Tytuł: „Skanowanie tęczówki oka jako sposób identyfikacji studentów podczas egzaminów”

Autor: Maria Kaczmarek – Wydział Prawa, Administracji i Ekonomii, Uniwersytet Wrocławski, Wrocław, IV rok.

W ciągu ostatnich lat zaobserwować można wzmożone zainteresowanie tematyką ochrony danych osobowych oraz wyraźne działania sektora publicznego ukierunkowane na skuteczną ich ochronę. Zjawisko to jest niewątpliwie formą odpowiedzi na dynamiczny rozwój nowoczesnych technologii i coraz większe możliwości związane z ułatwionym pozyskiwaniem danych[i]. Jednak jednym z najbardziej znaczących impulsów, które wpłynęły na obecny kształt tego sektora okazał się być wybuch pandemii COVID-19. Pojawienie się koronawirusa sprawiło, że dotychczasowe funkcjonowanie społeczeństwa przybrało zupełnie inną formę, a kontakty międzyludzkie ograniczone zostały do niezbędnego minimum. Konieczne było więc dostosowanie się do nowej rzeczywistości, co w rezultacie doprowadziło do potężnego rozwoju technologicznego oraz użycia Internetu, a co za tym idzie – powstania nowych form i możliwości gromadzenia oraz rejestrowania danych osobowych[ii]. Według badania przeprowadzonego przez OECD, ruch internetowy powstały w następstwie pandemii COVID-19 wzrósł aż o 60%[iii], a prognozy IDC wskazują, że przewidywany wzrost liczby danych w obrocie ma w 2025 r. osiągnąć 175 zettabajtów (w porównaniu do 33 zettabajtów w 2018 r.)[iv]. Za jeden z przejawów owego rozwoju technologicznego uznać można znaczne zwiększenie wykorzystania danych biometrycznych. Przykładem ich użycia mogą być techniki rozpoznawania twarzy celem dokonania płatności czy możliwość odblokowania smartfona poprzez skan linii papilarnych. Jednak w ramach przedmiotowej pracy analizie poddana zostanie kwestia dopuszczalności przetwarzania przez uczelnię danych biometrycznych w postaci tęczówki oka studenta, zbieranych w celu przeprowadzenia egzaminu, a także wynikających z tego działania obowiązków powstałych po stronie uczelni.

Aby poprawnie rozpatrzyć przedstawioną w kazusie sytuację, jako pierwsze konieczne będzie zdefiniowanie pojęcia danych biometrycznych. Według brzmienia art. 4 pkt 14 RODO[v], są *to „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne”*. By więc uznać, że w danym przypadku dojdzie do przetwarzania danych biometrycznych konieczne jest: (i) aby przetwarzane dane dotyczyły cech fizycznych, psychicznych lub behawioralnych danej osoby, (ii) poddane zostały procedurze specjalnego przetwarzania technicznego, (iii) były użyte w celu jednoznacznego zidentyfikowania danej

osoby[vi]. Poddając więc subsumpcji określony stan faktyczny, uznać należy, że w zaistniałej sytuacji uczelnia będzie przetwarzała dane biometryczne. Tęczówka oka studenta jest niewątpliwie jego cechą fizyczną, a przeprowadzenie weryfikacji tożsamości za pomocą rozwiązania przyporządkowującego określone punkty z tęczówki do stworzonego „klucza" uznać trzeba za rodzaj specjalnego przetwarzania technicznego. Bezsporna jest także kwestia celu owego przetwarzania, ukierunkowana na zidentyfikowanie tożsamości studenta.

W następnej kolejności rozważyć należy kwestię legalności przetwarzania tej kategorii danych osobowych. Podstawą przetwarzania danych studentów przez uczelnię jest art. 6 ust. 1 lit. e RODO, według którego działanie to jest legalne między innymi, gdy jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Warto w tym miejscu podkreślić, że mimo iż korzystanie z danych biometrycznych niesie ze sobą wiele zalet, takich jak łatwość i szybkość identyfikacji podmiotu, czy zmniejszone ryzyko ich sfałszowania, nie można pominąć zagrożeń płynących z ich przetwarzania. Dane biometryczne są bowiem niezmiennym i stale związanym z człowiekiem elementem, pozwalającym nie tylko na jego jednoznaczną identyfikację, ale również bardzo ograniczone możliwości ich zmiany w ciągu życia człowieka. To właśnie na skutek znaczącej ingerencji w prywatność jednostki, dopuszczalność przetwarzania tej kategorii danych jest na tak ograniczona, a po stronie administratora pojawia się konieczność wykazania niezbędności tego działania, jego celowości oraz proporcjonalności. Dane biometryczne są kategorią danych osobowych na tyle wrażliwych, że ich przetwarzanie jest co do zasady zabronione. Wspomniany zakaz potwierdzenie znajduje zarówno w postanowieniach RODO, jak i przyjętej przez Radę Europy Konwencji 108+[vii]. Nie jest to jednak zakaz absolutny, bowiem art. 9 ust. 2 lit. g RODO zawiera zamknięty katalog sytuacji, w których dozwolone będzie przetwarzanie tej kategorii danych. Jedną z nich jest zaproponowane w treści kazusu udzielenie przez podmiot wyraźnej zgody.

Udzielenie przez studenta zgody na przetwarzanie danych osobowych przez uczelnię nie może jednak zostać uznane za odpowiednią podstawę prawną w rozumieniu art. 9 ust. 2 lit. a RODO. Zgodnie z motywem 32, jak i art. 4 pkt 11 RODO, zgoda musi zostać wyrażona w sposób dobrowolny. Aby owa przesłanka została spełniona, należy rozpatrzeć ją pod kątem równowagi stron, a istnienie stosunku zwierzchnictwa uczelni wobec studenta może oznaczać, że brak jest możliwości wyrażenia przez niego w pełni dobrowolnego oświadczenia woli. Stanowisko to podkreśla motyw 43 RODO, jak i wytyczne Europejskiej Rady Ochrony Danych Osobowych dotyczące zgody[viii], według których mało prawdopodobne jest by organy publiczne mogły opierać się na tej podstawie przetwarzania, ze względu na brak równowagi między

administratorem a podmiotem danych osobowych. Tożsame podejście w kontekście dobrowolności udzielonej zgody przyjął sąd administracyjny w Marsylii, który w swoim orzeczeniu o sygnaturze N°1901249 z dnia 27 lutego 2020 r. uznał, że zgoda nie jest odpowiednią podstawą prawną do przetwarzania danych biometrycznych ucznia przez szkołę ze względu na istniejącą w tej relacji nierówność stron. W przedstawionej w kazusie sytuacji student nie miałby realnej możliwości wyboru, ponieważ istniałoby ryzyko poniesienia przez niego negatywnych konsekwencji w przypadku nieudzielenia zgody. Należy wziąć pod uwagę fakt, że w następstwie zawieszenia zajęć stacjonarnych na uczelniach, wielu studentów powróciło do rodzinnych domów i osobiste stawiennictwo na egzaminie mogłoby wiązać się z koniecznością poniesienia przez nich kosztów finansowych. Dodatkowo, nie można również wykluczyć prób wywierania przez egzaminatora nacisku czy presji wobec studenta, bowiem również i on zobligowany będzie do osobistego stawiennictwa na uczelni, w celu przeprowadzania osobnego egzaminu dla jednej osoby, bądź ich niewielkiej grupy.

Wobec powyższego, za odpowiednią podstawę prawną pozwalającą na przetwarzanie tej kategorii danych uznać należy wyjątek przewidziany przez art. 9 ust. 2 lit. g RODO, a więc gdy „*przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą*". Podstawą taką, mającą zastosowanie w opisanym stanie faktycznym jest wprowadzony ustawą z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2[ix] art. 76a Prawa o szkolnictwie wyższym i nauce[x], który pozwala uczelniom na przeprowadzanie zaliczeń i egzaminów kończących zajęcia poza siedzibą uczelni lub poza jej filią przy użyciu środków komunikacji elektronicznej. Powyższy wyjątek obarczony jest jednak pewnymi zasadami, które administrator obowiązany jest spełnić. Przede wszystkim konieczne jest zastosowanie się do ujętej w art. 5 ust. 1 lit. c RODO zasady minimalizacji, a więc określenia czy przetwarzanie tego rodzaju danych jest adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Przywołany artykuł wskazuje, że owe przetwarzanie ma być „niezbędne", co oznacza, że cel, dla którego zbierane są dane biometryczne nie może być osiągnięty innym sposobem.

Z przedstawionego stanu faktycznego wynika, że uczelnia, w celu ograniczenia podszywania się za studentów przez inne osoby, wprowadziła rozwiązanie polegające na skanowaniu tęczówki oka, które spowoduje możliwość pobrania przez niego pliku z zadaniem

egzaminacyjnym. Nie umniejszając zasadności wdrożenia przez uczelnię technik pseudonimizacji danych za pomocą stworzenia odpowiedniego klucza z szyfrem, nie można uznać, że będzie ona wystarczającym zabezpieczeniem, uzasadniającym przetwarzanie danych biometrycznych. Biorąc pod uwagę wymogi RODO związane z zasadą minimalizacji danych, ciężko byłoby zgodzić się ze stwierdzeniem, że owa propozycja stawiałaby im zadość. Potwierdza to stanowisko holenderskiego organu nadzoru, wydane dnia 28 kwietnia 2020 r.[xi], według którego wykorzystanie danych biometrycznych może być uzasadnione tylko w wyjątkowych sytuacjach, takich jak na przykład kontrola wstępu do pomieszczeń z uwagi na bardzo wysoką potrzebę zapewnienia bezpieczeństwa. Dodatkowo, jak wskazuje motyw 84 RODO, aby móc przetwarzać tak wrażliwe dane osobowe studentów, zwłaszcza przy użyciu nowych technologii, konieczne byłoby przeprowadzenie oceny skutków dla ochrony danych. Również Prezes Urzędu Ochrony Danych Osobowych w swoim Komunikacie z dnia 17 czerwca 2019 r.[xii] wskazując wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, wymienił między innymi sytuacje polegające na „*przetwarzaniu danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej*", a także „*innowacyjnym wykorzystaniu lub zastosowaniu rozwiązań technologicznych lub organizacyjnych*".

Sytuacja opisana w ramach stanu faktycznego pozwala stwierdzić, że istnieją inne, mniej inwazyjne sposoby zweryfikowania tożsamości studenta. Jako jedną z propozycji wskazać można możliwość użycia przez niego uczelnianego konta internetowego lub uczelnianej poczty mailowej, za pomocą których uzyska on dostęp do bazy dokumentów udostępnionych przez uczelnię. W tym przypadku za odpowiednią podstawę prawną pozwalającą na przetwarzanie danych osobowych studenta należałoby przyjąć art. 76a Prawa o szkolnictwie wyższym i nauce, w związku z 6 ust. 1 lit. e RODO. Jeżeli jednak uczelnia uzna, że opisany sposób weryfikacji jest niewystarczający, może zdecydować się na rozwiązanie, polegające na poleceniu studentowi okazania egzaminatorowi legitymacji studenckiej bądź dowodu osobistego (zasłaniając równocześnie inne dane, takie jak na przykład imiona rodziców) do kamery zainstalowanej na komputerze. Pozwoli to egzaminatorowi na zweryfikowanie tożsamości studenta bez konieczności przetwarzania danych biometrycznych, gdyż jak wskazuje wspomniany art. 4 pkt 14 RODO, aby uznać dane za biometryczne, muszą one zostać poddane specjalnemu przetwarzaniu technicznemu, którego w podanej propozycji brak – tożsamość zostaje zweryfikowana za pomocą czynnika ludzkiego, bez użycia środków automatycznego przetwarzania. Stanowisko to potwierdza motyw 51 RODO, według którego fotografie nie powinny zostać uznane za dane biometryczne, jeżeli nie są przetwarzane specjalnymi metodami

technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.

Niezależnie od wyboru metody weryfikacji tożsamości studenta, uczelnia zobligowana jest na mocy art. 24 RODO do zapewnienia pewnych podstawowych warunków technicznych i organizacyjnych dla przetwarzania i przechowywania danych osobowych studentów. Wśród nich wskazać należy przede wszystkim wdrożenie koncepcji „*privacy by design*" polegającej na aktywnym uwzględnianiu zabezpieczeń w samej technologii, na każdym etapie przetwarzania danych, zapewnienie poufności danych, ich zgodności, odpowiedniej kontroli dostępu i zabezpieczenie przed ich dostępem przez osobę nieupoważnioną. Konieczne będzie również zastosowanie się do koncepcji „*privacy by default*", nakładającej na administratora danych obowiązek postępowania zgodnie z zasadą minimalizacji i celowości. Szczególne środki powinny być jednak wdrożone w przypadku przetwarzania danych biometrycznych, a więc stosowanie wzorca biometrycznego, zalecenie przechowywania owych danych w kontrolowanej przez administratora bazie, zaprojektowanie systemów biometrycznych w sposób umożliwiający odwołanie elementów potwierdzających tożsamość w celu ich odnowienia lub trwałego usunięcia (na przykład poprzez użycie technologii „*Turbine*"), czy posiadanie automatycznego mechanizmu usuwania danych, aby uniknąć przechowywania informacji biometrycznych dłużej niż jest to konieczne[xiii].

W sytuacji przetwarzania przez uczelnię danych osobowych studentów, konieczne będzie spełnienie przez nią określonych obowiązków. Przede wszystkim, jako administrator danych osobowych, musi ona uczynić zadość nałożonemu na nią na mocy art. 13 RODO obowiązkowi informacyjnemu. Student powinien zostać poinformowany o danych dotyczących administratora, danych kontaktowych inspektora danych osobowych (o ile został wyznaczony), celu i podstawie przetwarzania oraz o odbiorcach jego danych. Dodatkowo, aby zapewnić gwarancję rzetelnego i przejrzystego przetwarzania, uczelnia musi poinformować o okresie ich przechowywania, a także poinformować o prawach przysługujących studentowi w związku z operacją przetwarzania. Na prawa te składają się przede wszystkim możliwość dostępu do danych go dotyczących, żądania ich sprostowania, usunięcia czy ograniczenia przetwarzania, a także możliwość wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych. W sytuacji, gdy uczelnia nie przewiduje udziału czynnika ludzkiego w procesie przetwarzania danych (na przykład w pełni powierzając systemowi skanującemu proces weryfikacji tożsamości studenta), będzie ciążył na niej obowiązek poinformowania studenta o możliwości zautomatyzowanego podejmowania decyzji, a także o ich zasadach, znaczeniu i przewidywanych konsekwencjach z niej wynikających. Informacje te muszą zostać mu

przekazane albo bezpośrednio przed zebraniem danych, albo w momencie ich zbierania, jednak nie później niż w chwili zbierania danych osobowych. RODO pozostawia dowolność co do sposobu wykonania obowiązku informacyjnego, a więc uczelnia może dostarczyć odpowiednie informacje przykładowo za pomocą poczty elektronicznej lub ustnie.

Konkludując, na podstawie przeprowadzonej analizy można dojść do wniosku, że mimo istnienia odpowiedniej podstawy prawnej do przetwarzania przez uczelnię danych biometrycznych w tak innowacyjnym rozwiązaniu, należy zwrócić uwagę, że jest to procedura bardzo ryzykowna. Z kolei dostępność innych, mniej ingerujących w prywatność studenta sposobów pozwalających na potwierdzenie jego tożsamości tylko potęguje przekonanie o nieproporcjonalności i nieadekwatności tej metody. Bez względu na wybrany rodzaj weryfikacji tożsamości uczelnia, jako administrator danych, będzie zobowiązana do spełnienia nałożonych na nią obowiązków, w szczególności obowiązku informacyjnego, polegającego na podaniu studentowi wszelkich wiadomości niezbędnych do zachowania przejrzystości, jak i rzetelności przetwarzania jego danych.

[ii] *European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy* COM (2014) 442 final, Brussels, 2 July 2014;

[iii] OECD (2020), *Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides*, Digital Economy Outlook 2020 Supplement, OECD, Paris;

[iv] IDC, 2018.;

[v] 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).;

[vi] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

[vii] Konwencja nr 108 RE o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, podpisana w Strasburgu dn. 28 stycznia 1981 r. (Ogłoszona D.n. 85-1203, 15 list. 1985.- JO 20 list. 1985. Weszła w życie 1.10.1985);

[viii] Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, Wersja 1.1., przyjęta dnia 4 maja 2020;

[ix] Ustawa z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (t.j. Dz. U. z 2021 r. poz. 737).

[x] Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2021 r. poz. 478 z późn. zm.);

[xi] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf

[xii] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. z 2019 r. poz. 666);

[xiii] Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych, przyjęta w dniu 27 kwietnia 2012 r.,