STUDIA PRAWA PUBLICZNEGO
2018 • NR 3 (23) ISSN 2300-3936
DOI: 10.14746/spp.2018.3.23.5

Aleksandra Pyka

Przetwarzanie danych biometrycznych. Aspekty prawne

Wprowadzenie

Wraz z rozwojem nowoczesnych technologii upowszechnieniu ulegają rozwiązania stosowane dotychczas jako unikatowe[1]. Tak też się stało z technikami biometrycznymi, a mianowicie z wykorzystywaniem niepowtarzalnych cech fizycznych, fizjologicznych i behawioralnych człowieka, do których zaliczyć należy linie papilarne, geometrię dłoni, ucha, ust bądź twarzy, tęczówkę oka, dno siatkówki oka, układ naczyń krwionośnych dłoni lub palca, charakterystykę głosu, sposób poruszania się, czy też sposób uderzania w klawiaturę, służące do identyfikacji i weryfikacji tożsamości[2]. Należy przy tym dodać, iż nie można traktować jako synonimów zwrotów „weryfikacja" oraz „identyfikacja", gdyż mają one odmienne znaczenia[3]. Weryfikacja (z wykorzystaniem danych biometrycznych w kontekście niniejszego artykułu) oznacza potwierdzenie deklarowanej tożsamości poprzez przetwarzanie niepowtarzalnych cech fizycznych, fizjologicznych oraz behawioralnych. Z kolei pod pojęciem identyfikacji należy rozumieć ustalenie tożsamości.

Przechodząc do zagadnienia prawnej ochrony danych biometrycznych, należy na wstępie pokrótce przybliżyć pojęcie biometrii (ang. *biometrics*),

[1] Zob. D.D. Zhang, *Biometric Solutions. For Authentication in an E-World*, Boston 2012, s. 1.

[2] Zob. Z. Gomółka, B. Twaróg, E. Żesławska, *Identyfikacja tożsamości z wykorzystaniem analizy geometrii dłoni*, „Edukcja – Technika – Informatyka" 2016, nr 4, s. 419.

[3] Zob. A. Zajkowska, W. Zimnoch, *Technologie biometryczne – istota i możliwości wykorzystania w MSP*, w: *Problemy współczesnej praktyki zarządzania*, t. 2, pod red. S. Lachiewicza, M. Matejuna, Łódź 2007, s. 205.

a także specyfikę technik biometrycznych. Jak wskazuje się w piśmiennictwie, „biometria to wiedza o rozpoznawaniu żywych osób na podstawie cech biologicznych"[4]. Etymologicznie termin „biometria" wywodzi się od greckich słów *bios* (życie) oraz *metron/metrein* (miara/mierzyć)[5].

Z perspektywy ochrony danych osobowych należy nadmienić, że w przypadku technik biometrycznych istotna pozostaje kwestia automatycznego[6] wykorzystywania wyżej wymienionych cech ludzkich, tj. z użyciem urządzeń umożliwiających identyfikację i weryfikację tożsamości[7]. Zostało to także podkreślone w dokumencie roboczym Grupy Roboczej Art. 29 ds. Ochrony Danych przyjętym w dniu 1 sierpnia 2003 r. (tzw. *Working document on biometrics*), tj. „Przetwarzanie danych biometrycznych jest obecnie często wykorzystywane w automatycznych procedurach uwierzytelniania/weryfikacji i identyfikacji". W definicji danych biometrycznych prawodawca unijny podkreślił, że przetwarzanie takich danych odbywa się przy użyciu specjalnych technik („wynika ze specjalnego przetwarzania technicznego"). Dla przykładu można podać sytuację, w której administrator danych przetwarza odwzorowane cyfrowo charakterystyczne punkty linii papilarnych (tzw. minucje). Z perspektywy materialnego zakresu stosowania 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)[8], zwanego dalej „rozporządzeniem ogólnym", nie ma to większego znaczenia, gdyż ten akt prawny dotyczy również procesów przetwarzania prowadzonych w sposób inny niż zautomatyzowany (art. 2 ust. 1 rozporządzenia ogólnego). Niemniej w piśmiennictwie wskazuje się na odmienne ukształtowanie przepisów omawianego aktu w zależności od tego, czy dane przetwarzane są automatycznie czy też

[4] Zob. P. Karlik, *Biometryczna identyfikacja osób w kontekście bezpieczeństwa imprez masowych*, „Ius Novum" 2012, nr 2, s. 97.

[5] *Uniwersalny słownik języka polskiego*, t. 1, pod red. S. Dubisza, Warszawa 2003, s. 267.

[6] W piśmiennictwie nierzadko przytacza się legalną definicję „automatycznego przetwarzania" zawartą w art. 2 lit. c) Konwencji Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzonej w Strasburgu dnia 28 I 1981 r. (Dz.U. 2003 Nr 3, poz. 25). Zob. D. Fleszer, *Zakres przetwarzania danych osobowych w działalności gospodarczej*, Warszawa 2008, s. 15.

[7] Zob. S. Nanavati, M. Thieme, R. Nanavati, *Biometrics. Identity Verification in a Networked World. A Wiley Tech Brief*, New York–Chichester–Weinheim–Brisbane–Singapore–Toronto, s. 9.

[8] Dz.Urz. UE L 119 z 4 V 2016 r., s. 1.

nie[9]. Może mieć to znaczenie w odniesieniu do korzystania z niektórych praw podmiotów danych, jak np. prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu (art. 22 rozporządzenia ogólnego). Konkludując, należy dodać, że przetwarzanie danych biometrycznych, jako proces zautomatyzowany, podlega przepisom rozporządzenia ogólnego, a sam sposób przetwarzania nie determinuje stosowania wyżej wymienionego aktu normatywnego.

W praktyce działalności Generalnego Inspektora Ochrony Danych Osobowych[10] zdarzały się przypadki, że administratorzy danych w celu uniknięcia konieczności wykazania prawidłowego stosowania Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[11] powoływali się na art. 2 ust. 3 wyżej wymienionego aktu prawnego. Administratorzy wskazywali tym samym, że takie zbiory (w których przetwarzano dane biometryczne) sporządzane były doraźnie i wyłącznie z przyczyn technicznych[12]. Takie założenie prowadziłoby do wyłączenia stosowania przepisów u.o.d.o. z wyjątkiem rozdziału 5 (dotyczącego zabezpieczenia danych osobowych). Należy w pełni zanegować taki pogląd, powołując się bowiem na przesłankę doraźności, trzeba brać pod uwagę nie wyłącznie „element czasowy", ale także to, jakiemu celowi służyć miało przetwarzanie danych (np. biometryczna kontrola dostępu). Warto przy tym nadmienić, iż przedstawiciele doktryny wskazywali, „że istotną rolę w zakresie praktycznego rozumienia art. 2 ust. 3 odgrywa czynnik czasu, w ciągu którego są przetwarzane dane osobowe. Poza tym konieczne jest rozważenie celu (zadań), któremu służyć ma przetwarzanie danych w określonej strukturze. O ile pierwszy z tych czynników (czas) nie jest z oczywistych powodów ściśle ustawowo określony (tzn. trudno o wskazanie precyzyjnych czasowych granic zbioru doraźnego), o tyle pojęcie doraźności musi być uzależnione od celu przetwarzania danych w zbiorze. Jeżeli dane tworzące określoną strukturę służą realizacji zasadniczego, głównego celu przetwarzania, trudno uznać tę strukturę za zbiór doraźny. Nie zmienia tego okoliczność, że okres jej przetwarzania

[9] Zob. P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentar*z, Warszawa 2018, s. 140.

[10] Obecnie Prezes Urzędu Ochrony Danych Osobowych, dalej „PUODO".

[11] Dz.U. 2016 r., poz. 922, dalej „u.o.d.o". Ustawa utraciła moc obowiązującą 25 V 2018 r. w związku z rozpoczęciem stosowania rozporządzenia ogólnego i uchyleniem dyrektywy 95/46/WE.

[12] Na ten temat szerzej zob. http://www.giodo.gov.pl/plik/id_p/4099/j/pl/ (dostęp: 16 VIII 2017).

jest relatywnie krótki"[13]. Tym samym przetwarzanie danych biometrycznych w systemach administratora danych – choćby weryfikacja podmiotów danych[14] trwała ułamki sekund – nie mogło spełniać powyższej przesłanki. Trudno wyobrazić sobie zbiór danych biometrycznych sporządzony doraźnie, wyłącznie ze względów technicznych, w którym to po wykorzystaniu danych dochodzić mogłoby do ich usunięcia lub anonimizacji. Tym samym wykluczyć należało możliwość podnoszenia zarzutu braku kompetencji do wszczęcia i prowadzenia postępowań (w tym wydawania decyzji administracyjnych) przez właściwy organ ds. ochrony danych osobowych (z wyłączeniem jednak uprawnienia do monitorowania obowiązku zabezpieczenia danych). Rozporządzenie ogólne o ochronie danych nie przewiduje wyłączenia swojego stosowania w odniesieniu do zbiorów danych sporządzanych doraźnie. Wnioskiem z powyższych rozważań jest stwierdzenie, że przetwarzanie danych biometrycznych nie jest „czynnością" doraźną, niemniej w nowym stanie prawnym – po rozpoczęciu stosowania rozporządzenia ogólnego – nie jest to szczególnie istotne.

Celem niniejszego artykułu jest przedstawienie problematyki przetwarzania danych biometrycznych w polskim porządku prawnym, w szczególności z uwzględnieniem dotychczasowego orzecznictwa sądów administracyjnych oraz ze wskazaniem obowiązujących przepisów prawa, a także zmian w tym zakresie, które nastąpiły po 25 maja 2018 r. W założeniu poczynionym przez autorkę artykuł przedstawia tematykę korzystania z rozwiązań biometrycznych z perspektywy regulacji normatywnych dotyczących ochrony danych osobowych, niemniej wskazano w nim również zagrożenia wynikające z przetwarzania danych biometrycznych.

1. Pojęcie danych biometrycznych

Ustawa o ochronie danych osobowych nie odnosiła się w żadnym z przepisów do pojęcia danych biometrycznych, niemniej nie stanowiło to w żadnym wypadku o wyłączeniu stosowania powyższego aktu do procesów przetwarzania takich danych. W dotychczas obowiązującym

[13] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. 4, Kraków 2007, s. 319.

[14] W niniejszym artykule przyjęto użycie zamiennie określeń „osoba, której dane dotyczą" oraz „podmiot danych" ze względu na dosłowne tłumaczenie pierwszego pojęcia wprost z rozporządzenia ogólnego, tj. *the data subject*.

akcie prawnym brak było ogólnej, legalnej definicji danych biometrycznych[15]. W polskim porządku prawnym funkcjonuje pojęcie danych biometrycznych i zostało ono zdefiniowane, niemniej odnosi się wyłącznie do danych biometrycznych w paszportach (zawężono zakres stosowania). Zgodnie z art. 2 pkt 1 Ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych[16] pod pojęciem danych biometrycznych – na potrzeby tego aktu – należy rozumieć „wizerunek twarzy i odciski palców umieszczone w dokumentach paszportowych w formie elektronicznej"[17]. W piśmiennictwie słusznie wskazuje się jednak, że jest to relatywnie wąski zakres znaczeniowy tego pojęcia[18]. Na marginesie warto dodać, że podjęto próbę zdefiniowania danych biometrycznych w opinii 4/2007 Grupy Roboczej Art. 29 ds. Ochrony Danych z 20 czerwca 2007 r. w sprawie pojęcia danych osobowych, która nie ma jednak charakteru wiążącego. I tak zgodnie z wyżej wymienioną opinią „dane te [biometryczne – dop. A.P.] można zdefiniować jako właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą wyłącznie danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopień prawdopodobieństwa".

Dopiero reforma prawa ochrony danych osobowych na szczeblu Unii Europejskiej skutkowała wprowadzeniem do rozporządzenia ogólnego definicji danych biometrycznych, która nie znajdzie ograniczenia w zastosowaniu. W myśl art. 4 pkt 14 tego aktu „dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną

[15] Podkreślić jednak należy, że funkcjonują różnorakie definicje „danych biometrycznych", którym nie można przypisać cech definicji legalnych. W formie egzemplifikacji wskazać można normę PN-ISO 19092:2010, zgodnie z którą pod pojęciem danych biometrycznych rozumieć należy „informacje wyodrębnione z próbki biometrycznej i stosowane do utworzenia wzorca odniesienia albo wzorca dopasowywanego" (*Informacja Generalnego Inspektora Ochrony Danych Osobowych o zagrożeniach płynących z upowszechnienia danych biometrycznych w kontaktach obywateli z instytucjami publicznymi i prywatnymi*, Warszawa 2017).

[16] Tekst jedn. Dz.U. 2016, poz. 758.

[17] W ustawie o dokumentach paszportowych (art. 18 ust. 1 pkt 11) ustawodawca wyodrębnił katalog danych, które są zamieszczane w dokumentach paszportowych, w tym właśnie dane biometryczne, przy czym takich danych nie zamieszcza się w paszportach tymczasowych.

[18] Szerzej zob. A. Bodnar, J. Michalski, *Dokument biometryczny a prawa człowieka*, w: *Dokumenty we współczesnym prawie*, pod red. E. Gruzy, Warszawa 2009, s. 51–61.

identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne". Prawodawca unijny zaliczył ponadto dane biometryczne w poczet „szczególnych kategorii danych osobowych" (art. 9 ust. 1 rozporządzenia ogólnego), bez względu na to, czy w wyniku ich przetwarzania „generowane" są dodatkowe informacje, jak chociażby ujawniające stan zdrowia (np. w wyniku skanowania tęczówki oka/dna siatkówki oka). Jak wskazywali przedstawiciele doktryny, „dane biometryczne zaliczone zostały do odpowiednika obecnie istniejącej na gruncie OchrDanychU kategorii danych wrażliwych"[19]. W przeciwieństwie do rozporządzenia ogólnego na gruncie u.o.d.o. dane biometryczne nie należały do zamkniętego katalogu danych szczególnie chronionych, o których stanowił art. 27 ust. 1 tego aktu. Warto dodać, że nierzadko dane biometryczne ujawniają dodatkowe dane, m.in. stan zdrowia czy pochodzenie etniczne lub rasowe. Dane biometryczne na gruncie rozporządzenia ogólnego należą bezwzględnie do szczególnych kategorii danych osobowych. Poprzednio obowiązująca u.o.d.o. nie wyodrębniała literalnie danych biometrycznych. Podsumowując powyższe rozważania, należy dodać, że zakwalifikowanie danych biometrycznych do szczególnych kategorii nie pozostaje bez znaczenia, m.in. w odniesieniu do podstaw dopuszczalności przetwarzania danych, czego autorka zamierza dowieść poniżej.

Dane biometryczne należą w pełni do informacji umożliwiających identyfikację osoby lub potwierdzających jednoznaczną identyfikację, a do tego są to dane tym cenniejsze, że niepowtarzalne. Specyfika przetwarzania tych danych wynika ze zwiększonego stopnia ingerencji w niezależność informacyjną jednostki, a w tym przypadku dotyczy to samej struktury fizycznej lub fizjologicznej, a także cech behawioralnych człowieka. Nierzadko w literaturze podkreśla się, iż „dane [tu dane biometryczne – dop. A.P.] nie mogą istnieć samoistnie. Ich występowanie zawsze wiąże się z pewnym nośnikiem, którego różnorodność jest bardzo szeroka […], ślady krwi, śliny, obraz wnętrza oka, odcisk palca itd.)"[20]. Warto zwrócić uwagę, że nie każde stosowanie technik biometrycznych przy użyciu określonych nośników (np. EKG, badanie tętna i ciśnienia krwi bądź pomiar temperatury ciała) pozwolą zidentyfikować lub zweryfikować konkretną osobę, a tym samym nie zawsze informacje takie można zaliczyć do danych biometrycznych.

[19] Zob. P. Litwiński, *Pojęcie danych osobowych w rozporządzeniu ogólnym o ochronie danych osobowych*, „Informacja w Administracji Publicznej" 2016, nr 3, s. 7.

[20] Zob. M. Bąba, *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, „Prawo Mediów Elektronicznych" 2016, nr 2, s. 26.

2. Niektóre prawne podstawy dopuszczalności przetwarzania danych biometrycznych

Pod pojęciem przetwarzania danych rozumieć należy „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie" (art. 4 pkt 2 rozporządzenia ogólnego). O legalności przetwarzania (w tak szeroko ujętym znaczeniu, jak wskazano w wyżej wymienionym przepisie) mówić można w sytuacji, gdy administrator będzie w stanie wykazać, że legitymuje się jedną z prawnych podstaw dopuszczalności przetwarzania danych. Zastosowanie konkretnych przesłanek będzie jednak uzależnione od kategorii przetwarzanych danych. W rozporządzeniu ogólnym wyodrębnia się „szczególnej kategorii dane osobowe", „dane osobowe dotyczące wyroków skazujących i naruszeń prawa" oraz dane nienależące do powyższych, które określić można mianem „danych zwykłych". Zasygnalizować należy, że prawodawca pozostawił państwom członkowskim swobodę w zakresie wprowadzenia „dalszych warunków", w tym ograniczeń przetwarzania danych biometrycznych (art. 9 ust. 4 rozporządzenia ogólnego). Zagadnienie to wymaga szerszego omówienia.

Problematyczna może stać się kwestia zaklasyfikowania danych osobowych do danych biometrycznych, co będzie miało wpływ na stosowanie konkretnych podstaw dopuszczalności przetwarzania. Identyfikowanie podmiotu danych dokonywane za pomocą skanu twarzy z danymi uprzednio wgranymi do bazy skanera (m.in. imię i nazwisko, zdjęcie twarzy w formacie jpg) nie wiąże się automatycznie z przetwarzaniem danych ujawniających pochodzenie rasowe lub etniczne, tj. szczególnych kategorii danych osobowych. Na gruncie rozporządzenia nie ma to większego znaczenia, gdyż dane biometryczne bezwzględnie należą do szczególnych kategorii danych osobowych i mogą być przetwarzane wyłącznie w oparciu o jedną z podstaw z art. 9 ust. 2 rozporządzenia ogólnego (na zasadzie odstępstwa od generalnego zakazu przetwarzania[21]). Odmiennie zaś w u.o.d.o. – należało badać,

[21] Szerzej zob. P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham 2017, p. 110.

czy dana operacja wiąże się dodatkowo z przetwarzaniem danych sensytywnych (np. system identyfikujący na podstawie wizerunku twarzy, umożliwiający kategoryzowanie osób ze względu na kolor skóry). Kwestię tę porusza także motyw 51 preambuły rozporządzenia ogólnego, który stanowi, że „przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją «danych biometrycznych» tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości". Podobnie w opinii 3/2012 Grupy Roboczej Art. 29 z dnia 27 kwietnia 2012 r. w sprawie zmian sytuacji w dziedzinie technologii biometrycznych wskazano, że przetwarzanie danych biometrycznych nie oznacza tym samym przetwarzania danych szczególnie chronionych. Nierzadko stosowanie określonych technik biometrycznych (np. skanerów twarzy) nie daje możliwości uzyskania informacji pozwalających na klasyfikację podmiotu danych ze względu m.in. na płeć, wzrost, kolor skóry. Jak wskazano w opinii 02/2012 Grupy Roboczej Art. 29 ds. Ochrony Danych przyjętej w dniu 22 marca 2012 r. w sprawie systemów rozpoznawania twarzy w usługach *online* i usługach komórkowych, „kiedy obraz cyfrowy zawiera twarz danej osoby, która jest w pełni widoczna, i umożliwia identyfikację tej osoby, obraz ten traktuje się jako dane osobowe". Powyższe stanowi, że przetwarzanie w zbiorach danych zdjęć m.in. w formacie jpg, na których to znajdują się charakterystyczne cechy fizyczne umożliwiające identyfikację osoby (np. nawet część twarzy), będzie odnosiło się do przetwarzania danych osobowych. Nie przesądza to o przetwarzaniu w tych procesach danych biometrycznych. W nawiązaniu do wyżej wymienionej opinii warto wspomnieć, że „obrazy cyfrowe przedstawiające ludzi mogą w niektórych przypadkach być uznane za szczególną kategorię danych osobowych. Szczególnie gdy wzory lub obrazy cyfrowe [wykorzystywane w systemach rozpoznawania twarzy – biorąc pod uwagę zagadnienie omawiane w artykule – wykorzystują dane biometryczne – dop. A.P.] przedstawiające ludzi są dodatkowo przetwarzane w celu pozyskania szczególnych kategorii danych, byłyby one z pewnością zaliczone do tej kategorii. Przykładem takiego zastosowania może być chęć otrzymania informacji na temat pochodzenia etnicznego, wyznania lub kondycji zdrowotnej danych osób".

Jak już wskazano, przetwarzanie danych biometrycznych wiązać się będzie z koniecznością wykazania przez administratora, że legitymuje

się on jedną z prawnych podstaw przetwarzania danych wskazanych w art. 9 ust. 2 rozporządzenia ogólnego[22]. Nie każda z tych przesłanek będzie miała jednak zastosowanie. Klasycznym tego przykładem jest przetwarzanie danych biometrycznych pracowników w celu ewidencjonowania czasu pracy. W tym przypadku w wątpliwość należy podać kwestię dobrowolności wyrażenia zgody przez pracownika w związku z przetwarzaniem jego danych biometrycznych[23]. Warto się przy tym odnieść do tezy wyroku Naczelnego Sądu Administracyjnego (NSA) z 1 grudnia 2009 r., który stanowi, że „brak równowagi w relacji pracodawca – pracownik stawia pod znakiem zapytania dobrowolność wyrażenia zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22 Kodeksu Pracy katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody na podstawie art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22 Kodeksu Pracy, stanowiłoby obejście tego przepisu"[24]. Takie stanowisko (odnośnie do pozyskiwania zgody od pracowników na przetwarzanie danych osobowych nie tylko w związku z przetwarzaniem danych biometrycznych) jest ugruntowane w orzecznictwie[25]. Sytuacja ta jednak zmienia się diametralnie w przypadku wdrożenia biometrycznej kontroli dostępu na określonych obszarach bądź w pomieszczeniach (np. teren inwestycji), kiedy to administratorem jest np. inwestor, a pozyskiwane są dane biometryczne pracowników wykonawcy. Nie kwestionuje się w tym przypadku przetwarzania danych pracowników wykonawcy, o ile takie dane są przetwarzane wyłącznie przez inwestora w celu kontrolowania dostępu na określony teren, a także gdy zapewnia się stosowanie alternatywnych metod weryfikacji tożsamości. W każdym przypadku administrator danych powinien zagwarantować podmiotom danych możliwość korzystania z „wariantowych" metod (np. w przypadku biometrycznej kontroli dostępu),

[22] Na gruncie uchylonej u.o.d.o. art. 23 ust. 1 lub art. 27 ust. 2. Szerzej zob. E. Bielak-Jomaa, *Wdrażanie rozwiązań biometrycznych a ochrona danych osobowych*, „IT w Administracji" 2016, nr 6.

[23] Zob. M. Korga, *Dane biometryczne i ich wykorzystywanie na gruncie stosunku pracy*, „Monitor Prawa Pracy" 2011, nr 12, s. 622.

[24] Szerzej zob. wyrok NSA z 1 XII 2009 r., sygn. I OSK 249/09, LEX nr 785755.

[25] Szerzej zob.: wyrok NSA z 6 IX 2011 r., sygn. I OSK 1476/10, LEX nr 965912; wyrok Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie z 18 VI 2010 r., sygn. II SA/Wa 151/10, LEX nr 643811.

takich jak karty magnetyczne. Tym bardziej zaskakująca w świetle niekwestionowanej linii orzeczniczej (powołanej powyżej) wydaje się próba wprowadzenia zmian w Kodeksie pracy[26] wynikająca z konieczności dostosowania przepisów krajowych do rozporządzenia ogólnego. Ministerstwo Cyfryzacji przedstawiło projekt z dnia 12 września 2017 r. ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych, w którym dopuszczono możliwość przetwarzania danych biometrycznych pracowników[27]. Powyższy projekt wprowadzał art. 22^2 § 2 do Kodeksu pracy w brzmieniu: „przetwarzanie przez pracodawcę danych biometrycznych obejmuje tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy i pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej" (art. 5 pkt 2 Przepisów wprowadzających ustawę o ochronie danych osobowych). Stwierdzić należy, że przepis ten był niezgodny z dotychczasową linią orzeczniczą sądów administracyjnych[28]. Wprowadzenie zmian w Kodeksie pracy jest zabiegiem podważającym pogląd, iż relacja pracodawca – pracownik jest nierównoważna, a zgoda ta nie jest wyrażona swobodnie[29]. Uregulowanie zgody, jako przesłanki egzoneracyjnej (tj. wyłączającej bezprawność przetwarzania danych biometrycznych) w nierównorzędnych relacjach wynikających ze stosunku pracy (podobnie jak i umów cywilnoprawnych), stanowi przejaw marginalizacji dotychczasowego dorobku orzeczniczego i nie zasługuje na aprobatę. Bez znaczenia jest forma wyrażenia zgody (papierowa lub elektroniczna), którą miałoby przybrać to oświadczenie woli. Powyższe rozważania pozwalają więc wysnuć wniosek, że administrator, przetwarzając dane biometryczne, powinien legitymować się stosowną przesłanką. W odniesieniu do pracowników należy jednak wyłączyć sposobność powoływania się na zgodę podwładnego, gdyż można podać w wątpliwość jej dobrowolność.

Nawiązując jeszcze do przesłanek legalizujących przetwarzanie danych biometrycznych, należy odnieść się do wyroku Wojewódzkiego

[26] Ustawa z dnia 26 VI 1974 r. Kodeks pracy (tekst jedn. Dz.U. 2018, poz. 917).

[27] Szerzej zob. M. Krzysztofek, *Zgoda pracownika jako podstawa przetwarzania danych biometrycznych w RODO i w projekcie Przepisów wprowadzających ustawę o ochronie danych osobowych*, IAP 2017, nr 4.

[28] Wyrok NSA z 6 IX 2011 r., sygn. I OSK 1476/10, LEX nr 965912; wyrok WSA w Warszawie z 18 VI 2010 r., sygn. II SA/Wa 151/10, LEX nr 643811; wyrok WSA w Warszawie z 27 XI 2008 r., sygn. II SA/Wa 903/08, LEX nr 521934.

[29] Szerzej zob. K. Malik, *Problematyka przetwarzania danych biometrycznych pracowników*, „Monitor Prawa Pracy" 2008, nr 12.

Sądu Administracyjnego w Warszawie z 16 grudnia 2015 r.[30], w którym to wskazano m.in. na konieczność legitymowania się przez administratora danych (tu spółkę z o.o.) jedną z podstaw do przetwarzania danych z art. 23 ust. 1 u.o.d.o. W tym przypadku spółka z o.o. przetwarzała dane biometryczne (odciski linii papilarnych) klientów klubu fitness bez podstawy prawnej. W powyższym judykacie podniesiono, że administrator danych nie pozyskiwał od klientów zgód na przetwarzanie danych biometrycznych, a także z treści umów zawieranych z podmiotami danych nie wynikało uprawnienie do gromadzenia i przechowywania wyżej wymienionych danych. Odnośnie do zgody należałoby (podobnie jak w powyższym orzeczeniu) wskazać, że „pierwszym wymogiem dla zgody, wynikającym ze sformułowania zakazu domniemywania zgody bądź jej dorozumienia, jest konieczność jasnego, wyraźnego, nienasuwającego wątpliwości pozytywnego oświadczenia woli przy tak samo wyraźnym jednoznacznym określeniu przedmiotu, którego zgoda dotyczy". W myśl art. 4 pkt 11 rozporządzenia ogólnego pod pojęciem zgody osoby, której dane dotyczą, należy rozumieć „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych". Żadna czynność konkludentna nie może stanowić podstawy do przypuszczania, że podmiot danych wyraził zgodę na przetwarzanie. W polskim porządku prawnym można odwołać się np. do normy art. 174 pkt 1 Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[31] wprowadzającej zakaz domniemywania/dorozumiewania zgody abonenta lub użytkownika końcowego z oświadczenia woli o innej treści. Należy podkreślić, że „dla wyrażenia zgody w rozumieniu art. 174 [p.t. – dop. A.P.] nie znajduje zastosowania przepis art. 60 k.c. wskazujący, że oświadczenie woli może być wyrażone przez każde zachowanie ujawniające wolę w sposób dostateczny"[32]. Stanowisko to jest aktualne i znajduje zastosowanie do zgody z art. 9 ust. 2 lit. a rozporządzenia ogólnego. Nie ma tym samym miejsca na doszukiwanie się takowej przesłanki w przypadku czynności konkludentnych (np. poprzez samo korzystanie z urządzeń przetwarzających dane biometryczne, takich jak skaner linii papilarnych czy opaska biometryczna). Ze względu na to, że

[30] Wyrok WSA w Warszawie z 16 XII 2015 r., sygn. II SA/Wa 658/15, LEX nr 1823555.

[31] Tekst jedn. Dz.U. 2017, poz. 1907, dalej „p.t.".

[32] Szerzej zob. K. Kawałek, M. Rogalski, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, s. 894.

dane biometryczne zostają zaliczone w poczet szczególnych kategorii danych osobowych, również rozporządzenie ogólne „uchyla" generalny zakaz przetwarzania tych danych w sytuacji, gdy „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". Możliwość wprowadzenia do prawodawstwa unijnego lub krajowego norm wykluczających uchylenie zakazu przetwarzania wydaje się rozwiązaniem korzystnym ze względu na nierzadką nierównorzędność relacji administrator – podmiot danych (m.in. w stosunkach pracy). Rozważania te prowadzą do wniosku, że literalne brzmienie rozporządzenia ogólnego uniemożliwia domniemywanie zgody na przetwarzanie danych (w tym biometrycznych) z innych oświadczeń bądź zachowań podmiotu danych.

W świetle rozporządzenia ogólnego jedną z podstaw dopuszczalności przetwarzania danych może być art. 9 ust. 2 lit. g. Generalny zakaz przetwarzania danych biometrycznych jest uchylony, jeśli w myśl powyższej normy prawnej „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, których dane dotyczą". Niekiedy mamy do czynienia z sytuacją, w której ustawodawca wprowadza do porządku krajowego tj. do poszczególnych aktów prawnych, wyliczenie enumeratywne dotyczące zakresu danych oraz wskazuje podmiot, któremu przysługuje status administratora. Przykładowo, podstawą do przetwarzania danych biometrycznych przez organy właściwe do wydawania paszportów w świetle Ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych[33] jest art. 18 ust. 1 pkt 11 tego aktu. Przepis ten uprawnia wyżej wymienione organy m.in. do pozyskiwania danych biometrycznych osób wnioskujących o paszport (określany mianem „paszportu biometrycznego"). Ponadto nawiązuje w swej treści do motywu 2 preambuły rozporządzenia 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[34]. Jak stanowi ten motyw, „paszport lub dokument podróży powinien

[33] Tekst jedn. Dz.U. 2016, poz. 758.

[34] Dz.Urz. UE L 385 z 29 XII 2004 r., s. 1.

zawierać identyfikatory biometryczne w celu zapewnienia niebudzącego wątpliwości związku pomiędzy dokumentem a jego prawowitym posiadaczem". Stosowanie rozwiązań biometrycznych w dokumentach paszportowych czy innych dokumentach podróży spełnia także funkcję „prewencyjną", tj. ma zapobiegać ewentualnym fałszerstwom wyżej wymienionych dokumentów lub kradzieżom tożsamości (np. chronić przed ich bezprawnym użyciem)[35].

Warto nadmienić, że art. 1 ust. 2 rozporządzenia Rady (WE) Nr 2252/2004 określa minimalny zakres danych biometrycznych przetwarzanych w paszportach lub innych dokumentach podróży, tj. obraz (wizerunek) twarzy. Niemniej nie wyklucza to możliwości przetwarzania innych danych, jak odciski palców, przy czym pozostawia się taką decyzję do podjęcia państwom członkowskim (tzw. klauzula *option and choices*). Na etapie prac legislacyjnych Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (WSiSW) wprowadziła do projektu wyżej wymienionego rozporządzenia pewne modyfikacje odnoszące się m.in. do obligatoryjnego wykorzystywania w paszportach zarówno wizerunku twarzy, jak i odcisków palców (tzw. biometria multimodalna[36]). Propozycja ta została odrzucona przez Parlament Europejski. W przypadku stosowania technik biometrycznych ważne jest, aby zagwarantować podmiotom danych możliwość korzystania z alternatywnych rozwiązań umożliwiających identyfikację ich tożsamości. W tej części artykułu wskazano jedynie wybiórczo najważniejsze podstawy dopuszczalności przetwarzania danych. Niewykluczone, że w perspektywie czasu upowszechnienie stosowania rozwiązań biometrycznych przyczyni się do rozszerzenia korzystania z pozostałych przesłanek.

3. Prawa osób, których dotyczą dane biometryczne

Administrator jest w świetle rozporządzenia ogólnego (podobnie jak w dotychczas obowiązującej u.o.d.o.) zobowiązany do spełnienia obowiązku informacyjnego wobec osób, których dane dotyczą (art. 13 i 14 rozporządzenia ogólnego). Dane biometryczne są pozyskiwane

[35] Patrz szerzej: K. Czaplicki, *Dokumenty tożsamości. Jawność i bezpieczeństwo*, Warszawa 2016.

[36] Szerzej zob. M.L. Gavrilova, M. Monwar, *Multimodal Biometrics and Intelligent Image Processing for Security Systems*, IGI 2013. Biometria multimodalna oznacza wykorzystanie więcej niż jednej techniki biometrycznej. Zob. P.S.P. Wang, *Pattern Recognition, Machine Intelligence and Biometrics*, Beijing–Berlin–Heidelberg 2012, s. 656.

przez administratora w wyniku bezpośredniego kontaktu z podmiotem danych (np. poprzez utworzenie cyfrowego odwzorowania charakterystycznych punktów linii papilarnych), a więc w takim przypadku znajdzie zastosowanie jedynie art. 13 rozporządzenia ogólnego („informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą"). Nie można wykluczyć, że dane biometryczne będą zbierane w sposób inny niż od osoby, której dane dotyczą, niemniej wówczas administrator będzie zobowiązany do wskazania źródła pochodzenia danych osobowych (art. 14 ust. 2 lit. f rozporządzenia ogólnego).

W art. 15 rozporządzenia ogólnego prawodawca uregulował prawo dostępu przysługujące osobie, której dane dotyczą. Przepis ten wskazuje, że „administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu" (art. 15 ust. 3). Nie zastrzeżono przy tym formy, w jakiej administrator ma przekazać wyżej wymienioną kopię danych. Wyjątkiem jest jedynie sytuacja, w której podmiot danych zwraca się do administratora drogą elektroniczną o przekazanie takiej kopii bez zastrzegania szczególnej formy. Tym samym osoba, której dane dotyczą, może wystosować wniosek do administratora o przekazanie na określonym nośniku kopii danych biometrycznych (m.in. cyfrowego odwzorowania zeskanowanej siatkówki oka) w dowolnej formie (np. powszechnie stosowaną drogą elektroniczną).

Kwestią nieco problematyczną z perspektywy uprawnień podmiotów danych może wydawać się realizacja prawa do sprostowania danych (art. 16 rozporządzenia ogólnego). Osoba, której dane dotyczą, co do zasady ma prawo do ich „poprawiania", niemniej należy zwrócić uwagę, że dane biometryczne są oparte na zasadniczo niezmiennych cechach fizycznych, fizjologicznych lub behawioralnych człowieka. Z literalnego brzmienia wyżej wymienionego przepisu nie wynika jednak, aby prawo do sprostowania danych dotyczyło osób, którym błędnie „przypisano" cudze dane biometryczne. Rozporządzenie wyraźnie stanowi, iż przepis ten znajduje zastosowanie do osób, których dane dotyczą, tj. do ich danych biometrycznych. Prawodawca odniósł się w tym przepisie jedynie do możliwości sprostowania własnych, nieprawidłowych danych.

Przetwarzanie danych biometrycznych wiąże się także z koniecznością ich usunięcia (z realizacją „prawa do bycia zapomnianym"). Rozporządzenie stanowi, że z powyżej wskazanym uprawnieniem podmiotu danych koreluje obowiązek spoczywający po stronie administratora do usunięcia takich danych w przypadku zaistnienia jednej z przesłanek zawartych w art. 17 ust. 1 lit. a–f. Podmiotom danych przysługuje

również prawo do ograniczenia przetwarzania danych (art. 18 rozporządzenia ogólnego). Oznacza to, iż w enumeratywnie wskazanych przypadkach osoby, których dane dotyczą, mogą żądać ograniczenia przetwarzania danych biometrycznych. Niekiedy jako przykład wskazuje się przetwarzanie wyżej wymienionych danych pracowników do ewidencjonowania czasu pracy na podstawie klauzuli prawnie usprawiedliwionego celu[37]. Rozporządzenie ogólne także wprowadziło (choć zmodyfikowaną) przesłankę prawnie uzasadnionego interesu realizowanego przez administratora lub przez stronę trzecią. Osoba, której dane dotyczą, mogłaby zatem skorzystać w tym przypadku z prawa do sprzeciwu (art. 21 rozporządzenia ogólnego), a administrator zostałby zobowiązany wówczas do ograniczenia przetwarzania danych biometrycznych do czasu stwierdzenia, czy prawnie uzasadnione podstawy po jego stronie są nadrzędne wobec podstaw sprzeciwu podmiotu danych. Niemniej art. 6 ust. 1 lit. f rozporządzenia ogólnego nie znajdzie w tym przypadku zastosowania, gdyż nie jest podstawą do wyłączenia zakazu przetwarzania danych biometrycznych (jest to zasadnicza różnica pomiędzy podstawami dopuszczalności przetwarzania danych na gruncie u.o.d.o. i rozporządzenia ogólnego). W polskim porządku prawnym na próżno doszukiwać się w judykaturze orzeczeń dotyczących przetwarzania danych biometrycznych na podstawie klauzuli prawnie usprawiedliwionego celu administratora danych obowiązującej w uchylonej już u.o.d.o.

W przypadkach przetwarzania danych biometrycznych w sposób zautomatyzowany opartych na zgodzie z art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a lub z art. 6 ust. 1 lit. b rozporządzenia ogólnego podmiot danych ma prawo do przenoszenia danych w myśl art. 20 tego aktu. Korzystając z tego prawa, osoba, której dane dotyczą, może żądać – przy uwzględnieniu możliwości technicznych – przesłania danych biometrycznych innemu administratorowi (tu znajduje zastosowane jedynie art. 9 ust. 2 lit. a rozporządzenia ogólnego. Podmiot danych może także sam przesłać dane, które uprzednio otrzymał w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Przesyłając dane, dotychczasowy administrator nie jest zobowiązany do badania legalności pozyskiwania danych przez innego administratora, tj. faktu, czy legitymuje się on podstawą prawną przetwarzania danych biometrycznych z wyżej wymienionych artykułów rozporządzenia ogólnego.

[37] Szerzej zob. D. Nowak, *Czy biometria jest bezpieczna*, „IT w Administracji" 2016, nr 8.

Wyżej poczynione rozważania prowadzą do stwierdzenia, że przetwarzanie danych biometrycznych wiąże się z koniecznością realizacji praw podmiotów danych. Nie z każdego uprawnienia osoba, której dane dotyczą, może skorzystać. Zwiększenie zakresu uprawnień wynika m.in. z tego, że dane biometryczne są przetwarzane w sposób zautomatyzowany.

4. Zagrożenia wynikające z przetwarzania danych biometrycznych

Z przetwarzaniem danych biometrycznych, tak jak z przetwarzaniem wszelkich innych danych osobowych, wiąże się „ingerencja w autonomię informacyjną jednostki"[38]. Pociąga to za sobą pewne zagrożenia z perspektywy prawa do ochrony danych osobowych, choć nadmienić należy, że w przypadku danych biometrycznych może mieć to wymierne skutki ze względu na niepowtarzalność źródła tych danych.

Potencjalne zagrożenia dla ochrony prywatności dostrzegła już Grupa Robocza Art. 29 ds. Ochrony Danych, do czego nawiązała w swej opinii 3/2012 przyjętej w dniu 27 kwietnia 2012 r. w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (00720/12/PL WP193). Warto przy tym nadmienić, że organ ten odniósł się także w opinii 2/2012 z 22 marca 2012 r. w sprawie systemów rozpoznawania twarzy w usługach *online* i usługach komórkowych (00727/12 PL WP 192) do kwestii zastosowania takich technik, m.in. w SNS (ang. *Social Networking Sites*). W obydwu opiniach dostrzeżono pewne zagrożenia dla ochrony prywatności w związku z wykorzystaniem biometrii twarzy jako środka identyfikacji i kategoryzacji osób, a także uwierzytelniania/weryfikacji ich tożsamości. Dane osobowe nierzadko mogą na przestrzeni czasu ulec zmianie. W celu egzemplifikacji należy wskazać choćby imię i nazwisko, których zmiana może nastąpić na podstawie przepisów Ustawy z dnia 17 października 2008 r. o zmianie imienia i nazwiska[39], lub też numer PESEL (art. 19 ust. 1 Ustawy z dnia 24 września 2010 r. o ewidencji ludności[40]). Dane biometryczne, jako dane osobowe, także mogą podlegać pewnym zmianom, aczkolwiek źródło ich pozyskiwania pozostaje zasadniczo niezmienne. W tym upatrywać należy zagrożeń

[38] Pismo Rzecznika Praw Obywatelskich z 6 VII 2015 r., https://www.rpo.gov.pl/sites/default/files/Do_MF_ws._identyfikacji_glosowej_podatnikow_dzwoniacych_na_Krajowa_Informacje_Podatkowa.pdf (dostęp: 23 VII 2017).

[39] Tekst jedn. Dz.U. 2016, poz. 10.

[40] Tekst jedn. Dz.U. 2017, poz. 657.

dla prywatności osób fizycznych, których dane biometryczne są przetwarzane. Powyższa opinia 3/2012 Grupy Roboczej Art. 29 wskazuje m.in. na dyskryminację genetyczną oraz kradzież tożsamości. Z zaniepokojeniem należy również patrzeć na próby tworzenia (bez podstawy prawnej) baz danych biometrycznych, które posłużyć mogłyby do weryfikacji tożsamości jednostki w kontaktach z organami administracji publicznej[41]. Wiązać się z tym może zagrożenie naruszenia konstytucyjnych praw i wolności jednostki.

5. Przetwarzanie danych biometrycznych a niektóre zasady dotyczące przetwarzania danych osobowych

Przetwarzanie danych biometrycznych wiąże się koniecznością przestrzegania generalnych zasad ochrony danych osobowych wyodrębnionych w art. 5 ust. 1 i 2 rozporządzenia ogólnego[42]. Spośród nich należy wyróżnić zasadę minimalizacji danych (ang. *data minimisation principle*) oraz zasadę ograniczenia przechowywania (ang. *storage limitation principle*).

Zgodnie z art. 5 ust. 1 lit. e rozporządzenia ogólnego „dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą («ograniczenie przechowywania»)". Z kolei zgodnie z zasadą minimalizacji danych

[41] Przykładowo należy wskazać propozycję Ministerstwa Finansów dotyczącą pozyskiwania danych biometrycznych (ściśle, poprzez rozpoznawanie głosu) podatników kontaktujących się z organem w ramach Krajowej Informacji Podatkowej bez podstawy prawnej. W niniejszej sprawie ingerował zarówno Rzecznik Praw Obywatelskich, jak i Generalny Inspektor Ochrony Danych Osobowych (GIODO). Jak wynika ze sprawozdania rocznego GIODO za rok 2015, „planowane rozwiązania polegające na nagrywaniu rozmów telefonicznych i analizie biometrycznej głosu, oprócz braku odpowiedniej podstawy prawnej, nie spełniały w opinii Generalnego Inspektora kryterium niezbędności" (www.giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2015.pdf, dostęp: 3 XI 2017).

[42] Szerzej zob. S. Gutwirth, R. Leenes, P. de Hert, *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Springer 2016.

„dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane" (art. 5 ust. 1 lit. c rozporządzenia ogólnego). W wyroku z 4 grudnia 2008 r.[43] (sprawa *S. and Marper przeciwko Zjednoczonemu Królestwu*) Europejski Trybunał Praw Człowieka (ETPC) orzekł, że bezterminowe przechowywanie (a tym samym, co należy dopowiedzieć, przetwarzanie) danych dotyczących m.in. DNA czy odcisków linii papilarnych osób, w stosunku do których zakończono postępowanie karne bez skazania, stanowi naruszenie prawa do prywatności w myśl art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[44]. ETPC odniósł się w omawianym wyroku zarówno do zasady ograniczenia przechowywania, jak i zasady proporcjonalności. Trybunał orzekł, że przechowywanie odcisków linii papilarnych osób, które ostatecznie nie zostały skazane za popełnienie zarzucanych im czynów zabronionych, bez ograniczenia czasowego stanowi naruszenie art. 8 Konwencji. Omawiany judykat zmienił dotychczasową linię orzeczniczą, gdyż wcześniej ETPC wyraźnie wskazywał, że pobranie i przechowywanie odcisków palców nie stanowi ingerencji w konwencyjne prawo do prywatności (sprawa *Van der Velden v. Niderlandy*, sprawa *Kinnunen v. Finlandia*)[45].

Zasada legalizmu wynika wprost z art. 5 ust. 1 lit. a rozporządzenia ogólnego, który stanowi, że „dane osobowe muszą być przetwarzane zgodnie z prawem […]". Odnosi się to zarówno do zgodności z przepisami rozporządzenia ogólnego, jak i ustawodawstwa krajowego. Warto nadmienić, iż podstawy dopuszczalności przetwarzania danych biometrycznych z art. 9 ust. 2 rozporządzenia ogólnego są autonomiczne. Problematyka przetwarzania danych biometrycznych zgodnie z literą prawa najczęściej dotyczy relacji nierównorzędnych, takich jak m.in. stosunek pracy (podstawa prawna do przetwarzania danych biometrycznych pracowników), czy też jednostka – organ administracji publicznej (skutek wertykalny[46], działanie administracji publicznej bez podstawy prawnej).

[43] Zob. „Przegląd Orzecznictwa Europejskiego Dotyczącego Spraw Karnych" 2008, z. 3–4, oprac. M. Wąsek-Wiaderek, s. 20–25, http://www.sn.pl/orzecznictwo/Orzecz_Euro_Karne/Orzecz_Euro_Karne_03–04_2008.pdf (dostęp: 20 VII 2017).

[44] Dz.U. 1993 Nr 61, poz. 284.

[45] Zob. „Przegląd Orzecznictwa Europejskiego Dotyczącego Spraw Karnych" 2006, z. 4, oprac. M. Wąsek-Wiaderek, s. 19–20, http://www.sn.pl/orzecznictwo/Orzecz_Euro_Karne/Orzecz_Euro_Karne_04_2006.pdf (dostęp: 20 VII 2017). Szerzej zob. E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Springer Science & Business Media 2013, s. 212.

[46] Zob. B. Jaworska-Dębska i in., *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, Warszawa 2013, s. 57.

6. Przetwarzanie danych biometrycznych przez organy ścigania

Zgodnie z art. 2 ust. 2 lit. d rozporządzenia ogólnego „niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom". W polskim porządku prawnym dane biometryczne są często wykorzystywane w prowadzonych przez organy ścigania postępowaniach. Przykładowo, w myśl art. 21h ust. 1 pkt 1 i 2 Ustawy z dnia 6 kwietnia 1990 r. o Policji[47] Komendant Główny jest administratorem danych zbiorów danych o nazwach Centralna Registratura Daktyloskopijna (CRD) oraz Automatyczny System Identyfikacji Daktyloskopijnej (AFIS, ang. *Automated Fingerprint Identification System*). W przedmiotowych zbiorach przetwarzane są odciski linii papilarnych, m.in. osób podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego.

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[48] operuje tą samą definicją danych biometrycznych jak rozporządzenie ogólne, co wynika ze spójności obydwu aktów normatywnych. Dyrektywa ta zawęża przesłanki dopuszczalności przetwarzania szczególnych kategorii danych osobowych, a więc tym samym i danych biometrycznych[49]. Powyższy akt normatywny wskazuje na możliwość zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożeń, gdy w celu jednoznacznego zidentyfikowania osoby przetwarzane są m.in. dane biometryczne (motyw 51 preambuły dyrektywy 2016/680). Z kolei rozporządzenie ogólne operuje zwrotem „poważne ryzyko" w odniesieniu do operacji przetwarzania szczególnych kategorii danych, a tym samym i danych biometrycznych (motyw 51 preambuły rozporządzenia ogólnego).

[47] Tekst jedn. Dz.U. 2016, poz. 1782.

[48] Dz.Urz. UE 2016 L 119 z 4 V 2016 r., s. 89.

[49] Por. art. 9 ust. 2 rozporządzenia ogólnego oraz art. 10 dyrektywy 2016/680.

Podsumowanie

Problematyka przetwarzania danych biometrycznych zyskała na znaczeniu w związku z upowszechnieniem technologii wykorzystujących wyżej wymienione dane do identyfikacji i weryfikacji podmiotów danych. Towarzyszyć temu może niekiedy brak świadomości co do konieczności czynienia zadość przepisom z zakresu ochrony danych osobowych (odpowiedniego zabezpieczenia danych, legitymowania się właściwą podstawą dopuszczalności przetwarzania etc.). Taka sytuacja mogła mieć miejsce zwłaszcza na gruncie ustawy o ochronie danych osobowych, ten bowiem akt normatywny nie odnosił się literalnie w żadnym z przepisów do danych biometrycznych, co mogło stwarzać wątpliwości dotyczące m.in. stosowania tej ustawy. Dopiero w rozporządzeniu ogólnym prawodawca wprowadził definicję tychże danych, a także zaklasyfikował je do szczególnych kategorii danych osobowych, których przetwarzanie wiązać się będzie z koniecznością zaistnienia jednej z przesłanek z art. 9 ust. 2 rozporządzenia ogólnego. Swego rodzaju osobliwość danych biometrycznych wynika ze źródła ich pozyskiwania (cechy fizjologiczne, fizyczne, behawioralne). Niemniej nie należy tego postrzegać jako argumentu za ograniczeniem przetwarzania danych biometrycznych. W perspektywie czasu rozwiązania biometryczne zapewne będą stanowić przykład rozwiązania technicznego, które ma służyć zabezpieczeniu pomieszczenia, w którym są przetwarzane dane osobowe. Na gruncie rozporządzenia ogólnego należy jednak podchodzić do tego z pewną dozą ostrożności.

Podsumowując zatem, należy stwierdzić, że rozporządzenie ogólne unormowało kwestię przetwarzania danych biometrycznych jedynie w zakresie ogólnym. Wprowadzenie legalnej definicji danych biometrycznych przyczyni się zapewne do rozwiania wątpliwości odnośnie do stosowania wyżej wymienionego aktu normatywnego do przetwarzania tychże danych. Oznacza to, że do operacji lub zestawów operacji przetwarzania danych biometrycznych znajdą zastosowanie zarówno ogólne zasady przetwarzania, konieczność legitymowania się podstawą dopuszczalności przetwarzania, jak i realizowania uprawnień podmiotów danych. Przepisy szczególne mogą w tym zakresie doprecyzowywać cel przetwarzania, czy też okres przechowywania.

BIOMETRIC DATA PROCESSING. LEGAL ASPECTS

Summary

Biometric data processing and related data protection issues have gained importance as a result of a wide use of technologies using such data for the identification and verification of data subjects. Problems may arise due to the lack of awareness of the need to comply with the provisions on the protection of personal data. Such a problem could also have arisen in Poland. The Act on personal data protection, no longer in force, did not refer literally to any of the provisions on biometric data. This potentially could raise doubts, *inter alia,* with regard to the application of this Act, especially since only the General Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) introduced a definition of such data and classified them in special categories of personal data, the processing of which will require one of the conditions set out in Article 9(2) of the General Regulation. Such singularity of biometric data results from the source of their acquisition (physiological, physical and behavioural traits). This, however, should not be seen as an argument for the limiting of the processing of biometric data. It is nevertheless important that the processing of these personal data is in line with the principles set out in the General Regulation. The use of biometrics is likely to become more widespread in the long term. This trend is already taking place, but there is a noticeable concern on the part of the data subjects about the collection of these data. The legal provisions repealed in the context of the data protection reform in 2018 have also been taken into account in the deliberations.

Keywords: biometrics – data processing – personal data