ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4147
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXII
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.132.8

KRZYSZTOF WYGODA
ORCID: 0000-0002-0997-5512
Uniwersytet Wrocławski

DOPUSZCZALNOŚĆ PRZETWARZANIA DANYCH BIOMETRYCZNYCH PRZEZ PRACODAWCÓW — UJĘCIE MODELOWE I PRAKTYCZNE

Abstrakt: Artykuł jest próbą wskazania rozwiązań, które powinny być stosowane w ramach podejmowania przez pracodawców decyzji o przetwarzaniu danych biometrycznych. Łączenie przetwarzania danych biometrycznych z prowadzeniem monitoringu jest, na gruncie rozwiązań wynikających z RODO i prawa krajowego, niezwykle skomplikowane. Spełnienie wszystkich warunków koniecznych do legalizacji takiego procesu przetwarzania danych jest, przynajmniej co do zasady, możliwe jedynie w bardzo ograniczonej liczbie przypadków i każdorazowo wymaga indywidualnej analizy dopuszczalności. W orzecznictwie sądowym od niedawna podejmuje się próby reinterpretacji wcześniejszego, niezwykle restrykcyjnego podejścia do przetwarzania danych biometrycznych.

Słowa kluczowe: dane osobowe, dane biometryczne, minimalizacja danych

UWAGI WPROWADZAJĄCE

Nie ulega wątpliwości, że każdy pracodawca, który przetwarza dane osobowe pracowników musi dostosować się nie tylko do wymogów płynących z kodeksu pracy[1] i innych norm prawa krajowego, ale również do standardów działania wynikających bezpośrednio z RODO[2].

Kolejnym aksjomatem jest uznanie pracodawcy za administratora w rozumieniu RODO — co nakłada na niego szereg obowiązków przypisanych mu w tym akcie, związanych z właściwym przygotowaniem i realizacją procesów przetwarzania danych osobowych.

[1] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. Dz.U. z 2022 r. poz. 1510, 1700) — dalej k.p.

[2] 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).

Ostatnią uwagą, którą poczynić należy na wstępie, jest podkreślenie ograniczonej przydatności zgody[3] jako podstawy legalizacji procesów przetwarzania danych osobowych mających miejsce w ramach relacji pracodawca–pracownik. Zarówno doktryna, jak i orzecznictwo podkreślają

> brak równowagi sił pomiędzy pracodawcą a jego pracownikami, pracownicy mogą wyrazić dobrowolną zgodę wyłącznie w wyjątkowych okolicznościach, w których fakt wyrażenia lub niewyrażenia przez nich zgody nie pociąga za sobą żadnych negatywnych konsekwencji. Przymiot dobrowolności zakłada bowiem rzeczywistą możliwość dokonania wyboru przez osoby, których dane dotyczą, oraz sprawowania przez nie kontroli[4]

nad procesem, choćby poprzez możliwość jego zastopowania z uwagi na swobodę cofnięcia zgody w dowolnym momencie jego realizacji.

1. POJĘCIE DANYCH BIOMETRYCZNYCH

Zawarta w art. 4 pkt 14 RODO definicja danych biometrycznych wskazuje, że status ten uzyskają tylko takie informacje o pracowniku, które łącznie spełniają wskazane w tym przepisie warunki. Muszą być zatem takimi danymi osobowymi, które odnoszą się do określonych cech (fizycznych, fizjologicznych lub behawioralnych osoby fizycznej), na podstawie których, przy użyciu specjalnych metod technicznych, jest możliwa jednoznaczna identyfikacja osoby fizycznej lub potwierdzenie jej tożsamość. Użycie zwrotu „takie jak", poprzedzające wskazane w przepisie przykłady owych cech, jednoznacznie potwierdza, że nie mogą być one traktowane enumeratywnie, a jedynie jako najbardziej typowe czy najczęściej występujące (przynajmniej w ocenie prawodawcy). Pracodawca powinien zatem uznać, że cechy fizyczne i fizjologiczne, które będą umożliwiały identyfikację pracowników obejmować mogą na przykład linie papilarne, wygląd siatkówki lub tęczówki oka, twarzy, kształt małżowiny usznej, geometrię ręki, układ naczyń krwionośnych dłoni, głos i jego barwę. Z kolei cechy behawioralne to między innymi charakter pisma, dynamika pisania, sposób poruszania się, dialekt czy nawyki pracownika (również te odnoszące się do wykonywania zlecanych mu czynności)[5].

---

[3] Szerzej zob. np. M. Mazewski, *Prawo do wyrażenia i wycofania zgody na przetwarzanie danych*, [w:] *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017, s. 45–69.

[4] D. Dörre-Kolasa, *Pozyskiwanie danych osobowych osoby ubiegającej się o zatrudnienie i pracownika na podstawie przepisów KP*, [w:] *Ochrona danych osobowych w zatrudnieniu*, red. D. Dörre-Kolasa, Warszawa 2020, s. 81. Szerzej na ten temat zarówno we wskazanym opracowaniu, jak również A. Nerka, *Komentarz do art. 7*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 170–174.

[5] Zob. *Opinia 4/2017 w sprawie pojęcia danych osobowych, WP 136*, s. 13, European Commission, 20.06.2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf (dostęp: 3.01.2023).

Samo utrwalenie tego typu informacji (co w przypadku ich niektórych kategorii może mieć miejsce dość często — na przykład w związku z monitoringiem wizyjnym czy nagrywaniem rozmów) nie stanowi jednak problemu z punktu widzenia zakazu ich przetwarzania wynikającego z art. 9 RODO. Dzieje się tak, gdyż koniecznym składnikiem uznania, że mamy do czynienia z przetwarzaniem danych biometrycznych jest ich przetworzenie specjalnymi metodami technicznymi, pozwalającymi (co do zasady) na ich używanie w zautomatyzowanych systemach identyfikacyjnych (w przypadku cech behawioralnych, zamiast „prostego" mechanicznego porównania cech mogą być stosowane systemy oparte o sztuczną inteligencję, a co najmniej o samouczące się sieci neuronowe). To właśnie owo techniczne podejście do przetwarzania sprawia, że pojawiają się dane biometryczne, mimo że *de facto* dość często nie dochodzi do bezpośredniego utrwalenia samych cech czy ich pełnego obrazu, a jedynie do stworzenia czegoś w rodzaju cyfrowego wzorca porównawczego (na przykład cyfrowej mapy charakterystycznych punktów pojawiających się w liniach papilarnych czy wzorze siatkówki), który następnie służy jako profil używany przez system identyfikacji do wskazywania najlepszego dopasowania danych pojawiających się w czytniku kontrolnym z utrwalonym szablonem cech konkretnego pracownika. Można bez ryzyka pomyłki stwierdzić, że użycie metod technicznych do utrwalenia obrazu czy systemowego zapisu innych parametrów rzeczywistości, obejmujące utrwalenie pewnych cech osoby fizycznej, samo w sobie nie stanowi przetwarzania danych biometrycznych. Odnosząc się do założeń definicyjnych byłoby jedynie swego rodzaju zwykłym czy też standardowym przetwarzaniem technicznym, podczas gdy z art. 4 pkt 14 RODO wypływa konieczność podjęcia czynności mieszczących się w pojęciu „specjalnego przetwarzania technicznego" danych, które w pewnym uproszczeniu można utożsamić z dokonaniem stosownych pomiarów pozwalających na tworzenie wzorców czy profili służących do umożliwienia lub potwierdzenia jednoznacznej identyfikacji osoby fizycznej[6]. Przy czym bez realnego (lub choćby planowanego w późniejszym czasie) dokonywania owego specyficznego przetransponowania danych do postaci wzorców, służących następnie do dokonywania lub potwierdzania jednoznacznej identyfikacji, trudno mówić o przetwarzaniu danych biometrycznych. Zatem działanie monitoringu wizyjnego (nawet tego o wysokiej rozdzielczości) nie implikuje *per se* przetwarzania danych biometrycznych odnoszących się do wyglądu pracowników czy innych możliwych do zidentyfikowania przez administratora (pracodawcę) osób fizycznych. Dopiero użycie (lub co najmniej planowanie takiego wykorzystania) oprogramowania służącego do identyfikacji osób, które „wzbogaci" model i prawdopodobnie cel użу-

[6] Na te aspekty związane z wyjaśnieniem pojęcia danych biometrycznych zwraca również uwagę J. Rzymowski, *RODO — GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*, Łódź 2020, s. 541–552.

cia systemu monitorującego, da podstawę do stwierdzenia, że mamy do czynienia z przetwarzaniem danych biometrycznych w ramach monitoringu.

Systemy zapewniające zautomatyzowaną identyfikację powinny charakteryzować się jej wysoką skutecznością i być odporne na:

— możliwości pominięcia dokonania weryfikacji tożsamości (na przykład poprzez ominięcie bramki czy brak prawidłowego odczytu cech przez czytnik o zbyt niskiej czułości);

— występowanie nieprawidłowego rozpoznania konkretnej osoby lub brak jej rozpoznania (choćby z uwagi zbyt małą elastyczność sytemu, który w przypadku najmniejszej niezgodności z wzorcem wskazuje na brak identyfikacji, lub przeciwnie — w przypadku pokrycia się jedynie części cech dokonuje identyfikacji);

— niemożności sprawdzenia niektórych osób (choćby ze względów religijnych — zakrycie twarzy, czy zbyt słabą widoczność linii papilarnych).

Wszystko to sprawia, że procesy uwzględniające przetwarzanie danych biometrycznych wymagają uprzedniego przygotowania, co pozwala na pełne zastosowanie zasad wynikających ze stosowania art. 25 RODO i uwzględnienia zasad ochrony danych już na etapie ich projektowania, a następnie bieżącą kontrolę wdrożonego systemu w działaniu.

2. DANE BIOMETRYCZNE A MONITORING

Nie wchodząc w niuanse regulacji k.p. dotyczących możliwości stosowania monitoringu przez pracodawców[7], należy przyjąć dopuszczalność korzystania z tej formy przetwarzania danych osobowych. Oczywiście każdorazowe użycie monitoringu wizyjnego czy innych jego form wymaga uprzedniego przygotowania i spełnienia szeregu warunków wynikających zarówno z RODO, jak i k.p. (art. 22^2–22^3 k.p.). Pracodawca, chcąc realizować swoje uprawnienia z tym związane, musi niejednokrotnie porzucić założenie jego szerokiego stosowania, gdyż nie zawsze da się to wystarczająco uzasadnić zarówno w kontekście celowości, jak i niezbędności przetwarzania. Należy bowiem pamiętać, że z uwagi na znaczącą ingerencję w prawa osób monitorowanych (zwłaszcza w prywatność) jego stosowanie (zarówno w formie monitoringu wizyjnego, jak i występującego w innej postaci) co do zasady nie jest uzasadnione nadrzędnym interesem administratora, szczególnie jeżeli cel jego zainstalowania nie jest wystarczająco konkretny. W przypadku pracodawców jest to dodatkowo limitowane wskazaniami wynikającymi z art. 22^2 § 1 i 22^3 § 1 k.p, które przedmiotowo zawężają zakres celów

[7] Na temat warunków i zasad stosowania monitoringu zob. np.: D. Dörre-Kolasa, *Monitoring,* [w:] *Ochrona danych w zatrudnieniu*, s. 169–204; J. Wezgraj, *Monitoring wizyjny a ochrona danych osobowych. Wymagania rodo, przepisy sektorowe oraz wytyczne UODO*, Wrocław 2019; D. Dörre-Kolasa, *Ochrona danych osobowych pracowników*, [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2022, s. 827–858.

uzasadniających wprowadzenie monitoringu. Powstaje więc pytanie, czy z uwagi na zakaz przetwarzania danych osobowych szczególnych kategorii włączenie w proces monitoringu przetwarzania danych biometrycznych jest w ogóle możliwe, a jeśli tak, to jaka przesłanka legalizująca takie działanie może być brana pod uwagę przez pracodawców.

Pozytywna odpowiedź na tak postawione pytania, przy uwzględnieniu uwarunkowań działalności pracodawców wynikających z niewątpliwego zawężania dopuszczalnego zakresu przetwarzanych przez nich kategorii danych pracowniczych, wynikającego z kolei z samego k.p., wydaje się dość mało prawdopodobna, nie można jej jednak całkowicie wykluczyć. Zwłaszcza w jednostkowych przypadkach pracodawców (administratorów), których specyfika działalności (wymagająca szczególnej dbałości o ograniczenia dostępu do określonych obszarów, zasobów czy informacji) może teoretycznie uzasadniać sięganie po dane biometryczne jako informacje wspierające kontrolę dostępu (w aspekcie uzyskiwania wysokiego stopnia pewności co do tożsamości, a zatem i posiadanych uprawnień przez konkretnych pracowników).

Prowadząc analizę we wskazanym wyżej kontekście, należy jeszcze raz podkreślić, że wprowadzenie monitoringu przez pracodawcę wymaga, by dostosował się on do rozwiązań wynikających z k.p. Co prowadzi do wniosku, że pracodawca musi ograniczyć się nie tylko do katalogu celów uzasadniających wprowadzenie monitoringu w prawie pracy, ale również skorelować to z celami wynikającymi pośrednio z art. 9 ust. 2 RODO — tam bowiem zawarte zostały wskazania pozwalające ograniczyć działanie zakazu przetwarzania danych biometrycznych[8]. Należy dodatkowo podkreślić, że w sytuacji korzystania z rozwiązań obejmujących użycie danych biometrycznych pojawi się dodatkowy problem kwalifikacji prawnej stosowanego monitoringu.

W przypadku wprowadzenia warstwy biometrycznej do działania systemów rejestrujących obrazy trudno będzie uznać ową hybrydę za zwykły monitoring

[8] Spośród wielu przesłanek uchylających zakaz przetwarzania tych danych, ujętych w art. 9 ust. 2 RODO, w omawianym kontekście największe możliwości dają pracodawcom cztery: „a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą; […] f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy; g) 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”.

wizyjny (nawet jeśli rozpoznawanie cech biometrycznych i identyfikacja osoby będzie oparta wyłącznie na obrazie rejestrowanym przez kamery). Z kolei użycie specjalistycznych czytników rejestrujących/odczytujących cechy biometryczne już jednoznacznie przenosi nas do „innych form monitoringu" — co teoretycznie może dodatkowo zawężać swobodę wyboru celu dla tego typu procesu przetwarzania danych. Należy jednak zaznaczyć, że tylko szczegółowa analiza konkretnego przypadku pozwoliłaby na rozstrzygnięcie, czy mamy do czynienia z odrębnymi procesami przetwarzania danych (monitoringiem i przetwarzaniem danych biometrycznych), czy z jednym procesem bazującym na przetwarzaniu danych zwykłych i szczególnych kategorii.

Reasumując: pracodawca, który zamierza wprowadzić tego rodzaju rozwiązanie, musi bardzo ostrożnie definiować rzeczywisty cel przetwarzania — nie naruszając wiążących go norm k.p. dotyczących możliwości wdrożenia szczególnych form monitoringu (zarówno w przypadku rozszerzonego o warstwę biometryczną monitoringu wizyjnego, jak i stosowania specjalnych czujników i czytników w celach monitorowania pracowników), lub starać się odrębnie zdefiniować równoległe procesy monitorowania i przetwarzania danych biometrycznych. Przy czym z uwagi na fakt, że przetwarzane mają być dane z kategorii szczególnych, warto zbadać, czy tych samych celów nie można osiągnąć w inny — mniej ingerujący w prywatność — sposób, przy którym nie będzie konieczne przetwarzanie danych biometrycznych. Przeprowadzenie oceny ryzyka bądź analizy konieczności przetwarzania tej szczególnej kategorii danych warto oprzeć (o ile to oczywiście możliwe) na dotychczasowych działaniach podejmowanych przez administratora. W przypadku wykazania, że wcześniej stosowane środki nie gwarantowały odpowiednio wysokiego poziomu realizacji założonego celu przetwarzania, sięgnięcie po dane biometryczne może okazać się dopuszczalne (o ile sam proces uda się to odpowiednio „zalegalizować") zarówno z punktu widzenia zasady celowości, jak i minimalizacji.

3. UŻYCIE DANYCH BIOMETRYCZNYCH — WĄTPLIWOŚCI WYNIKAJĄCE Z ORZECZNICTWA

Jak wskazano wyżej, samo wprowadzenie przez pracodawcę monitoringu nie wydaje się być szczególnie trudne — choć bez wątpienia wymaga spełnienia kilku warunków formalnych i materialnych, które definiowane są zarówno w RODO, jak i bezpośrednio w k.p. Warunki owe odnoszą się jednak nie tylko do uzyskania podstawy legalizującej proces przetwarzania (spośród wskazanych w art. 6 i 9 RODO — odrębnie dla danych zwykłych i uzupełniająco do danych szczególnych kategorii), ale również realizacji procesu w zgodzie

z zasadami ustanowionymi w art. 5 ust. 1 RODO, które — co należy wyraźnie podkreślić — odgrywają szczególną rolę wśród norm prawnych dotyczących ochrony danych osobowych zawar-

tych w RODO. Przyjmuje się bowiem, że zasady te nie są jedynie postulatami odczytywanymi z całokształtu przepisów o ochronie danych osobowych, ale mają wręcz charakter normatywny — są wiążącymi normami prawa, wyznaczającymi określony sposób postępowania, mając szczególne znaczenie dla stosowania i interpretacji przepisów o ochronie danych osobowych[9].

To właśnie te reguły postrzegane są jako główna przeszkoda we wdrożeniu przetwarzania danych biometrycznych przez pracodawcę (tym bardziej, jeśli ma to być powiązane z monitoringiem). Wiąże się to z ustaleniami, które poczyniono na kanwie wcześniej obowiązujących przepisów dotyczących ochrony danych osobowych.

Zarówno dyrektywa 95/46/WE[10], jak i ustawa o ochronie danych osobowych z 1997 roku[11] zawierały podobne (choć, co należy podkreślić, nietożsame) rozwiązania prawne, ale orzecznictwo pochodzące z tamtego okresu do dziś traktowane jest jako znacząca wskazówka służąca ocenie dopuszczalności przetwarzania danych biometrycznych. Dotyczy to w szczególności wyroku NSA z 1 grudnia 2009 roku[12], którego główne tezy wskazują, że:

— ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności (wyrażona w art. 26 ust. 1 pkt 3 uodo97) jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania;

— uznanie faktu wyrażenia przez pracownika zgody na przetwarzanie jego danych (na gruncie art. 23 uodo97) za okoliczność legalizującą pobranie od pracownika innych danych niż wskazane w art. 22^1 k.p. stanowiłoby naruszenie tegoż przepisu, gdyż powoduje jego obejście. Sama wyrażona na prośbę pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych, narusza prawa pracownika i swobodę wyrażenia przez niego woli;

— wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania (w rozumieniu art. 26 ust. 1 pkt 3 uodo97).

Takie podejście powinno jednak zostać (przynajmniej częściowo) zrewidowane w związku z przeformułowaniem zasad przetwarzania wyrażonych w art. 5

[9] Wyrok WSA w warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20, CBOSA (dostęp: 3.01.2023); z powołaniem na P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

[10] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, 23.11.1995, OJ 281/31, dalej: dyrektywa 95/46/WE.

[11] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2016 r. poz. 922. ze zm. — dalej: uodo97).

[12] Wyrok NSA z dnia 1 grudnia 2009 r., I OSK 249/09, CBOSA (dostęp 3.01.2023).

RODO — a zwłaszcza zasady „minimalizacji danych”[13]. Obowiązek jej stosowania bez wątpienia dotyczy administratora. Jak słusznie zauważa Arwid Mednis, jest on

niezależny od legitymowania się przesłanką legalności przetwarzania danych. Dotyczy to również przetwarzania danych osobowych na podstawie zgody. Innymi słowy, administrator przetwarzający dane na podstawie pozyskanej zgody jest nadal zobowiązany do przestrzegania zasady minimalizacji danych. Nie ulega również wątpliwości, że zasada ta, podobnie jak pozostałe wymienione w art. 5 RODO, ma charakter normatywny i jest samoistnym obowiązkiem nałożonym na administratora[14].

Należy podkreślić, że termin „minimalizacja danych” stanowi skrótowe (zaproponowane przez samego prawodawcę unijnego) określenie zasady w myśl której dane osobowe używane w procesie przetwarzania muszą być „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane” (art. 5 ust. 1 lit. c RODO). Warto przy tym odnotować stanowisko WSA w Warszawie, który wskazuje, że

określenie „adekwatne” oznacza „odpowiednie, zgodne, proporcjonalne, nienadmierne” i może być traktowane jako synonim słowa „stosowne”. Adekwatność i stosowność rozumieć można jako konieczność zachowania odpowiednich proporcji zakresu danych do celów przetwarzania i przetwarzanie tylko takich danych, które są potrzebne dla realizacji określonych celów. […]

Niemniej jednak, co trzeba wyraźnie podkreślić, odczytywanie z analizowanego przepisu normy nakazującej ograniczenie danych jedynie do niezbędnego minimum i przetwarzanie tylko takich danych, bez których nie da się osiągnąć celu […], uznać należy za interpretacją zbyt daleko idącą. […]

Zdaniem Sądu, wymóg niezbędności należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania[15].

Takie podejście pozwala nieco odejść od literalnego traktowania wymogów adekwatności i minimalizacji — w którym adekwatność sprowadza się do oceny przydatności (nieodzowności) występowania określonego rodzaju danych na drodze realizacji celu założonego w procesie przetwarzania, natomiast minimalizacja prowadzi do uznania, że jeśli taki założony cel można osiągnąć bez przetwarzania określonego rodzaju danych, to nie należy takich danych przetwarzać. W tym miejscu warto powołać się na podsumowanie dokonane przez A. Mednisa (którego dokonał na kanwie glosowanego orzeczenia II SA/Wa 809/20) wskazujące, że:

sąd przyznaje w uzasadnieniu, że wymogi minimalizacji i adekwatności nie są ze sobą spójne, a ich spełnienie należy oceniać łącznie, co w konsekwencji oznacza, że „nie powinno się przyznawać prymatu minimalizacji kosztem adekwatności”. Jednocześnie podkreśla, jak ważne są okoliczności konkretnej sprawy […]. Słusznie sąd odrzuca sugestię PUODO, że dane biometryczne mogą być

[13] Szerzej na temat zasady minimalizacji poza wskazanymi już publikacjami komentarzowymi zob. P. Drobek, *Komentarz do art. 5*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz ,Warszawa 2018, s. 322–344.

[14] A. 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” 25, 2021, nr 4 (52), s. 134.

[15] Wyrok WSA w Warszawie z 7 sierpnia 2020 r., II SA/Wa 809/20, CBOSA (dostęp: 3.01.2023).

wykorzystywane tylko wyjątkowo, i to w takich celach, jak np. bezpieczeństwo osobowe, przemysłowe czy ochrona informacji itp. Takie ograniczenie znikąd bowiem nie wynika. Oczywiste jest, że sięganie po dane biometryczne jest daleko idącą ingerencją w sferę prywatności, niemniej nie oznacza to, że […] ich użycie będzie niedopuszczalne niezależnie od okoliczności. Słusznie zatem sąd, biorąc pod uwagę okoliczności sprawy, dopuścił możliwość weryfikacji biometrycznej[16].

ADMISSIBILITY OF BIOMETRIC DATA PROCESSING BY EMPLOYERS: MODEL AND PRACTICAL APPROACH

Summary

The article is an attempt to indicate solutions that should be used as part of employers' decisions on the processing of biometric data. Combining the processing of biometric data with monitoring is, on the basis of the solutions resulting from the GDPR and national law, extremely complicated. Meeting all the conditions necessary to legalize such a data processing process is, at least in principle, possible only in a very limited number of cases and each time requires an individual admissibility analysis. In judicial decisions, attempts have been made recently to reinterpret the previously extremely restrictive approach to the processing of biometric data.

Keywords: personal data, biometric data, data minimization

BIBLIOGRAFIA

Dörre-Kolasa D., *Ochrona danych osobowych pracowników*, [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2022.

Dörre-Kolasa D., *Pozyskiwanie danych osobowych osoby ubiegającej się o zatrudnienie i pracownika na podstawie przepisów KP*, [w:] *Ochrona danych osobowych w zatrudnieniu*, red. D. Dörre-Kolasa, Warszawa 2020.

Drobek D., *Komentarz do art. 5*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz Warszawa 2018.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Mazewski M., *Prawo do wyrażenia i wycofania zgody na przetwarzanie danych*, [w:] *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, red. B. Fischer, M. Sakowska-Baryła, Wrocław 2017.

Mednis A., *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" 25, 2021, nr 4 (52).

Nerka A., *Komentarz do art. 7*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.

Opinia 4/2017 w sprawie pojęcia danych osobowych, WP 136, European Commission, 20.06.2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf.

Rzymowski J., *RODO — GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*, Łódź 2020.

Wezgraj J., *Monitoring wizyjny a ochrona danych osobowych. Wymagania rodo, przepisy sektorowe oraz wytyczne UODO*, Wrocław 2019.

[16] A. Mednis, *Wykorzystanie danych biometrycznych w szkole…*, s. 135.