

MATEUSZ KUPIEC

Przetwarzanie danych biometrycznych dzieci w związku z korzystaniem ze szkolnej stołówki. Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 10 października 2024 r., III OSK 4804/21

Processing Children's Biometric Data in the Context of Using a School Canteen. Commentary to the Judgment of the Supreme Administrative Court of 10.10.2024, III OSK 4804/21

Abstract

The commentary is a critical analysis of the Supreme Administrative Court (NSA) ruling, which found that the processing of students' biometric data by a school for verifying payments for the use of the school canteen services complies with the requirements of the GDPR. The analysis elaborates in detail on the court's interpretation of the principle of data minimization, purpose limitation, and the criterion of "freely given" consent. The author points out inaccuracies in the court's assessment, arguing that the processing of children's biometric data in this manner constitutes a disproportionate interference with their privacy. The author discusses the court's reasoning regarding the relationship between the consent of the data subject and the data processing principles outlined in Article 5 of the GDPR. Concerns are also raised about the court's assessment that the legal guardians' consent was "freely given", which, according to the author, fails to sufficiently account for the relationship between the school and students and the potential imbalance of power between the parties.

KEYWORDS: biometrics, children, GDPR, privacy, school

SŁOWA KLUCZOWE: biometria, dzieci, szkoła, prywatność, RODO

MATEUSZ KUPIEC – magister prawa, Instytut Nauk Prawnych Polskiej Akademii Nauk, ORCID – 0000-0001-7280-8955, e-mail: m.kupiec@inp.pan.pl

Przedmiotem głosowanego orzeczenia Naczelnego Sądu Administracyjnego (dalej: NSA) jest ocena zgodności z przepisami RODO^[1] przetwarzania przez Szkołę X (dalej: Szkoła) odcisków palców uczniów korzystających z usług stołówki szkolnej w celu weryfikacji uiszczenia opłaty za posiłek wydany w danym dniu. Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) stwierdził naruszenie przez placówkę przepisów art. 5 ust. 1 lit. c oraz art. 9 ust. 1 RODO w związku z takim wykorzystaniem danych biometrycznych dzieci i decyzją nałożył na nią administracyjną karę pieniężną w wysokości 20 000 zł^[2]. NSA, podzielając stanowisko wyrażone przez Wojewódzki Sąd Administracyjny (dalej: WSA) w Warszawie^[3], który uchylił wyżej wskazaną decyzję Prezesa UODO, oddalił skargę kasacyjną organu. Wyrok NSA wymaga pogłębionego komentarza w szczególności ze względu na przyjętą przez skład orzekający wykładnię zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO), zasady ograniczonego celu przetwarzania (art. 5 ust. 1 lit. b RODO) oraz wymogu „dobrowolności” zgody na przetwarzanie danych biometrycznych uczniów wyrażoną w ich imieniu przez opiekunów prawnych.

Dokonując weryfikacji zarzutu skarżącego kasacyjnie organu dotyczącego dokonania błędnej interpretacji przez WSA zasady minimalizacji danych, NSA uznał, że przetwarzanie danych biometrycznych dzieci w celu korzystania przez nie ze stołówki szkolnej jest adekwatne do celu, dla którego są przetwarzane, tj. ustalenia, czy konkretny uczeń jest uprawniony do otrzymania posiłku w danym dniu. W ocenie składu orzekającego art. 5 ust. 1 lit. c RODO nakazuje administratorowi ograniczanie przetwarzania danych osobowych wyłącznie do sytuacji, gdy jest to niezbędne do osiągnięcia celu przetwarzania i nie istnieją inne rozsądne sposoby jego realizacji bez przetwarzania danych osobowych, przy uwzględnieniu porównywalnych kosztów i zasobów. Tym samym według NSA zasada minimalizacji wprowadza wymóg proporcjonalnego zakresu przetwarzania danych, dopuszczając operacje na danych tylko wtedy i tylko w takim

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 Nr 119, 1 ze zm.), dalej: RODO.

² Prezes Urzędu Ochrony Danych Osobowych, decyzja z dnia 18 lutego 2020 r., ZSZZS.440.768.2018, <https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018> [dostęp: 12.04.2025].

³ Wyrok WSA w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20.

zakresie, jaki jest niezbędny do osiągnięcia zamierzonego celu. Należy stwierdzić, że NSA prawidłowo zinterpretował art. 5 ust. 1 lit. c RODO jako warunek nakazujący administratorowi ograniczenie zakresu przetwarzanych danych osobowych do informacji niezbędnych do realizacji określonych przez niego celów, o ile cele te nie mogą zostać osiągnięte bez ich wykorzystania^[4]. Pomimo dokonania poprawnej wykładni zasady minimalizacji danych, zdaniem autora NSA błędnie ocenił przetwarzanie danych biometrycznych dzieci przez Szkołę w związku z korzystaniem przez nie ze stołówki jako spełniające wymogi art. 5 ust. 1 lit. c RODO. Dane osobowe można uznać za adekwatne do osiągnięcia celu przetwarzania, gdy ich przyporządkowanie do tego celu jest uzasadnione i nie budzi wątpliwości, a ich zakres ogranicza się do danych niezbędnych dla realizacji celu, przy czym szczególne kategorie danych nie mogą być przetwarzane w błahych, pospolitych celach^[5]. Wskazanie przez unijnego prawodawcę w art. 9 ust. 2 RODO dodatkowych wymogów warunkujących dopuszczalność przetwarzania tego rodzaju informacji odzwierciedla jego zamiar, aby szczególne kategorie danych osobowych zawsze były przetwarzane w możliwie najwęższym zakresie^[6]. Praktyki polegającej na wykorzystywaniu przez Szkołę przekształconych we wzorce biometryczne odcisków palców dzieci z powodów organizacyjnych, wynikających z potrzeby weryfikacji uiszczenia opłaty za wydanie posiłku w stołówce, nie można natomiast uznać za obiektywnie adekwatną, stosowną i niezbędną do realizacji tak sformułowanego celu potwierdzenia tożsamości ucznia. Takie działanie stanowi bowiem nieproporcjonalną ingerencję w prywatność dziecka (z uwagi na niewspółmierność pomiędzy relatywnie prozaicznym celem operacji na danych, jakim jest weryfikacja uiszczenia opłaty za usługę, a bardzo poważną ingerencją w sferę autonomii informacyjnej dziecka).

Szkoła już przed sądem pierwszej instancji argumentowała, że weryfikacja opłat za obiady początkowo odbywała się za pomocą elektronicznej

⁴ Alexander Roßnagel i Philipp Richter, "Article 5. Principles Relating to Processing of Personal Data," w *General Data Protection Regulation Article-by-Article Commentary*, red. Indra Spiecker gen. Döhmman et al. (Baden-Baden: Nomos, 2023), 279 – 280.

⁵ Eike Michael Frenzel, "Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten," w *Datenschutzgrundverordnung. Bundesdatenschutzgesetz*, red. Boris Paal i Daniel Pauly (München: C.H. Beck, 2021), Nb. 35.

⁶ Michèl Finck i Asja Biega, "Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems", *Technology and Regulation*, nr 1 (2021): 57 i przywołane tam stanowiska organów nadzorczych z zakresu ochrony danych osobowych.

karty obiadowej, a system czytnika linii papilarnych został wprowadzony dopiero później, gdy wcześniej stosowane rozwiązania okazały się niewystarczające ze względów organizacyjnych (np. dzieci często gubiły karty lub zapominały je zabrać)^[7]. Przetwarzanie danych biometrycznych nie jest jednak zwykłą operacją techniczną. Proces ten polega na przekształcaniu unikalnych cech człowieka w ich ustandaryzowane cyfrowe odwzorowania, co w konsekwencji prowadzi do uprzedmiotowienia jednostki – sprowadzenia jej do zbioru mierzalnych właściwości – oraz ograniczenia jej kontroli nad sposobem, w jaki wykorzystywane są informacje o podstawowym znaczeniu dla jej tożsamości^[8]. Osoby, których dane biometryczne dotyczą, nie mogą same zmienić swoich cech fizycznych, na podstawie których utworzono wzorzec biometryczny, w takim stopniu, aby szablony przestały umożliwiać ich pośrednią lub bezpośrednią identyfikację^[9]. Warto dodać, że systemy biometryczne są projektowane przede wszystkim z myślą o dorosłych i jako takie rozwiązania te nie zawsze są odpowiednie do wykorzystania na potrzeby rozpoznawania dzieci. Niektóre cechy biometryczne dzieci zmieniają się wraz z wiekiem, co może powodować konieczność ponownego uzyskania próbek biometrycznych, np. pobrania obrazu odcisku palca^[10]. Uwzględniając powyżej przedstawiony unikalny charakter danych biometrycznych, należy uznać, że wykorzystanie cyfrowego odwzorowywania odcisku palca ucznia przez Szkołę do weryfikacji dokonania płatności za posiłki w stołówce stanowi naruszenie zasady minimalizacji danych. Problemy organizacyjne związane z korzystaniem z tradycyjnych metod uwierzytelniania tożsamości uczniów nie stanowią

⁷ Wyrok WSA w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20.

⁸ Christiane Wendehorst i Yannik Duller, *Biometric Recognition and Behavioural Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on Their Current and Future Use in Public Spaces* (Brussels: European Parliament, 2021), 44, [https://www.europarl.europa.eu/thinktank/en/document/IPOLE_STU\(2021\)696968](https://www.europarl.europa.eu/thinktank/en/document/IPOLE_STU(2021)696968) [dostęp: 12.04.2025].

⁹ Ibidem. Okoliczność ta zwiększa także ryzyko dla praw i wolności podmiotów danych w przypadku naruszenia ochrony danych biometrycznych – np. w wyniku uzyskania do nich dostępu przez nieuprawnioną osobę trzecią – szerz. Agencia Española de Protección de Datos (AEPD) i European Data Protection Supervisor (EDPS), *14 Misunderstandings with Regard to Biometric Identification and Authentication*, 4, https://www.edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en [dostęp: 12.04.2025].

¹⁰ UNICEF, *Faces, Fingerprints and Feet: Guidance on Assessing the Value of Including Biometric Technologies in UNICEF-Supported Programmes*, 6, <https://data.unicef.org/resources/biometrics/> [dostęp: 12.04.2025].

obiektywnej przeszkody dla Szkoły w zastosowaniu rozwiązań mniej inwazyjnych dla prywatności dzieci takich jak karty dostępu^[11] lub metody weryfikacji biometrycznej, które wykorzystują mniej charakterystyczne cechy biometryczne – np. porównywanie geometrii dłoni^[12]. Ustalając proporcjonalny zakres danych dzieci, który ma zostać wykorzystany do realizacji określonego celu przetwarzania, administratorzy powinni zwracać uwagę na szczególną podatność tej grupy podmiotów danych na potencjalne zagrożenia związane z przetwarzaniem informacji na ich temat^[13]. NSA, kontrolując zgodność zaskarżonego orzeczenia z prawem w granicach swojej właściwości, w szczególności w kontekście oceny sądu pierwszej instancji dotyczącej spełnienia przez Szkołę zasady minimalizacji danych, powinien uwzględnić specyficzny charakter danych biometrycznych dzieci oraz związane z nimi ryzyko naruszenia ich praw i wolności.

W dalszej części omawianego orzeczenia NSA stwierdził istnienie silnej normatywnej korelacji pomiędzy zasadą ograniczenia celu przetwarzania danych osobowych (art. 5 ust. 1 lit. b RODO) a zgodą osoby fizycznej na przetwarzanie danych, uznając, że prawidłowo wyrażona zgoda, spełniająca wymogi określone w RODO (dobrowolność, konkretność, świadomość i jednoznaczność), skutkuje wyraźnym określeniem celu przetwarzania. Zdaniem składu orzekającego to zgoda podmiotu wyznacza ramy

¹¹ Szkoła mogła wprowadzić rozwiązania, które ograniczyłyby potencjalne zakłócenia w codziennym funkcjonowaniu stołówki i nie wymagałyby przetwarzania danych biometrycznych uczniów – np. elektroniczne powiadomienia przypominające dzieciom i ich rodzicom o konieczności zabrania karty obiadowej przed wyjściem z domu. Dodatkowo przyjęcie odpowiedniej procedury umożliwiającej szybkie wydawanie duplikatów kart uczniom mogłoby także znacząco zmniejszyć zakłócenia codziennego funkcjonowania stołówki w przypadku zgubionych lub utraconych kart.

¹² Podobnie Commission nationale de l'informatique et des libertés (CNIL), Délibération 2011-147 du 19 mai 2011, <https://www.legifrance.gouv.fr/cnil/id/CNIL-TEXT000024880869> [dostęp: 12.04.2025]. CNIL uznał, że skanowanie odcisków palca uczniów szkoły średniej i porównywanie ich kształtu naczyń krwionośnych na potrzeby weryfikacji możliwości korzystania ze stołówki narusza zasadę minimalizacji danych, ponieważ stanowi nieproporcjonalną ingerencję w prywatność uczniów, zwłaszcza że cechy biometryczne dzieci są niestabilne i zmienne w czasie – szerz. Claire Gayrel, "The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL's Deliberations," *Computer Law & Security Review* 32, nr 3 (2016): 457.

¹³ Zgodnie z motywem 38 RODO uzasadnieniem szczególnej ochrony danych osobowych dzieci jest ich mniejsza świadomość ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.

dopuszczalności dokonywania przez administratora operacji na danych, w tym cel, zakres, ilość, sposób i okres przetwarzania danych, przez co jej uzyskanie realizuje zasadę minimalizacji danych (art. 5 ust. 1 lit. c RODO). W konsekwencji NSA uznaje, że Prezes UODO jako organ nadzoru nie może kwestionować celu przetwarzania danych osobowych, zakresu i ilości przetwarzanych danych, sposobu oraz okresu ich przetwarzania przyjętego przez administratora i osobę, która udzieliła zgody na przetwarzanie danych osobowych. Twierdzenie NSA, że wyrażenie przez osobę, której dane dotyczą, ważnej zgody w rozumieniu RODO jest równoznaczne ze spełnieniem zasad przetwarzania danych z art. 5 RODO, należy poddać krytyce, ponieważ takie stanowisko nie znajduje oparcia ani w treści normatywnej rozporządzenia, ani w preambule do niego. Zasady przetwarzania danych osobowych wymienione w tym przepisie mają bowiem status metanorm, które wpływają na wszystkie inne przepisy rozporządzenia^[14]. W wyniku realizacji obowiązków określonych w rozporządzeniu administratorzy urzeczywistniają zasady z art. 5 RODO w taki sposób, aby przetwarzanie danych osobowych służyło ludzkości^[15]. Pogląd NSA o podrzędności zasad ograniczonego celu przetwarzania i minimalizacji danych do jednej z podstaw prawnych przetwarzania danych – zgody osoby, której dane dotyczą – należy zatem uznać za sprzeczny z wewnętrzną systematyką RODO, która przypisuje art. 5 RODO nadrzędny charakter do pozostałych przepisów rozporządzenia jako wytycznych określających granice ich wykładni. Wbrew argumentacji NSA osoby, których dane dotyczą (lub osoby działające w ich imieniu), udzielając administratorowi zgody na przetwarzanie ich danych, nie formułują wspólnie z nim „subiektywnej oceny” co do zgodności procesu przetwarzania z art. 5 RODO, a jedynie wyrażają przyzwolenie na konkretne warunki (okoliczności) przetwarzania danych przedstawione przez administratora. Ustalenie konkretnych, wyraźnych i prawnie uzasadnionych celów przetwarzania danych, a także adekwatnego, stosownego, niezbędnego zakresu danych do osiągnięcia tego celu jest wyłączną rolą podmiotu, który sprawuje kontrolę nad procesem przetwarzania danych, a nie osoby, której dane dotyczą. Europejska Rada Ochrony Danych (dalej: EROD) jednoznacznie wyjaśnia, że uzyskanie

¹⁴ Data Protection Commission, *Quick Guide to the Principles of Data Protection*, 1, https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf [dostęp: 12.04.2025].

¹⁵ Roßnagel i Richter, „Article 5,” 264 – 265.

zgody osoby fizycznej ani nie zwalnia administratora danych z obowiązku przestrzegania zasad przetwarzania zawartych w art. 5 RODO, ani nie wpływa na ich zakres^[16]. Zdaniem EROD wyrażenie przez osobę zgody na przetwarzanie jej danych osobowych nie sprawia, że dopuszczalne staje się gromadzenie tych informacji na jej temat, które nie są niezbędne do realizacji określonego przez administratora celu przetwarzania^[17]. Zgoda jest tylko jedną z podstaw prawnych przetwarzania danych i jej uzyskanie nie może zwalniać administratora z obowiązku przestrzegania ogólnych zasad przetwarzania danych osobowych, które należy uwzględnić w pierwszej kolejności, projektując proces przetwarzania danych^[18]. Przyjęcie, tak jak twierdzi NSA, że zgoda podmiotu danych jako przejaw jego woli wpływa „na rozumienie zakresu normowania i stosowania zasad przetwarzania danych” oraz uniemożliwia organowi nadzoru ocenę zgodności przetwarzania z art. 5 RODO, doprowadziłoby do nieakceptowalnej sytuacji z punktu widzenia *ratio legis* RODO, w której administratorzy mogliby wykorzystywać oświadczenia woli osoby, której dane dotyczą, jako uzasadnienie przetwarzania nadmiarowych informacji na jej temat. W konsekwencji taki sposób wykładni przepisów rozporządzenia uczyniłby ze zgody podmiotu danych środek służący do potencjalnej legitymizacji każdej nieproporcjonalnej ingerencji w jego podstawowe prawo do ochrony danych osobowych. Kompetencje organu nadzoru z zakresu monitorowania i kontroli przestrzegania przepisów o ochronie danych osobowych, w tym możliwość zakwestionowania zgodności działań administratora z RODO, nie mogą zostać ograniczone w wyniku udzielonego administratorowi oświadczenia osoby, której dane dotyczą. Uzupełniając

¹⁶ Europejska Rada Ochrony Danych, *Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679*, 5, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [dostęp: 12.04.2025].

¹⁷ Ibidem. W piśmiennictwie wskazuje się także, że uznanie przetwarzania przez administratora informacji należących do szczególnych kategorii danych za „adekwatne” art. 5 ust. 1 lit. c RODO jest wątpliwe, nawet jeśli osoba, której dane dotyczą, wyraziła wyraźną zgodę na określony cel przetwarzania związany z zakresem przetwarzanych danych – tak Roßnagel i Richter, „Article 5,” 280.

¹⁸ Wykazanie przez administratora istnienia odpowiedniej podstawy prawnej do przetwarzania danych osobowych jest warunkiem koniecznym, lecz niewystarczającym dla zapewnienia ogólnej zgodności operacji danych z RODO – każda operacja na danych osobowych musi spełniać wymagania określone w art. 5, który ustanawia podstawowe zasady przetwarzania danych – tak Giovanni Sartor, „Article 6. Lawfulness of Processing,” w *General Data Protection Regulation Article-by-Article Commentary*, red. Indra Spiecker gen. Döhmman et al. (Baden-Baden: Nomos, 2023), 293.

należy dodać, że obowiązek realizowania zasad z art. 5 RODO może być potencjalnie ograniczony prawem Unii Europejskiej lub prawem państwa członkowskiego, któremu podlega administrator, o ile takie ograniczenie spełnia warunki określone w art. 23 RODO – przepis ten nie zawiera jakiegokolwiek odniesienia do zgody osoby, której dane dotyczą, w kontekście przesłanek uzasadniających wpływanie przez unijnego lub krajowego prawodawcę na zakres stosowania wymogów rozporządzenia.

Sąd słusznie zauważył, że zgoda podmiotu danych jest samodzielną przesłanką przetwarzania i może być stosowana niezależnie od innych podstaw prawnych z art. 6 ust. 1 RODO oraz art. 9 ust. 2 RODO, co wynika z rozłącznego charakteru każdej z przesłanek. Taki pogląd został już wyrażony przez sąd pierwszej instancji w omawianej sprawie i został on zaaprobowany w piśmiennictwie jako zgodny z systematyką RODO^[19]. Krytycznie należy jednak ocenić argument NSA o przesądzeniu przez unijnego prawodawcę, że „autonomia osoby udostępniającej swoje dane ma najwyższą moc legitymizującą proces ich przetwarzania”. Każda z podstaw prawnych przetwarzania danych osobowych wskazanych w art. 6 ust. 1 RODO i każdy z warunków dopuszczalności określonych art. 9 ust. 2 RODO ma bowiem samodzielny i równoprawny charakter – żadne z nich nie mają uprzywilejowanego statusu w stosunku do pozostałych przesłanek^[20] (na co zresztą sam NSA zwraca uwagę we wcześniejszej części uzasadnienia wyroku). Tym samym niemożliwe jest uznanie za prawidłowy w świetle RODO poglądu NSA o nadrzędności tych przesłanek przetwarzania danych, które odnoszą się do oświadczenia woli osoby fizycznej, nad pozostałymi podstawami prawnymi z art. 6 ust. 1 RODO i art. 9 ust. 2 RODO.

Omawiając tę część uzasadnienia, należy również krytycznie odnieść się do argumentacji NSA, który porównuje przesłankę zgody podmiotu danych (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO) z wyjątkiem dopuszczającym przetwarzanie szczególnych kategorii danych, o którym mowa w art. 9 ust. 2 lit. e RODO, dotyczącym danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą. W ocenie NSA „oczywiste upublicznienie swoich wrażliwych danych osobowych jest formą wyrażenia zgody na ich przetwarzanie [...] i nie sposób również

¹⁹ Arwid Mednis, „Wykorzystanie danych biometrycznych w szkole. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20,” *Gdańskie Studia Prawnicze*, nr 4 (2021): 133

²⁰ Dominik Lubasz, „5. Przesłanki legalizacyjne przetwarzania danych osobowych,” w *Meritum. Ochrona danych osobowych*, red. Dominik Lubasz (Warszawa: Wolters Kluwer, 2022), 121 oraz Sartor, „Article 6,” 293.

weryfikować, czy upublicznione dane osobowe będą adekwatne do celu ich przetwarzania, albowiem na moment ich upublicznienia nie da się ustalić, czy w ogóle będą przetwarzane, a jeżeli tak, to w jakim celu”. Samo upublicznienie przez podmiot danych informacji na jego temat, o którym mowa w art. 9 ust. 1 lit. e RODO, nie jest bowiem wystarczające dla uznania, że osoba ta udzieliła zgody na przetwarzanie danych osobowych w rozumieniu RODO^[21]. Upublicznienie danych w sposób oczywisty przez osobę fizyczną nie jest formą wyrażenia „wyraźnej zgody” z art. 9 ust. 2 lit. a RODO, lecz stanowi po prostu kolejną, alternatywną sytuację, w której unijny prawodawca uznał za dopuszczalne przetwarzanie szczególnych kategorii danych^[22]. Każdy z warunków dopuszczalności określonych w art. 9 ust. 2 RODO jest niezależny od pozostałych i możliwość jego zastosowania wobec określonego procesu przetwarzania wymaga dokonania autonomicznej oceny^[23]. Co więcej, wyrażenie przez podmiot danych zgody, o której mowa w art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO, jest oświadczeniem woli skierowanym wyłącznie do jednego określonego podmiotu – administratora danych uzyskującego zgodę – podczas gdy „oczywiste upublicznienie”, o którym mowa w art. 9 ust. 2 lit. e RODO, jest działaniem polegającym na ujawnieniu danych osobowych nieokreślonemu kręgowi adresatów przez osobę, której dane dotyczą. Udzielając zgody na przetwarzanie danych osobowych, jednostka wyraża zatem bezpośrednio chęć, aby jej dane były wykorzystywane w związku z przedstawionym jej celem administratora, którego tożsamość jest jej znana. Natomiast „upubliczniając w oczywisty sposób” szczególne kategorie danych, osoba fizyczna wyraźnie okazuje

²¹ Wyrok TSUE z dnia 4 października 2024 r. w sprawie C446/21, *Maximilian Schrems przeciwko Meta Platforms Ireland Ltd*, EU:C:2024:834, pkt 82; podobnie opinia rzecznika generalnego Athanasiosa Rantosa z dnia 25 kwietnia 2024 r. w sprawie C-446/21, *Maximilian Schrems przeciwko Meta Platforms Ireland Ltd*, pkt 40, 43, 45–47. Przedmiotem sprawy, której dotyczyły przywołane orzeczenie i opinia rzecznika generalnego, była ocena zgodności z RODO przetwarzania danych dotyczących orientacji seksualnej jednostki przez platformę internetową w celach marketingowych, po tym jak zostały one ujawnione opinii publicznej przez podmiot danych podczas dyskusji panelowej.

²² Council of Europe, European Court of Human Rights, European Data Protection Supervisor i European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law – 2018 Edition* (Luxembourg: Publications Office of the European Union, 2018), 182, <https://data.europa.eu/doi/10.2811/58814> [dostęp: 12.04.2025].

²³ Wyrok TSUE z dnia 21 grudnia 2023 r. w sprawie C-667/21, *ZQ przeciwko Medizinischer Dienst der Krankenversicherung Nordrhein*, EU:C:2023:1022, pkt 47.

zamiar podania do publicznej wiadomości wysoce osobistych informacji na swój temat, jednocześnie dopuszczając możliwość, że w rezultacie takiego zachowania z jej danymi będzie potencjalnie mógł zapoznać się każdy. Postawienie zatem przez NSA znaku równości pomiędzy warunkiem dopuszczalności określonym w art. 9 ust. 2 lit. e RODO a zgodą na przetwarzanie danych osobowych wydaje się zatem zbyt daleko idącym stwierdzeniem. Ponadto sam fakt „oczywistego upublicznienia” szczególnych kategorii danych osobowych przez podmiot danych nie zwalnia administratora z obowiązku realizacji zasad przetwarzania danych osobowych z art. 5 RODO, co zostało już przesądzone w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE)^[24] oraz w stanowiskach EROD^[25]. Dla zaistnienia obowiązku realizacji zasad przetwarzania danych osobowych z art. 5 RODO, zwłaszcza zasady ograniczonego celu przetwarzania i minimalizacji danych, bez znaczenia jest wskazywany przez NSA brak możliwości ustalenia przez administratora w momencie ujawnienia przez osobę fizyczną informacji na jej temat, czy będzie on w ogóle wykorzystywał te dane. Nie istnieje bowiem przetwarzanie bez celu^[26]. Administrator ustala cel przetwarzania danych oraz zakres informacji niezbędnych do jego osiągnięcia przed rozpoczęciem przetwarzania danych osobowych, a samo publiczne ujawnienie przez osobę fizyczną jej danych osobowych nie jest równoznaczne z automatycznym podjęciem przez administratora czynności zmierzających do ich wykorzystania.

Zastrzeżenia budzi także wniosek NSA o braku naruszenia przez Szkołę zasady „dobrowolności” zgody w związku ze zbieraniem oświadczeń woli opiekunów prawnych dotyczących przetwarzania danych biometrycznych dzieci ze względu na korzystanie przez nie ze szkolnej stołówki. NSA uznał, że takie zgody zostały wyrażone dobrowolnie, ponieważ odmowa ich wyrażenia nie skutkowałą niewydaniem posiłku, a weryfikacja opłacenia posiłku była możliwa alternatywnie poprzez podanie przez ucznia nazwiska i numeru umowy. NSA zauważył, że choć pierwotnie regulamin stołówki przewidywał pierwszeństwo dla dzieci z identyfikacją biometryczną w dostępie do stołówki, to po zmianie regulaminu przez Szkołę w praktyce

²⁴ Wyrok TSUE (Wielka Izba) z dnia 24 września 2019 r. w sprawie C-136/17, GC i in. przeciwko CNIL, EU:C:2019:773, pkt 64.

²⁵ Europejska Rada Ochrony Danych, *Wytyczne 8/2020 dotyczące targetowania użytkowników mediów społecznościowych*, 35, https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_o82020_on_the_targeting_of_social_media_users_pl_o.pdf [dostęp: 12.04.2025].

²⁶ Roßnagel i Richter, „Article 5,” 273.

wszystkie dzieci ustawiały się w jednej kolejce. Zdaniem autora taka ocena NSA może budzić wątpliwości, ponieważ niedostatecznie uwzględnia ona znaczenie kontekstu, w którym Szkoła uzyskała zgodę osób działających w imieniu podmiotów danych. Zgodnie z motywem 43 RODO oświadczenie woli osoby fizycznej nie stanowi ważnej zgody w rozumieniu rozporządzenia, gdy ma miejsce wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem danych. Przyjmuje się, że taki „brak równowagi sił” ma miejsce, gdy podmiot danych jest pozbawiony możliwości dokonania rzeczywistego wyboru (wyrażenia albo niewyrażenia zgody) ze względu na istnienie przymusu, presji lub braku możliwości swobodnego okazania woli^[27]. Oznacza to, że przy ocenie dobrowolności zgody, udzielonej zwłaszcza na przetwarzanie szczególnych kategorii danych^[28], należy uwzględniać nie tylko istnienie samej możliwości dokonania wyboru przez osobę, której dane dotyczą, lecz również charakter relacji pomiędzy nią a administratorem, w tym całokształt okoliczności, w których uzyskiwana jest jej zgoda^[29]. NSA w swojej wykładni wydaje się pomijać, że nieodłącznym elementem działania szkół jest podległość ucznia wobec nich. Znacząca rola instytucji edukacyjnych w kształtowaniu życia dziecka może powodować, że opiekunowie prawni wyrażający zgodę na przetwarzanie danych dzieci w związku z codziennym funkcjonowaniem szkoły nie będą mieli rzeczywistej alternatywy wobec zaakceptowania warunków zaproponowanych przez placówkę oświatową^[30]. Dzieje się tak z obawy przed wykluczeniem dziecka z grupy rówieśniczej lub jego stygmatyzacją przez władze szkoły. Nie można podzielić stanowiska składu orzekającego, że sam fakt ustawiania się uczniów w jednej kolejce do stołówki, niezależnie

²⁷ EROD, *Wytyczne 05/2020*, 8 – 10.

²⁸ Ze względu na wysoce osobisty charakter szczególnych kategorii danych z art. 9 ust. 1 RODO oraz ich znaczenie dla praw i wolności osoby, której dane dotyczą, należy przyjąć bardzo rygorystyczne kryteria dla oceny spełnienia warunku „dobrowolności” zgody wyrażanej na przetwarzanie danych biometrycznych – podobnie Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, *Positionspapier zur biometrischen Analyse*, 28, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_positionspapier_biometrie.pdf [dostęp: 12.04.2025].

²⁹ Judith Rauhofer i Burkhard Schafer, „Article 4(11). Consent,” w *General Data Protection Regulation Article-by-Article Commentary*, red. Indra Spiecker gen. Döhmman et al. (Baden-Baden: Nomos, 2023), 204 – 205.

³⁰ Datatilsynet (obecnie Integritetsskyddsmyndigheten), *Decyzja z dnia 20 sierpnia 2019 r., nr DI-2019-2221*, 4, <https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf> [dostęp: 12.04.2025].

od sposobu weryfikacji opłacenia posiłku (skanowanie odcisku palca przy pomocy czytnika biometrycznego albo uwierzytelnianie tożsamości ucznia w systemie poprzez imię, nazwisko i numer umowy), jest wystarczającą przesłanką dla wykluczenia zaistnienia negatywnych konsekwencji dla uczniów, których opiekunowie prawni nie wyrazili zgody na przetwarzanie danych biometrycznych lub zgodę tę wycofali. NSA zbyt pochopnie i bez pogłębionej refleksji odrzucił argumentację skarżącego kasacyjnie organu, według której wydłużona weryfikacja tożsamości dziecka w systemie za pomocą imienia, nazwiska i numeru umowy negatywnie wpływa na ocenę „dobrowolności” zgody w rozumieniu RODO. Wydłużony proces wchodzenia na stołówkę szkolną stanowi negatywną konsekwencję dla dzieci, których opiekunowie prawni nie wyrazili zgody na przetwarzanie ich danych biometrycznych, ponieważ naraża je na nierówne traktowanie i potencjalne wykluczenie przez szkolną społeczność. Dzieci te muszą bowiem spędzać więcej czasu na „ręcznej” weryfikacji swojej tożsamości z wykorzystaniem tzw. „danych zwykłych”, co może prowadzić do stresu, dyskomfortu oraz poczucia odmienności od rówieśników, którzy szybciej potwierdzają uiszczenie opłaty za wydany posiłek przy pomocy skanu odcisku palca.

Uwzględniając zatem kontekst zbierania zgód na przetwarzanie danych biometrycznych dzieci, należy uznać, że dłuższy okres weryfikacji opłacenia posiłku w danym dniu i związane z tym opóźnienie w świadczeniu usługi stanowią negatywną konsekwencję dla dzieci, których opiekunowie prawni nie wyrazili zgody na przetwarzanie ich danych biometrycznych³¹. Dla zapewnienia równego traktowania uczniów Szkoła powinna była zaoferować im równoważny, alternatywny wobec czytnika linii papilarnych sposób uwierzytelniania, umożliwiający porównywalnie szybkie

³¹ Prezes UODO nie jest jedynym organem nadzorczym z zakresu ochrony danych, który podnosi, że okoliczność dłuższego czekania w kolejce do stołówki szkolnej przez dzieci, których uprawnienie do otrzymania posiłku jest weryfikowane przy pomocy środków uwierzytelniania niewykorzystujących biometrię, stanowi niekorzystną konsekwencję dla dzieci. W ocenie francuskiego organu ochrony danych sytuacja, w której uczniowie korzystający z tradycyjnych metod uwierzytelniania, niewykorzystujących biometrii, muszą czekać dłużej na możliwość skorzystania z posiłków w stołówce szkolnej niż dzieci korzystające z weryfikacji biometrycznej, stanowi negatywną konsekwencję dla podmiotu danych, która powoduje niespełnienie zasady „dobrowolności zgody” w rozumieniu RODO – zob. Commission nationale de l’informatique et des libertés (CNIL), Les dispositifs biométriques pour l’accès aux cantines scolaires, <https://www.cnil.fr/fr/les-dispositifs-biometriques-pour-lacces-aux-cantines-scolaires> [dostęp: 12.04.2025].

potwierdzenie uprawnienia do korzystania ze stołówki, np. karty zbliżeniowe^[32], breloki, opaski, kody QR wyświetlane w aplikacji mobilnej. Stanie przez uczniów w jednej kolejce do stołówki niezależnie od wybranego sposobu weryfikacji płatności za posiłek nie jest wystarczające do uznania zgody za „dobrowolnie” wyrażoną w rozumieniu RODO, ponieważ nie niweluje faktycznych różnic w sposobie i czasie obsługi poszczególnych uczniów. Zasadniczym zagadnieniem nie jest układ kolejki do szkolnej stołówki, lecz to, że dzieci korzystające z metod uwierzytelniania opartych o wiedzę (imię, nazwisko i numer umowy) muszą poświęcić więcej czasu na potwierdzenie opłacenia posiłku w porównaniu do uczniów, których dane biometryczne są przetwarzane. Ta różnica w czasie obsługi powoduje nierówność i potencjalne negatywne konsekwencje, w szczególności dyskomfort czy poczucie gorszego traktowania. Ustawienie uczniów w jednej kolejce jest tylko pozorną formą równego traktowania, która nie rozwiązuje problemu podziałów wśród dzieci wynikających z różnic w szybkości i łatwości korzystania ze szkolnej stołówki.

Osobnego komentarza, wykraczającego poza ścisłą ocenę wyroku, wymaga posługiwanie się w analizowanej sprawie zarówno przez NSA, WSA w Warszawie, jak również Prezesa UODO pojęciem „identyfikacji biometrycznej” w odniesieniu do przetwarzania danych biometrycznych dzieci przez Szkołę w związku z korzystaniem ze szkolnej stołówki. Używanie tego terminu w kontekście stanu faktycznego, w jakim została wydana decyzja skarżącego kasacyjnie organu, należy bowiem uznać za nieprawidłowe. Identyfikacja biometryczna jest operacją polegającą na ustaleniu tożsamości osoby fizycznej poprzez porównanie jej danych biometrycznych ze wszystkimi wzorcami biometrycznymi przechowywanymi w bazie danych podczas procesu kojarzenia zarejestrowanych szablonów „jeden do wielu”^[33]. Tymczasem celem przetwarzania danych biometrycznych uczniów (przekształconych we wzorce biometryczne odcisków palców) przez Szkołę było ustalenie, czy konkretne dziecko uiściło opłatę za posiłek wydany w danym dniu i mogło korzystać ze szkolnej stołówki. Takie wykorzystanie danych należy zatem uznać za „weryfikację biometryczną”,

³² Podobnie Grupa Robocza Art. 29, *Opinia nr 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół)*, 16, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [dostęp: 1.04.2025]; CNIL, *Les dispositifs biométriques* [dostęp: 12.04.2025].

³³ Grupa Robocza Art. 29, *Opinia nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych*, 6, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [dostęp: 12.04.2025].

tj. proces porównywania danych biometrycznych danej osoby fizycznej (uzyskanych w czasie weryfikacji) z pojedynczym wzorcem biometrycznym przechowywanym w referencyjnej bazie danych jedynie w celu potwierdzenia, że dana osoba fizyczna jest osobą, za którą się podaje, i jest uprawniona do uzyskania dostępu do określonych zasobów lub usług^[34].

Podsumowując, stanowisko NSA wyrażone w komentowanym orzeczeniu należy ocenić krytycznie, ponieważ jest sprzeczne z podstawowymi założeniami i celami prawa ochrony danych osobowych. Uzasadnienie wyroku, że przetwarzanie danych biometrycznych uczniów w stanie faktycznym sprawy było obiektywnie proporcjonalne do realizacji celu przetwarzania danych (weryfikacja uiszczenia opłaty za posiłek w szkolnej stołówce), należy uznać za nieprzekonujące. Przyjęta przez NSA interpretacja relacji zgody podmiotu danych i zasad przetwarzania z art. 5 RODO jest sprzeczna z wykładnią systemową rozporządzenia. Niezrozumiała jest też formułowana w uzasadnieniu wyroku analogia pomiędzy zgodą na przetwarzanie danych a przesłanką oczywistego upublicznienia informacji należących do szczególnych kategorii danych z art. 9 ust. 2 lit. e RODO. Podobnie negatywnie należy ocenić wnioski NSA co do spełnienia warunku „dobrowolności” zgody udzielanej przez opiekunów prawnych uczniów na przetwarzanie ich danych biometrycznych. Wprowadzanie weryfikacji biometrycznej do codziennych, rutynowych czynności w instytucjach edukacyjnych, takich jak potwierdzenie dokonania opłaty za posiłek w szkolnej stołówce, może sprawić, że dzieci zaczną postrzegać techniki nadzoru oparte na wykorzystywaniu ich unikalnych cech fizycznych lub behawioralnych jako coś zwyczajnego i niewzbudzającego kontrowersji. W dłuższej perspektywie taka praktyka może sprzyjać przyzwyczajeniu się dzieci do funkcjonowania w środowisku, które normalizuje – motywowane wygodą – ujawnianie wysoce osobistych kategorii danych, prowadząc w ich dorosłym życiu do stopniowego zubożenięcia wobec ochrony prywatności, a nawet do utrwalenia przekonania o dopuszczalności zewnętrznej ingerencji w autonomię informacyjną jednostki.

³⁴ Ibidem. Uzupełniając należy dodać, że pojęcia „identyfikacja biometryczna” oraz „weryfikacja biometryczna” posiadają obecnie definicje legalne określone odpowiednio w art. 3 pkt 35 i 36 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (Dz.U. UE.L. z 2024 r., poz. 1689).

Bibliografia

- Finck, Michèle i Asja Biega. "Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems." *Technology and Regulation*, nr 1 (2021): 44 – 61. <https://doi.org/10.26116/techreg.2021.004>.
- Frenzel, Eike Michael. "Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten." W *Datenschutzgrundverordnung. Bundesdatenschutzgesetz*, red. Boris Paal i Daniel Pauly. München: C.H. Beck, 2021.
- Gayrel, Claire. "The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL's Deliberations." *Computer Law & Security Review* 32, nr 3 (2016): 455 – 464. <https://doi.org/10.1016/j.clsr.2016.01.013>.
- Lubasz, Dominik. "5. Przesłanki legalizacyjne przetwarzania danych osobowych." W *Meritum. Ochrona danych osobowych*, red. Dominik Lubasz, 119 – 142. Warszawa: Wolters Kluwer, 2022.
- Mednis, Arwid. "Wykorzystanie danych biometrycznych w szkole. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20." *Gdańskie Studia Prawnicze*, nr 4 (2021): 129 – 137. <https://doi.org/10.26881/gsp.2021.4.08>.
- Rauhofer, Judith i Burkhard Schafer. "Article 4(11). Consent." W *General Data Protection Regulation Article-by-Article Commentary*, red. Indra Spiecker gen. Döhmman, Vagelis Papakonstantinou, Gerrit Hornung i Paul De Hert, 195 – 216. Baden-Baden: Nomos, 2023.
- Roßnagel, Alexander i Philipp Richter. "Article 5. Principles Relating to Processing of Personal Data." W *General Data Protection Regulation Article-by-Article Commentary*, red. Indra Spiecker gen. Döhmman, Vagelis Papakonstantinou, Gerrit Hornung i Paul De Hert. Baden-Baden: Nomos, 2023.
- Sartor, Giovanni. "Article 6. Lawfulness of Processing." W *General Data Protection Regulation Article-by-Article Commentary*, red. Indra Spiecker gen. Döhmman, Vagelis Papakonstantinou, Gerrit Hornung i Paul De Hert, 291 – 328. Baden-Baden: Nomos, 2023.
- Wendehorst, Christiane i Yannik Duller. *Biometric Recognition and Behavioural Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on Their Current and Future Use in Public Spaces*. Brussels: European Parliament, 2021. [https://www.europarl.europa.eu/think-tank/en/document/IPOL_STU\(2021\)696968](https://www.europarl.europa.eu/think-tank/en/document/IPOL_STU(2021)696968).



