Białostockie Studia Prawnicze
2020 vol. 25 nr 4

DOI: 10.15290/bsp.2020.25.04.06
Received 05.06.2020
Accepted 28.08.2020

Mateusz Kupiec
Uniwersytet Jagielloński, Polska
kupiec67@gmail.com
ORCID: https://orcid.org/0000–0001-7280–8955

Ochrona danych osobowych studentów w dobie rozwoju technologii biometrycznych wyzwaniem dla polskich uczelni

Protection of Students' Personal Data in Times of Development of Biometric Technologies as a Challenge for Universities in Poland

Abstract: Biometric technologies have been gaining popularity lately. An increasing number of enterprises and public entities worldwide are using them for security measures. Many universities in the European Union have also begun to recognise the benefits of implementing biometric systems in their organisations, and it is just a matter of time before universities in Poland join them as well. However, biometric data used by such systems are especially sensitive as they may reveal intimate information about data subjects. As such, they are counted among special categories of personal data, the processing of which is in principle prohibited by art. 9 (1) GPDR. Furthermore, the processing of students' personal data demands special care from universities as they are vulnerable data subjects. Students are namely subordinate to university authorities, which significantly limits their scope of autonomy. Therefore, the use of biometric technologies poses a challenge for universities in Poland. The following article aims to present the main reasons why students are vulnerable data subjects and which legal grounds provided by GDPR are most suitable for processing their biometric data by universities.
Keywords: students, biometrics, GDPR, right to privacy, personal data protection
Słowa kluczowe: studenci, biometria, RODO, prawo do prywatności, ochrona danych osobowych

Wprowadzenie

Właściwe funkcjonowanie uczelni wyższych nie jest możliwe bez wykorzystywania danych osobowych, co nakłada na nie obowiązek dostosowania struktury organizacyjnej do wymogów wynikających z krajowego porządku prawnego oraz przede

wszystkim bezpośrednio z RODO[1]. Nakaz działania uczelni wyższych zgodnie z najwyższymi obowiązującymi standardami międzynarodowymi, moralnymi (a do takich należy właśnie ochrona autonomii informacyjnej jednostek) został również podkreślony przez ustawodawcę w preambule do Prawa o szkolnictwie wyższym i nauce[2], jak i w treści art. 3 wspomnianej ustawy. Największą grupę osób, których dane osobowe są przetwarzane na uczelniach, stanowią studenci. Chociaż początkowo wydawało się, że uczelnie wyższe jako administratorzy danych osobowych skutecznie wywiązują się z obowiązków wynikających z RODO[3], to praktyka stosowania rozporządzenia pokazała, że niektórym z nich nie udało się zapewnić wystarczającego poziomu bezpieczeństwa przetwarzanym danym osobowym. Świadczy o tym wyciek danych ze Szkoły Głównej Gospodarstwa Wiejskiego (SGGW), związany z kradzieżą laptopa, na którym przetwarzane były dane osobowe kandydatów na studia w procesie rekrutacji[4]. Przeprowadzona w związku z tym wydarzeniem kontrola Prezesa Urzędu Ochrony Danych Osobowych wykazała poważne zaniedbania natury technicznej jak i organizacyjnej ze strony uczelni, polegające między innymi na braku aktualizacji i przeglądów przyjętych polityk bezpieczeństwa oraz na uchybieniach związanych ze sposobem sprawowania funkcji inspektora ochrony danych[5]. Warto również dodać, że do podobnych incydentów związanych z danymi osobowymi studentów doszło niedawno na Politechnice Warszawskiej[6] oraz na SWPS Uniwersytecie Humanistycznospołecznym (SWPS)[7]. Tym samym wydaje się, że część polskiego szkolnictwa wyższego może niedostatecznie rozumieć zagrożenia i wyzwania wynikające z korzystania z nowych technik przetwarzania informacji w celu przetwarzania danych osobowych.

Powyższe wątpliwości co do przygotowania krajowych uczelni wyższych na wyzwania technologiczne drugiej dekady XXI wieku stają się coraz bardziej aktualne w dobie wzrostu znaczenia i obecności systemów sztucznej inteligencji w nowoczesnej edukacji. Zmiany te wiążą się bowiem nieuchronnie z kolejnymi dylematami w kontekście ochrony autonomii informacyjnej studentów. Wspomniane wyzwa-

1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE L 119 z 4.5.2016, dalej: RODO).

2 Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, Dz.U. z 2020 r. poz. 85, ze. zm. (dalej: prawo o szkolnictwie wyższym i nauce).

3 M. Kawecki, Uczelnie poradziły sobie z RODO (WYWIAD), https://serwisy.gazetaprawna.pl/edukacja/artykuly/1286710,maciej-kawecki-o-stosowaniu-RODO-przez-uczelnie-wyzsze.html (20.05.2020).

4 Wszczęcie postępowania wobec SGGW, https://uodo.gov.pl/pl/138/1464 (20.05.2020).

5 *Ibidem*.

6 Nieuprawniony dostęp do danych z Politechniki Warszawskiej, https://uodo.gov.pl/pl/138/1518 (20.05.2020).

7 Dostęp do danych SWPS, https://uodo.gov.pl/pl/138/1512 (20.05.2020).

nia stają się szczególne widoczne w kontekście wzrostu znaczenia rozwiązań biometrycznych, z których zaczynają korzystać niektóre zagraniczne uczelnie[8], dążąc do usprawnienia swojego funkcjonowania w relacjach z kształconymi przez nie osobami. Funkcjonowanie takich rozwiązań opiera się na znaczącej ingerencji w autonomię informacyjną jednostek co sprawia, że stanowią one zagrożenie dla tego obszaru prywatności studentów. Z tego względu rozpoczęcie korzystania przez władze jednej z amerykańskich uczelni z niektórych rodzajów technologii biometrycznych spotkało się z protestem tej części wspólnoty akademickiej[9].

Tym samym celem opracowania jest analiza problemów związanych z ochroną danych osobowych studentów w aspekcie korzystania przez polskie uczelnie wyższe z szeroko rozumianych systemów biometrycznych. Przedstawione zostaną zagadnienia legalności stosowania rozwiązań biometrycznych przez uczelnie wyższe w ich relacjach ze studentami. Pomocne dla analizy problemu będzie również przedstawienie studentów jako podmiotów, których dane osobowe powinny być przetwarzane przez uczelnię przy zachowaniu daleko idącej ostrożności.

1. Szczególna wrażliwość studentów jako podmiotów danych w relacjach z uczelnią

Na wstępie niniejszych rozważań warto wskazać, dlaczego ochrona danych osobowych studentów powinna być szczególnie ważna dla współczesnego szkolnictwa wyższego. W przeciwnym razie nie będzie możliwe pełne zrozumienie istoty wyzwań dla szkolnictwa wyższego w kontekście gwarancji autonomii informacyjnej tej grupy.

W odróżnieniu od przepisów Ustawy z 27 lipca 2005 r. – Prawo o szkolnictwie wyższym[10] w obecnej ustawie brak jest legalnej definicji studenta. Nie stoi to jednak na przeszkodzie, aby kierując się doświadczeniem życiowym uznać, że studentami są wszystkie osoby kształcące się na studiach pierwszego lub drugiego stopnia albo na jednolitych studiach magisterskich. Jednocześnie należy zauważyć, że pozycja studentów w ich relacjach z uczelnią może być postrzegana zarówno horyzontalnie[11] jak

8 Biometrics in Schools, Colleges & Universities: Application and Impact, https://www.m2sys.com/blog/biometric-identification/biometrics-in-schools-colleges-universities-application-and-impact/ (20.05.2020).

9 University students concerned by facial recognition technology on campus, https://www.studyinternational.com/news/facial-recognition-campus/ (20.05.2020), Amid coronavirus, USC is requiring facial recognition scans of students living on campus, but the technology sparks controversyhttp://www.uscannenbergmedia.com/2020/05/15/amid-coronavirus-usc-is-requiring-facial-recognition-scans-of-students-living-on-campus-but-the-technology-sparks-controversy/ (20.05.2020).

10 Dz.U. z 2017 r. poz. 2183 ze. zm.

11 Studenci mogą być bowiem postrzegani jako klienci uczelni, odbiorcy oferowanych przez nie usług edukacyjnych, oraz jako członkowie tworzącej ją wspólnoty akademickiej.

i wertykalnie. Dla celów niniejszego opracowania szczególne znaczenie będzie mieć drugie ze wspomnianych ujęć. Biorąc pod uwagę przepisy RODO stosunek pomiędzy szkołą wyższą a kształconymi przez nią studentami będzie mieć charakter pionowy: administrator danych osobowych (uczelnia) – osoba, której dane dotyczą (student). Należy bowiem zauważyć, że jednostki, których dane osobowe są przetwarzane przez administratora, nie mogą wspólnie z nim ustalać celów lub sposobów tego procesu[12]. Brak możliwości współdecydowania o wykorzystywanych przez uczelnię nowych technikach przetwarzania informacji uwypukla również fakt, że szkoła wyższa jest zakładem administracyjnym, w którym jego użytkownicy – studenci – podlegają władztwu zakładowemu[13]. Należy zauważyć, że na władztwo zakładowe składa się zakres upoważnień dla organów zakładu do jednostronnego kształtowania stosunków prawnych z jego użytkownikami oraz uprawnienie organów zakładu do realizowania własnych zarządzeń, zmierzających do osiągania celów zakładu przy zastosowaniu przymusu administracyjnego[14].

Powyższe okoliczności mają doniosłe znaczenie dla ochrony danych osobowych tej części wspólnoty akademickiej, ponieważ przesądzają one o tym, że grupę tę trzeba zaliczyć do kategorii tzw. wrażliwych podmiotów danych (z ang. *vulnerable data subjects*[15]*, vulnerable natural persons*[16]). Wprawdzie RODO nie wyodrębnia wprost takiej kategorii podmiotów, ale w rezultacie zastosowania gramatycznej wykładni treści rozporządzenia zauważono[17], że nakazuje ono szczególną ostrożność przy przetwarzaniu danych osobowych niektórych podmiotów[18]. Pogląd ten należy uznać za słuszny, ponieważ postrzeganie przez jednostkę granic własnej prywatności, której elementem jest właśnie autonomia informacyjna, zależy nie tylko od czynników kulturowych czy biologicznych (wiek), ale również właśnie od jej pozycji spo-

12 A. Sobczyk, RODO. Rozproszona władza publiczna, Kraków 2019, s. 64.

13 Postanowienie NSA z dnia 25 września 1986 r., SA/Gd 513/86, OSP 1998, z. 3, poz. 88.

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

15 G. Malgieri, J. Niklas, Vulnerable Data Subjects, „Computer Law and Security Review", Special Issue on Data Protection and Research 2020, vol. 37, s. 1 i n., https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=3569808 (20.05.2020).

16 Motyw 75 preambuły do RODO.

17 Anglojęzyczna treść motywu 75 preambuły do RODO wskazuje bowiem, że „the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from (…) where personal data of vulnerable natural persons, in particular of children are processed". Użyty przez unijnego prawodawcę zwrot „in particular", który został przetłumaczony w polskiej wersji RODO jako „w szczególności", wskazuje na otwarty katalog podmiotów wrażliwych (z ang. *vulnerable*). Tym samym możliwe jest, że również przetwarzanie danych osobowych innych podmiotów niż dzieci może wymagać od administratorów danych osobowych szczególnej ostrożności i staranności.

18 G. Malgieri, J. Niklas, Vulnerable…, *op. cit*., s. 7.

łecznej[19]. Powyższe stanowisko znajduje również potwierdzenie w orzecznictwie Europejskiego Trybunału Praw Człowieka (ETPC) w kontekście interpretacji treści art. 8 Europejskiej Konwencji Praw Człowieka. Trybunał uznał bowiem w wyrokach w sprawach Trabajo Rueda przeciwko Hiszpanii[20] oraz K.U. przeciwko Finlandii[21] istnienie takich podmiotów (z ang. *other vulnerable individuals*), których prywatność (a więc i dane osobowe) wymaga szczególnych gwarancji[22]. Nie da się bowiem zagwarantować odpowiedniej ochrony autonomii informacyjnej jednostek, nie biorąc jednocześnie pod uwagę właśnie ich rzeczywistej sytuacji faktycznej. W związku z powyższym należy dojść do wniosku, że RODO tworzy dodatkową warstwę ochronną dla podmiotów danych wymagających szczególnego traktowania[23].

Co więcej, jak wynika z opinii Grupy Roboczej Art. 29, potrzeba specjalnego traktowania pewnych kategorii osób, których dane dotyczą, ma charakter kontekstualny i związana jest z brakiem równorzędnej relacji pomiędzy nimi a administratorem danych osobowych[24]. Zdaniem Grupy dla oceny pozycji konkretnej osoby względem administratora jej danych osobowych istotne jest m.in. to, że jest ona na przykład studentem[25]. Dla procesu przetwarzania danych osobowych mają więc znaczenie okoliczności, które wskazują lub mogą wskazywać na zależność jednostki od podmiotu decydującego o celach i sposobie przetwarzania jej danych osobowych. Z tego właśnie względu w kontekście relacji student – uczelnia doniosłe znaczenie ma przedstawione wcześniej władztwo zakładowe. Ma ono bowiem charakter stosunku administracyjnoprawnego[26], którego cechą jest nierównorzędność podmiotów oraz nadrzędność organów zakładu (uczelni) wobec jego użytkowników, co sprawia, że uczelnia jednostronnie może wpływać na sytuację studentów. W związku z brakiem równorzędnej pozycji pomiędzy szkołami wyższymi a studentami podmioty te, rozpoczynając proces przetwarzania danych osobowych kształconych przez nie osób, muszą każdorazowo brać pod uwagę fakt, że autonomia informacyjna członków tej grupy podlega szczególnej ochronie w kontekście korzystania przez nich ze świad-

19 M. Rojszczak, Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warszawa 2019, s. 35.

20 Wyrok ETPC z 30 maja 2017 w sprawie *Trabajo Rueda v. Spain*, nr skargi 32600/12.

21 Wyrok ETPC z 2 grudnia 2008 w sprawie *K.U. v. Finland*, nr skargi 2872/02.

22 European Court of Human Rights, Press Unit, Factsheet – New technologies, s. 5 i s. 12, https://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf (20.05.2020).

23 European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, s. 25, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (20.05.2020).

24 Opinia 06/2014 Grupy Roboczej Art. 29 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, s. 46, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pl.pdf (20.05.2020).

25 *Ibidem,* s. 46–47.

26 M. Stahl (red.), Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie, Warszawa 2016, s. 282.

czeń uczelni (w tym przypadku – edukacji, możliwości kształcenia się i otrzymania tytułu zawodowego), a także samego przebywania na terenie zakładu. Okoliczność ta będzie mieć znaczący wpływ na dopuszczalność stosowania przez uczelnie rozwiązań opartych na przetwarzaniu systemów biometrycznych, co zostanie przedstawione w dalszej części opracowania.

2. Dopuszczalność stosowania rozwiązań biometrycznych przez uczelnie

2.1. Charakterystyka rozwiązań biometrycznych

Pojęcie biometrii wywodzi się z greckich wyrazów *bios* oraz *metron*, oznaczających kolejno 'życie' oraz 'pomiar', i obejmuje swoim zakresem technologie pozwalające na identyfikację jednostek w oparciu o ich indywidualne cechy fizyczne, fizjologiczne lub behawioralne. Należy bowiem zauważyć, że każda część lub właściwość ludzkiego ciała, które zawierają informacje o człowieku, mogą służyć do jego identyfikacji, jeżeli da się je tylko wykryć i zmierzyć. Współcześnie technologie biometryczne są wykorzystywane przez aplikacje, które umożliwiają automatyczną identyfikację lub weryfikację tożsamości konkretnej osoby, tzw. systemy biometryczne[27]. Szczegółowy sposób działania systemu biometrycznego może różnić się w zależności od tego, jakie pozyskuje on informacje. Jednakże celem stosowania takich rozwiązań jest zawsze rozpoznawanie pewnych wzorów, co pozwala charakteryzować proces działania każdego systemu w pewien uproszczony sposób:

- system pozyskuje i rejestruje informacje (*input*), np. ogólny kształt dłoni przyłożonej do skanera;
- następnie interesujące system dane są wyodrębniane z ogółu zarejestrowanych informacji (*acquisition*);
- odpowiedni algorytm dokonuje standaryzacji (*normalisation*) pozyskanego w ten sposób obrazu w zakresie m.in. rozmiaru, barw, co ułatwia proces poddania go analizie;
- w kolejnym etapie tworzy on wzór (*feature extraction*) z przetworzonego obrazu;
- system klasyfikuje pozyskany wzór na potrzeby jego rozpoznania;
- przetworzony wzór jest porównywany z informacjami znajdującymi się w bazie podmiotu stosującego dany system biometryczny (*comparision*)[28];

27 Opinia 3/2012 Grupy Roboczej Art. 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych, s. 4, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_pl.pdf (20.05.2020).

28 Na podstawie: Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes s. 8, https://data.unicef.org/wp-content/uploads/2019/10/Biometrics_guidance_document_faces_fingersprint_feet-July-2019.pdf (20.05.2020).

– przetworzony obraz oraz pozostałe dane zostają zapisane lub automatycznie usunięte w zależności od potrzeb, dla których konkretny podmiot stosuje system biometryczny w swojej strukturze.

2.2. Możliwe zastosowania dla biometrii na uczelniach wyższych

Technologie biometryczne są niczym innym jak rozwiązaniami opartymi na zastosowaniu sztucznej inteligencji w celu identyfikacji lub uwierzytelnienia. Pod pierwszym z tych pojęć należy rozumieć proces porównywania danych biometrycznych danej osoby (uzyskanych w momencie identyfikacji) z szeregiem szablonów biometrycznych przechowywanych w bazie danych podmiotu[29], podczas gdy uwierzytelnianie to procedura bezpieczeństwa, która opiera się na analizie niepowtarzalnych cech charakterystycznych konkretnej osoby w celu sprawdzenia, czy jest ona tym, za kogo się podaje[30]. Tym samym biometria wydaje się idealnym sposobem do zapewniania bezpieczeństwa na uczelni poprzez na przykład kontrolę dostępu do pomieszczeń, laboratoriów. Już teraz w niektórych państwach[31] karty identyfikacyjne, na których zapisane są dane biometryczne, stosuje się na wielu uniwersytetach w takim właśnie celu oraz jako środek do sprawniejszej identyfikacji studentów podczas egzaminów[32]. Dzięki zastosowaniu biometrii na przykład w postaci czytników linii papilarnych jako środka bezpieczeństwa, władze uniwersytetu mogą ograniczyć ryzyko, że nieuprawniona osoba będzie mogła swobodnie poruszać się po terenach lub obiektach należących do uczelni[33]. Co więcej, zastosowanie biometrii (np. technologii rozpoznawania twarzy) może służyć uwierzytelnianiu tożsamości użytkownika systemów informatycznych uczelni, co zmniejszy ryzyko przejęcia przez nieuprawnione osoby dostępu do baz danych uczelni. W ten sposób podmioty te zwiększyłyby poziom bezpieczeństwa przetwarzanych danych osobowych i w konsekwencji mogłyby stać się bardziej odporne na część zagrożeń związanych z obecnością w cyberprzestrzeni[34].

---

29 Opinia 3/2012…, *op. cit*., s. 6.

30 Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania, s. 21, https://op.europa.eu/pl/publication-detail/-/publication/aace9398–594d-11ea-8b81–01aa75ed71a1/language-pl/format-PDF (20.05.2020).

31 W szczególności w Stanach Zjednoczonych Ameryki. Przykładem takiego zastosowania systemów biometrycznych są środki wdrożone przez Auburn University w stanie Alabama w celu kontroli dostępu do należących do niej obiektów sportowych.

32 R. Lewandowski, Biometria – nowe zastosowania, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 159 http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-e75c5ccf-d9d9–4f7b-8bdc-57654cce7549 (20.05.2020).

33 Biometrics at Universities: 5 Ways Biometric Data Can Be Used To Enhance Learning, https://blogs.harvard.edu/blockchain/biometrics-at-universities-5-ways-biometric-data-can-be-used-to-enhance-learning/ (20.05.2020).

34 Niemniej jednak należy pamiętać, że istnieją metody pozwalające na ominięcie uwierzytelniania przy pomocy biometrii i w konsekwencji przejęcia tożsamości innej osoby, np. ataki typu spoofing.

Biometria behawioralna może być również stosowana jako środek nadzoru studentów podczas egzaminów pisemnych w celu eliminacji ryzyka potencjalnych oszustw. Systemy oparte na tej technice dokonują pomiaru w czasie rzeczywistym (najczęściej za pomocą monitoringu wizyjnego) zachowania konkretnej osoby (np. egzaminowanego) i polegają na analizie m.in. siły naciśnięć klawiszy, sposobu poruszania się lub siedzenia[35]. Postrzegają więc one jednostkę jako pewną całość zdefiniowanych wcześniej scenariuszy zachowania, przez co system może rozpoznać działania odbiegające od przyjętych standardów, np. zaglądanie w pracę kolegi/koleżanki piszącej egzamin obok[36]. W sytuacji odejścia od wcześniej zarejestrowanego szablonu system mógłby w takim przypadku odpowiednio oznaczyć na zapisie z monitoringu sali egzaminacyjnej studenta podejrzanego o nieetyczne postępowanie w celu szczegółowej weryfikacji danej sytuacji przez egzaminatora.

2.3. Stosowanie technologii biometrycznych na uczelniach a przepisy RODO

W związku z powyższym warto zauważyć, że funkcjonowanie systemów biometrycznych jest oparte na przetwarzaniu szczególnej kategorii danych osobowych, tzw. danych biometrycznych, które RODO definiuje jako dane osobowe wynikające ze specjalnego przetwarzania technicznego, dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne[37]. Przedstawiony wcześniej uproszczony model funkcjonowania systemu biometrycznego można zaklasyfikować jako „specjalne przetwarzanie techniczne", które powoduje nieodwracalną modyfikację związku pomiędzy cechami fizycznymi jednostki a jej tożsamością[38]. Z tego względu unijny prawodawca zdecydował się uznać dane tego rodzaju za dane szczególnej kategorii, których przetwarzanie jest co do zasady zakazane (art. 9 ust. 1 RODO).

Wspomniany zakaz nie ma jednak charakteru bezwzględnego. Stanowi on bowiem wskazówkę interpretacyjną, która nakazuje administratorowi stosowanie ścieśniającej wykładni sytuacji, w których dopuszczono przetwarzanie szczególnych kategorii danych osobowych[39]. Takie okoliczności zostały wyszczególnione w treści art. 9 ust. 2 RODO i mają one charakter warunków dopuszczalności. W kontekście codziennego funkcjonowania uczelni potencjalnymi przesłankami legalizującymi proces przetwarzania wydają się: wyraźna zgoda studenta (art. 9 ust. 2 lit. a RODO) lub niezbędność przetwarzania „ze względów związanych z ważnym interesem pu-

35 Opinia 3/2012…, *op. cit*., s. 18.

36 Using AI and biometrics to enhance exam proctoring, https://www.biometricupdate.com/202001/using-ai-and-biometrics-to-enhance-exam-proctoring (20.05.2020).

37 Art. 4 pkt 14 RODO.

38 Opinia 3/2012…, *op. cit*., s. 2.

39 W. Chomiczewski, Przesłanki legalizacyjne przetwarzania danych osobowych, (w:) D. Lubasz (red.), Meritum Ochrony Danych Osobowych, Warszawa 2020 s. 139.

blicznym, 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" (art. 9 ust. 2 lit. g RODO).

Wyraźna zgoda jednostki stanowi takie oświadczenie woli, którego sposób wyrażenia sprawia, że fakt akceptacji procesu przetwarzania przez osobę, której dane dotyczą, nie ulega wątpliwości. Co więcej, aby takie oświadczenie było ważne, musi ono stanowić dobrowolne, konkretne, świadome i jednoznaczne okazanie woli (art. 4 pkt 11 RODO). Kluczowe znaczenie dla oceny dopuszczalności wyraźnej zgody studenta jako podstawy przetwarzania dotyczących go danych biometrycznych przez uniwersytet będzie mieć odpowiedź na pytanie, czy w relacji student – władze uczelni można mówić o dobrowolności. Na etapie wcześniejszych rozważań wykazane zostało, że studenci należą do grupy podmiotów danych osobowych charakteryzujących się szczególną podatnością w relacji z administratorem ich danych osobowych (uczelnią) z racji braku równorzędnej pozycji pomiędzy nimi. W motywie 43 preambuły do RODO podkreślono, że zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym. Sama uczelnia oraz jej organy nie są wprawdzie organami administracji publicznej w znaczeniu ustrojowym, ale są organami w znaczeniu funkcjonalnym[40], wyposażonymi w przedstawione wcześniej władztwo administracyjne. Tym samym zgoda studenta na stosowanie systemów biometrycznych nie zawsze może być dobrowolna, ponieważ nie znajduje się on jako jednostka w pozycji równorzędnej do władz uczelni. Warto zauważyć, że podobną wykładnią posłużył się również szwedzki organ nadzorczy (Datainspektionen) w decyzji nakładającej karę na szkołę stosującą technologię rozpoznawania twarzy do monitorowania obecności uczniów[41]. Organ ten wskazał, że monitorowanie obecności uczniów przy użyciu takiego rozwiązania stanowi jednostronny środek do sprawowania kontroli oraz że uczniowie znajdują się w sytuacji zależności od szkoły zarówno m.in. odnośnie do możliwości otrzymywania pomocy materialnej, stypendiów, jaki i kontynuowania nauki[42]. Wnioski te wydają się również trafne w przedmiocie sytuacji studentów na uczelni. Wobec powyższego wyraźna zgoda studentów na wykorzystanie dotyczących ich danych biometrycznych w celu na przykład kontroli

40 L. Klat-Wertelecka, Organy szkoły wyższej w postępowaniu administracyjnym, (w:) J. Blicharz, A. Sus, A. Chrisidu-Budnik (red.), Zarządzenia szkołą wyższą, Wrocław 2014, s. 124, http://www.repozytorium.uni.wroc.pl/Content/63647/12_Klat_Wertelecka_Lidia.pdf, (20.05.2020).

41 Facial recognition in school renders Sweden's first GDPR fine, https://www.datainspektionen.se/nyheter/2019/facial-recognition-in-school-renders-swedens-first-gdpr-fine/ (20.05.2020).

42 Decyzja Szwedzkiego Urzędu Ochrony Danych z dnia 20 sierpnia 2019 roku, nr DI–2019-2221, s. 4–5. https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf (20.05.2020).

dostępu do pomieszczeń uniwersytetu nie zawsze będzie stanowić ważną podstawę przetwarzania w świetle RODO.

Artykuł 9 ust. 2 lit. g RODO daje natomiast administratorowi możliwość oparcia legalności procesu przetwarzania danych biometrycznych na szczególnym interesie publicznym, wynikającym z prawa unijnego lub wewnętrznego prawa członkowskiego. Należy zauważyć, że administratorzy korzystający z tej przesłanki muszą przetwarzać dane osobowe w ramach zadań i kompetencji przyznanych im na podstawie przepisów prawa. Pojęcie interesu publicznego ma charakter nieostry i stanowi klauzulę generalną odsyłającą do prawa materialnego. Można jednak przyjąć, że interes publiczny wiąże się z określonymi wartościami, celami lub z potrzebami, które mają doniosły charakter dla społeczeństwa[43]. W tym kontekście wydaje się, że przetwarzanie danych biometrycznych studentów mogłoby służyć rektorowi uczelni do realizacji nałożonego na niego ustawowego obowiązku dbania o utrzymanie porządku i bezpieczeństwa na terenie uczelni (art. 50 ust. 1 prawa o szkolnictwie wyższym i nauce). Jednakże nie wydaje się, żeby zastosowanie systemów biometrycznych do tego celu było niezbędne i proporcjonalne, ponieważ istnieją inne skuteczne sposoby jego realizacji, które nie wymagają przetwarzania danych biometrycznych, na przykład kontrola dostępu do pomieszczeń uczelni za pomocą legitymacji studenckich. Ponadto żaden przepis na gruncie prawa o szkolnictwie wyższym i nauce obecnie nie przewiduje gwarancji, które mogłyby zostać uznane za „odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą" w świetle art. 9 ust. 2 lit. g RODO.

Wnioski

Rozwój systemów biometrycznych niesie ze sobą nowe możliwości, ale również i wyzwania dla uczelni wyższych. Przetwarzanie danych biometrycznych z racji ich szczególnej wrażliwości wymaga bowiem szczególnej ostrożności po stronie administratora danych osobowych. Kontekst ich przetwarzania przez uniwersytety może powodować poważne ryzyko dla podstawowych praw i wolności studentów w związku z brakiem równorzędnej pozycji pomiędzy nimi jako podmiotami danych a władzami uczelni. Z tego też względu ochrona danych osobowych studentów powinna być brana każdorazowo przez uczelnie pod uwagę w przypadku implementacji nowych rozwiązań bazujących na przetwarzaniu informacji, które pozwalają na identyfikację konkretnych osób. Warto też zauważyć, że stosowanie systemów biometrycznych nie wydaje się niezbędne na przykład do zapewnienia bezpieczeń-

43 A. Żurawik, „Interes publiczny, „interes społeczny" i „interes społecznie uzasadniony". Próba dookreślenia pojęć, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, nr 2, s. 62, https://doi.org/10.14746/rpeis.2013.75.2.5 (20.05.2020).

stwa studentów lub ochrony mienia uczelni, ponieważ cel ten może zostać osiągnięty w sposób, który w mniejszym stopniu ingeruje w autonomię informacyjną jednostek.

Jednocześnie należy zauważyć, że obecnie w polskim porządku prawnym brakuje przepisów, które pozwalałyby uczelniom na przetwarzanie danych biometrycznych studentów w celu identyfikacji lub weryfikacji tożsamości. *De lege ferenda* można postulować ich wprowadzenie przez ustawodawcę pod warunkiem, że będą one zawierać „środki ochrony praw podstawowych i interesów osoby, której dane dotyczą", o których mowa w art. 9 ust. 2 lit. g RODO. Do takich środków w kontekście przetwarzania danych biometrycznych przez uczelnie można zaliczyć na przykład wymóg konsultacji z samorządem studenckim przed podjęciem decyzji o korzystaniu z systemu biometrycznego.

BIBLIOGRAFIA

Chomiczewski W., Przesłanki legalizacyjne przetwarzania danych osobowych, (w:) D. Lubasz (red.), Meritum Ochrony Danych Osobowych, Warszawa 2020.

Klat-Wertelecka L., Organy szkoły wyższej w postępowaniu administracyjnym, (w:) J. Blicharz, A. Sus, A. Chrisidu-Budnik (red.), Zarządzenia szkołą wyższą, Wrocław 2014.

Lewandowski R., Biometria – nowe zastosowania, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17.

Malgieri G., Niklas J., Vulnerable Data Subjects, „Computer Law and Security Review", Special Issue on Data Protection and Research 2020, vol. 37.

Rojszczak M., Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warszawa 2019.

Sobczyk A., RODO. Rozproszona władza publiczna, Kraków 2019.

Stahl M. (red.), Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie, Warszawa 2016.

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

Żurawik A., „Interes publiczny", „interes społeczny" i „interes społecznie uzasadniony". Próba

dookreślenia pojęć, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, nr 2.