

Malwina Magdalena Rosłonek

UMK Toruń

Biometria jest nauką, która koncentruje się na pomiarach istot żywych dla określenia ich indywidualnych cech i właściwości. Bada zarówno cechy fizyczne takie jak rozkład charakterystycznych punktów na twarzy, kształt dłoni czy uszu jak również cechy ściśle związane z zachowaniem – sposób chodzenia czy pisania. Z wyników badań tej dziedziny chętnie korzystają również inne nauki¹. Budowa i układ linii papilarnych stanowią główne zainteresowanie daktyloskopii, czyli działu techniki kryminalistycznej zajmującego się identyfikacją osób oraz zwłok na podstawie linii papilarnych i poletkowej budowy skóry. Kolejne badania XIX - wiecznych kryminologów, biologów i rzeszy innych badaczy prowadziły do coraz to nowszych odkryć. Faulds zauważył, że linie papilarne mogą stanowić potencjalny środek identyfikacji sprawców przestępstw. Herschel zaobserwował, że linie papilarne są niezmiennie. Największym osiągnięciem Galtona natomiast było przeprowadzenie dowodu matematycznego na niemożność spotkania dwóch osób o identycznym układzie linii papilarnych² Obserwacje te doprowadziły do szybkiego rozpowszechniania się nowej, skutecznej metody walki z przestępczością.

Współcześnie biometria znajduje coraz szersze zastosowanie w czynnościach codziennego życia - podczas autoryzacji dostępu do systemów informatycznych czy weryfikacji tożsamości np. w obszarze usług płatniczych. Zastosowanie danych biometrycznych w tych obszarach motywowane jest koniecznością wdrażania nowych rozwiązań, bezpieczniejszych niż wykorzystywanie kodów czy haseł w celu minimalizowania liczby przypadków kradzieży tożsamości użytkowników usług płatniczych wykorzystujących urządzenia elektroniczne³.

W obliczu coraz większego rozwoju nowych technologii oraz postępującej komercjalizacji metod biometrycznej identyfikacji i weryfikacji tożsamości, pojawiają się

¹ <http://www.cpd.mswia.gov.pl/technologia/biometria/>

² Cz. Grzeszy, Daktyloskopia, Wyd. CLK, Warszawa 1997

³ K. Sawicka, Wykorzystanie biometrii w procesie uwierzytelniania użytkowników elektronicznych usług płatniczych, „Monitor Prawniczy” | 23/2018

pytania dotyczące ochrony autonomii informacyjnej jednostki i ściśle z nią związanego prawa do prywatności.

Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby⁴. Jako szczególny rodzaj danych osobowych wymagają specjalnej ochrony. Ich przetwarzanie co do zasady jest zabronione poza sytuacjami przewidzianymi art. 9 ust. 2 Rozporządzenia ogólnego o ochronie danych osobowych (RODO). Wśród przesłanek legitymizujących przetwarzanie danych wrażliwych jakimi są dane biometryczne wskazano m.in. wyrażenie zgody podmiotu danych osobowych (chyba, że przepisy unijne lub krajowe wykluczają możliwość uchylenia zakazu przetwarzania danych biometrycznych), niezbędność przetwarzania danych biometrycznych dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody) ; konieczność przetwarzania ze względu na ważny interes publiczny⁵.

Zaistnienie jednej z przesłanek wymienionych w wyżej wskazanych przepisach stanowi podstawę dla przetwarzania danych biometrycznych. Proces ten musi jednak spełniać szereg warunków. Po pierwsze konieczna jest ocena zasadności zastosowania danych biometrycznych. Na ocenę te składają się następujące kwestie: niezbędność przetwarzania dla osiągnięcia celu (cel musi być istotny) istnienie alternatywnych środków o mniejszym stopniu inwazyjności służących realizacji celu. Kolejnym warunkiem jest wskazanie istnienia podstawy prawnej wykorzystania przedmiotowych danych. Relevantną kwestią jest sprawdzenie czy administrator danych zapewnia właściwą ochronę przetwarzanych danych⁶.

Analizując stan faktyczny przedstawiony w kazusie można mieć wątpliwości co do niezbędności, celowości oraz proporcjonalności przetwarzania tej kategorii danych. Istnieją bowiem alternatywne metody umożliwiające potwierdzenie tożsamości studenta podchodzącego do egzaminu bez tak istotnej ingerencji w jego autonomię informacyjną, przez chociażby okazanie legitymacji studenckiej do kamery podczas egzaminu. Wykorzystanie danych biometrycznych jest bardzo daleko idącą ingerencją w prywatność

⁴ Art. 4 pkt 14 RODO

⁵ Art. 9 ust. 2 RODO

⁶ A Plichta, [Dane biometryczne a ochrona danych osobowych \(lex.pl\)](#) [data dostępu: 26.05.2021 r.]

jednostki. Cel przetwarzania tego typu danych osobowych musi być na tyle poważny, aby usprawiedliwić konieczność przetwarzania.

Identyfikacja z zastosowaniem danych biometrycznych wiąże się ze skomplikowaną i złożoną procedurą, wymagającą zastosowania zaawansowanych technologicznie rozwiązań. Podstawą biometrycznej autentykacji jest porównanie zarejestrowanej w systemie uprzednio odczytanej próbki w postaci wzoru biometrycznego lub identyfikatora, z próbką nowo wykrytą w czasie procesu logowania. Na proces identyfikacji biometrycznej składa się wykrycie, przetworzenie i przyjęcie. Czujnik np. kamera wykrywa próbkę i następnie wyodrębnia z niej wyróżniające się cechy, które modyfikowane są w przetworzony wzorzec biometryczny. Następnie matematyczne przedstawienie wzorca zostaje rejestrowane w nośniku pamięci i wykorzystywana w późniejszym procesie weryfikacji tożsamości⁷. Mimo braku przechowywania zapisu obrazu oka i jego cech biometrycznych, system musi przechowywać klucz, który powiązany jest z określoną osobą. Ewentualny wyciek tego typu informacji może stwarzać potencjalne, wysokie ryzyko dla praw i wolności jednostki, której dotyczą. W tym miejscu nie sposób nie wspomnieć o kwestii technicznego zabezpieczenia przetwarzania danych biometrycznych. Konieczne jest opracowywanie kompleksowych regulaminów pracy z systemami informatycznymi, szkolenie pracowników uczestniczących w procesie przetwarzania danych osobowych. Fundamentem jest aktualizowanie programów antywirusowych i wszelkich aplikacji operacyjnych systemu⁸. Realia jednak często odbiegają od wymaganych standardów co nierzadko ma negatywne konsekwencje.

Co do podstawy prawnej działania uczelni można uznać za nią wyrażenie zgody przez studenta co stanowić będzie przesłankę z art. 9 RODO. Zgoda ta powinna być wyraźna i dobrowolna⁹. Element dobrowolności w przedmiotowej sprawie wydają się być jednak wątpliwy. Po pierwsze uwzględnić należy fakt czy wyrażenie zgody na przetwarzanie danych nie jest uzależnione od czynników zewnętrznych. W prezentowanym stanie faktycznym będzie to konieczność uzyskania zaliczenia egzaminu dla realizacji dalszej edukacji a także zależność studenta od podmiotu decydującego o sposobie i celach przetwarzania. W stosunku między administratorem danych – Uczelnią, a podmiotem danych – Studentem zauważalna jest wyraźna nie równorzędność tych dwóch podmiotów. Stosunek ten nosi znamiona

⁷ <https://biofinger.pl/biometria/> [dostęp: 27.05.2021 r.]

⁸ [Jak zgodnie z RODO zabezpieczyć dane osobowe? - PIT.pl](#) [dostęp: 28.05.2021 r.]

⁹ 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). Komentarz pod redakcją Pawła Litwińskiego.

stosunku administracyjnoprawnego w którym jedna ze stron wyposażona jest we władztwo administracyjne dzięki któremu może wywierać wpływ na sytuację podmiotu słabszego¹⁰. Student jest pozbawiony realnej szansy współdecydowania o celach i sposobach przetwarzania jego danych przez uniwersytet. Co niejako stawia go przed faktem dokonanym – brak zgody w zakresie przyjętego przez uczelnię sposobu i celu przetwarzania danych może wiązać się z zaistnieniem negatywnych dla niego konsekwencji. Dodatkowym aspektem wpływającym na swobodę wyrażenia zgody przez studenta jest konieczność osobistego przyjazdu na egzamin w warunkach stacjonarnych, w przypadku niewyrażenia aprobaty dla techniki weryfikacji tożsamości proponowanej przez Uniwersytet A. W obliczu stanu zagrożenia epidemicznego przyjazd studenta do budynku uniwersytetu (co często wiąże się z pokonywaniem wielu kilometrów a także koniecznością zorganizowania noclegu) może narazić studenta na dodatkowy stres a także ryzyko zakażenia. Konkludując zgoda, która nie spełnia warunków ogólnych określonych w Rozporządzeniu tj. nie jest wyraźna i dobrowolna, nie może być przesłanką legalizującą proces przetwarzania danych¹¹

¹⁰ A. Zieliński, Podmiotowość prawna (w:) S. Pikulski (red.) *Ius et lex. Księga Jubileuszowa Profesora Andrzeja Kabata*, Olsztyn 2004, s. 488.

¹¹ <https://uodo.gov.pl/pl/138/1943> [dostęp: 28.05.2021 r.]