowanie wykorzystania sztucznej inteligencji do przewidywania schematów ataków. Kolejny z trendów dotyczy nowych regulacji prawnych odnoszących się między innymi do kwestii ochrony danych osobowych. W maju 2018 r. wchodzi w życie GDPR – *General Data Protection Regulation*. Jest ona bardzo ważna ze względu na to, iż będzie miała wpływ na to, w jaki sposób firmy mogą przetwarzać i przechowywać dane osobowe. GDPR nałoży na organizacje m.in. obowiązek zgłaszania wycieków danych w określonym terminie od wystąpienia zdarzenia. Ponadto GDPR przeniesie odpowiedzialność na kierownictwo firmy, co spowoduje, że bezpieczeństwo przestanie być tylko kwestią techniczną, ale będzie miało konsekwencje dla całej organizacji. Pozostałe trendy dotyczą: kampanii randomware, zwiększenia liczby ataków na bezserwerowe aplikacje, sposobu, w jaki użytkownicy postrzegają prywatność, ataków na hostowane aplikacje biznesowe, czyli takie, które zawierają dane sprzedażowe, dotyczące globalnych kampanii marketingowych oraz danych osobowych klientów, ataków na systemy obsługujące kryptowaluty.

Zwrócono również uwagę na innowacyjne podejście do zwalczania rosnącej liczby zaawansowanych zagrożeń, przez zastosowanie technologii blockchain, która umożliwia przechowywanie danych w rozproszony, zdecentralizowany sposób, zapobiegający wyciekom dużych ilości danych. Umożliwia to przeciwdziałanie manipulowaniu danymi, gdyż wszelkie zmiany są od razu widoczne dla wszystkich podłączonych do danej sieci blockchain.

[6] T. Kowalczyk, *15 trendów bezpieczeństwa w 2018 r.*, „Computerworld" 2018, 01, s. 54–58.

Eksperci od bezpieczeństwa są zgodni, że będzie rosła liczba zagrożeń na urządzenia mobilne. Przewiduje się, iż głównym celem będzie system Android, a cyberprzestępcy nadal będą próbowali wykorzystywać sklep Google Play do dystrybucji szkodliwego kodu.

Usługi zaufania

Uregulowania prawne związane z warunkami funkcjonowania usług zaufania na jednolitym rynku cyfrowym Unii Europejskiej znajdują się w rozporządzeniu 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[7].

W prawie polskim aktem prawnym zawierającym regulacje dotyczące usług zaufania, jak na przykład podpisu elektronicznego, jest ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Wejście w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 implikuje nowy porządek prawny w obszarze usług zaufania, co spowodowało konieczność dostosowania prawa krajowego do nowych uwarunkowań. Celem regulacji zawartych w ustawie o usługach zaufania, identyfikacji elektronicznej i zmianie niektórych ustaw jest wydanie przepisów w odniesieniu do kwestii wskazanych przez eIDAS, jako pozostające w kompetencji państw członkowskich oraz dokonanie koniecznych do prawidłowej realizacji rozporządzenia eIDAS zmian w aktach rangi ustawowej[8].

Dane osobowe, dane biometryczne i ich przetwarzanie w rozumieniu ustawy o ochronie danych osobowych

Zgodnie z art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2 ustawy).

[7] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A31999L0093 (dostęp: 20.01.2018 r.).

[8] https://legislacja.rcl.gov.pl/docs/2/12283556/12343453/12343454/dokument221661.pdf (dostęp: 20.01.2018 r.).

Stosownie do ust. 3 powołanego przepisu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nieracjonalnych, nieproporcjonalnie dużych nakładów kosztów, czasu lub działań[9].

W obszarze rozumienia biometrii oraz danych biometrycznych i możliwości ich przetwarzania funkcjonuje wiele definicji tych pojęć[10].

W dokumencie GIODO zwrócono uwagę na dwie główne kategorie technik biometrycznych, które związane są z rodzajami próbek biometrycznych. Wyróżnia się techniki fizyczne i fizjologiczne oraz techniki behawioralne. W pierwszej grupie technik fizycznych i fizjologicznych wykonuje się pomiary i porównuje fizyczne i fizjologiczne cechy danej osoby. Do cech tych zalicza się: kształt i układ linii papilarnych palca, kształt i układ naczyń krwionośnych palca, obraz tęczówki lub siatkówki oka, kształt i rysy twarzy, kształt dłoni, ucha lub ust, zapach ciała, cechy charakterystyczne głosu, wzór DNA.

Techniki behawioralne wykorzystuje się do pomiarów zachowania danej osoby. Techniki te obejmują cechy charakterystyczne podpisu odręcznego (kształt liter oraz sposób i dynamika ich tworzenia), dynamikę pisania na klawiaturze, sposób poruszania się (chodu), cechy odzwierciedlające myśli podświadome, takie jak oszustwo, kłamstwo itp. Zwraca się również uwagę na techniki mające podstawy psychologiczne obejmujące pomiar reakcji na konkretne sytuacje lub testy, mające na celu dopasowania do danego profilu psychologicznego. Wymienione techniki mogą mieć zastosowanie między innymi do rozpoznawania w tłumie osób mających określone zamiary, np. kradzież, ale też stany emocjonalne związane z zamiarem popełnienia przestępstwa typu przemyt narkotyków czy też akt terrorystyczny.

Dla jakości i niezawodności przetwarzania danych biometrycznych bardzo istotne są wymagania dotyczące właściwości źródeł danych biometrycznych. Do najważniejszych wymagań zalicza się: uniwersalność, unikalność, stałość, łatwość pobrania, wydajność, akceptowalność oraz łatwość obejścia.

W dokumencie GIODO znajdują się również informacje dotyczące najczęściej stosowanych miar oceny skuteczności systemów biometrycznych. Do miar tych zalicza się wskaźnik fałszywej akceptacji i wskaźnik fałszywego odrzucenia. Wskaźnik błędnych akceptacji (ang. *False Acceptance Rate* – FAR), jest to prawdopodobieństwo tego, że system biometryczny nieprawidłowo zidentyfikuje daną osobę lub nie odrzuci oszusta. Wskaźnik FAR pozwala na pomiar procentu nieważnych próbek dopasowania, które zostały nieprawidłowo zaakcep-

[9] http://www.giodo.gov.pl/pl/319/973 (dostęp: 20.01.2018 r.).

[10] https://www.ksoin.pl/wp-content/uploads/2017/09/Informacja-GIODO-o-zagrożeniach-płynących-z-upowszechnienia-danych-biometrycz.pdf (dostęp: 20.01.2018 r.); norma PN-ISO 19092: 2008; http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679 (dostęp: 20.01.2018 r.).

towane. Wskaźnik FRR (ang. *False Rejection Rate*) – wskaźnik błędnych odrzuceń określany jest jako prawdopodobieństwo, że w systemie dojdzie do błędnego odrzucenia.

Należy zwrócić uwagę na to, iż wartości parametrów FAR i FRR silnie zależne są od rodzaju próbki biometrycznej. Do najczęściej stosowanych technik przetwarzania danych biometrycznych zalicza się: biometrię linii papilarnych, biometrię układu żył krwionośnych palca, biometrię kształtu dłoni, biometrię układu żył krwionośnych dłoni, biometrię tęczówki oka, biometrię siatkówki oka, biometrię rysów twarzy, biometrię głosu.

Pojawiają się również zagrożenia związane z przetwarzaniem danych biometrycznych. Przetwarzanie danych w systemie biometrycznym obejmuje rejestrację, przechowywanie i kojarzenie (identyfikacja lub weryfikacja). Na uwagę zasługuje zagrożenie związane z możliwością użycia danych bez wiedzy osoby, której dane dotyczą, ponieważ wiele danych biometrycznych może być zarejestrowane i wykorzystane przez system biometryczny bez wiedzy osoby, której dotyczą.

Status prawny technologii biometrycznych zawarty jest w aktach prawnych składających się na reformę ochrony danych, które zostały opublikowane w dniu 4 maja 2016 r. w Dzienniku Urzędowym UE L 119[11].

Większość definicji, w tym RODO, definiuje dane biometryczne w kontekście weryfikacji lub identyfikacji osób. Definicje te nie obejmują w związku z tym przetwarzania danych biologicznych, fizycznych, fizjologicznych, czy powtarzalnych czynności osoby, które nie umożliwiają weryfikacji lub identyfikacji osoby, lecz mogą być wykorzystywane w innych celach, jak np. ocena zmęczenia, stresu, stanów emocjonalnych czy stanu zdrowia[12].

Zakończenie

Opracowanie projektu nowych regulacji prawnych o ochronie danych osobowych wynika z konieczności zapewnienia stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE)[13]. Ministerstwo Cyfryzacji odpowiada za podjęcie działań legislacyjnych zapewniających pełne i skuteczne stosowanie ogólnego rozporządzenia w polskim porządku prawnym. Projekt ustawy przewiduje między innymi możliwość wykorzystania biometrii w prawie pracy. Rozporządzenie Parlamentu Europejskiego wprowadza definicję danych biometrycz-

[11] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L:2016:119:TOC (dostęp: 20.01.2018 r.); http://giodo.gov.pl/1520147/id_art/9278/j/pl (dostęp: 20.01.2018 r.).

[12] https://www.ksoin.pl/wp-content/uploads/2017/09/Informacja-GIODO-o-zagrozeniach--plynacych-z-upowszechnienia-danych-biometrycz.pdf (dostęp: 20.01.2018 r.).

[13] http://giodo.gov.pl/1520147/id_art/9278/j/pl (dostęp: 20.01.2018 r.).

nych i zalicza dane biometryczne do szczególnej kategorii danych osobowych, które są danymi osobowymi wrażliwymi. Określa także podstawy prawne dla przetwarzania danych biometrycznych. Z przetwarzaniem danych biometrycznych związany jest także obowiązek przeprowadzenia tzw. oceny skutków dla ochrony danych osobowych (art. 35 RODO). Analiza danych z raportu KPMG wskazuje na wzrastającą liczbę zagrożeń związanych z oszustwami komputerowymi. Dlatego bardzo ważne jest zapewnienie bezpieczeństwa danych, w tym danych biometrycznych oraz usług zaufania.

Bibliografia

Kowalczyk T., *15 trendów bezpieczeństwa w 2018 r.,* „Computerworld" 2018, 01.
Norma PN-ISO 19092: 2008.

Prawodawstwo

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

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.

Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011, nr 225, poz. 1350).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., nr 229, poz. 1536).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2016 r., poz. 922).

Netografia

https://www.gov.pl/cyfryzacja/konsultacje-spoleczne-projektu-przepisow-wdrazajacych-ogolne--rozporzadzenie-o-ochronie-danych-rodo- (dostęp: 20.01.2018 r.).

http://giodo.gov.pl/1520147/id_art/9278/j/pl (dostęp: 20.01.2018 r.).

https://home.kpmg.com/pl/pl/home/about.html (dostęp: 20.01.2018 r.).

http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A31999L0093 (dostęp: 20.01.2018 r.).

https://legislacja.rcl.gov.pl/docs/2/12283556/12343453/12343454/dokument221661.pdf (dostęp: 20.01.2018 r.).
http://www.giodo.gov.pl/pl/319/973 (dostęp: 20.01.2018 r.).
https://www.ksoin.pl/wp-content/uploads/2017/09/Informacja-GIODO-o-zagrożeniach-płynących-z-upowszechnienia-danych-biometrycz.pdf (dostęp: 20.01.2018 r.); norma PN-ISO 19092: 2008; http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679 (dostęp: 20.01.2018 r.).
http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ:L:2016:119:TOC (dostęp: 20.01.2018 r.).
http://giodo.gov.pl/1520147/id_art/9278/j/pl (dostęp: 20.01.2018 r.).
https://www.ksoin.pl/wp-content/uploads/2017/09/Informacja-GIODO-o-zagrożeniach-płynących-z-upowszechnienia-danych-biometrycz.pdf (dostęp: 20.01.2018 r.).
http://giodo.gov.pl/1520147/id_art/9278/j/pl (dostęp: 20.01.2018 r.).