t. LXVII, nr 1/2026 DOI 10.33226/0032-6186.2026.1.2

Dr hab. Helena Szewczyk
Uniwersytet Śląski w Katowicach
ORCID: 0000-0002-1425-981X
e-mail: helena.szewczyk@us.edu.pl

Ochrona dóbr osobistych pracownika a rozwój nowych technologii na przykładzie stosowania systemów biometrycznych. W stulecie urodzin Profesora Tadeusza Zielińskiego. Cz. I

The protection of employee personal rights and the development of new technologies, illustrated by the example of biometric systems. On the centenary of the birth of Professor Tadeusz Zieliński. Vol. I

…prawo z bezprawiem ścierać się będzie zawsze, tak samo jak dobro pozostaje w nieustannym konflikcie ze złem.
Tadeusz Zieliński, *Droga do Ziemi Obiecanej*, Książka i Wiedza, 2002

Streszczenie
W ostatnim okresie rozwój technologii z dziedziny sztucznej inteligencji skutkuje coraz bardziej powszechną automatyzacją procesu gromadzenia danych biometrycznych (m.in. wizerunku) oraz rozwojem inteligentnych algorytmów. Rozwój ten w dużym stopniu jest wspierany przez coraz szersze zastosowanie sztucznej inteligencji w procesach identyfikowania jednostek, pozwalające na osiąganie lepszych i bardziej dokładnych wyników przy przetwarzaniu danych biometrycznych. Stosowanie różnych technik biometrycznych oraz przetwarzanie w ten sposób danych na masową skalę budzi jednak wątpliwości natury prawno-etycznej, a także rodzi pytania o zasadność i konieczność sprawowania „biometrycznej kontroli" nad społeczeństwem. Przetwarzanie danych biometrycznych niewątpliwie wymaga zastosowania podwyższonych standardów ochrony, ponieważ wiąże się ze zwiększonym ryzykiem naruszenia praw i wolności osób zatrudnionych. Ryzyko to materializuje się zwłaszcza w kontekście zjawiska dyskryminacji oraz naruszenia dóbr osobistych.

Słowa kluczowe
ochrona pracowników; dobra osobiste; nowe technologie; systemy biometryczne; dane biometryczne

JEL: K31

Abstract
Recently, the development of artificial intelligence technologies has resulted in more and more widespread automation of the process of collecting biometric data (including image) and the development of intelligent algorithms. This development is largely supported by the increasingly widespread use of artificial intelligence (AI) in individual identification processes, enabling better and more accurate results when processing biometric data. However, the use of various biometric techniques and the processing of data in this way on a mass scale raises legal and ethical concerns and raises questions about the validity and necessity of exercising "biometric control" over society. The processing of biometric data undoubtedly requires the application of increased protection standards because it is associated with an increased risk of violating the rights and freedoms of employees. This risk materializes especially in the context of discrimination and violation of personal rights. However, employers' rights arising from the employment relationship may not violate the personal rights of employees.

Keywords
protection of employees; personal goods; new technologies; biometric systems; biometric data

creative commons Uznanie autorstwa 2.0 Polska

Uwagi wprowadzające

Biometria jest wiedzą o automatycznym rozpoznawaniu ludzi w oparciu o ich cechy biologiczne, anatomiczne i fizjologiczne, na przykład linii papilarnych (odcisków palców), tęczówki oka, obrazu twarzy, geometrii dłoni, głosu i pewnych ludzkich zachowań, takich jak: elektroniczny lub biometryczny podpis czy sposób poruszania się. Polega to na zbadaniu przez system pobranych od danej osoby próbek biometrycznych i porównanie ich z posiadanymi wzorcami. W stosunkach zatrudnienia dane biometryczne pracowników służą przede wszystkim jako skuteczna forma identyfikacji i kontroli pracowników. W praktyce dane biometryczne mogą być wykorzystywane przez pracodawców w procesie rekrutacji, do kontroli czasu pracy, do weryfikowania dostępu pracowników do wybranych obszarów zakładów pracy lub do uzyskania określonych informacji. Swego czasu pracodawcy wprowadzali ewidencje czasu pracy za pomocą urządzeń biometrycznych funkcjonujących na podstawie odczytu części ciała pracowników i sprawdzali wykorzystywanie przez nich czasu pracy, itp. W coraz szerszym zakresie są one również wykorzystywane do kontroli pracowników za pomocą monitoringu audiowizualnego w zakładach pracy (Dörre-Kolasa, 2023, s. 63–79; Jabłoński, 2023, s. 13–30).

Granice wykorzystywania danych osobowych (biometrycznych) pracowników i kandydatów do pracy stanowią *de lege lata* przede wszystkim przepisy konstytucji RP, ratyfikowanych umów i porozumień międzynarodowych, unijnych aktów prawnych obowiązujących w naszym kraju, a także właściwe regulacje cywilnoprawne, przepisy kodeksu pracy oraz ustawy o ochronie danych osobowych (Golonka, 2010, s. 257). W Konstytucji RP nie ma wprawdzie wyraźnych odwołań do danych biometrycznych, ale przepisy konstytucyjne określają jednak nadrzędne zasady istotne dla problematyki tych danych, ponieważ dotyczą kwestii ochrony prywatności poszczególnych jednostek. Problematyka danych biometrycznych wiąże się z ochroną życia prywatnego, skoro dane te zawierają informacje o indywidualnych cechach biologicznych jednostek. Przepis art. 51 ust. l Konstytucji RP stanowi, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Przepis ten zawiera wyraźne upoważnienie ustawowe, jakie jest niezbędne, aby można było od konkretnej osoby domagać się określonych informacji, a więc także ujawnienia jej danych biometrycznych. Nie mniej istotny jest art. 47 Konstytucji, który stanowi, że każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Powstaje pytanie jak wygląda wykorzystywanie danych biometrycznych pracownika w stosunku pracy w dobie rozwoju nowoczesnych technologii? Czy uwzględnione zostały interesy obu stron stosunku pracy ze szczególnym uwzględnieniem ochrony dóbr osobistych pracowników? Dane biometryczne w szczególny sposób identyfikują bowiem pracownika i jest to sposób wykorzystywania danych pracownika dość głęboko ingerujący w sferę jego prywatności, a nawet intymności. Tym bardziej, że w ostatnim okresie rozwój technologii z dziedziny sztucznej inteligencji skutkuje coraz bardziej powszechną automatyzacją procesu gromadzenia danych biometrycznych (m.in. wizerunku) oraz rozwojem inteligentnych algorytmów (Szpunar, 2019, s. 11 i n.; Bąba, 2024, s. 195–209).

Warto zatem zweryfikować hipotezy, że przy okazji pozyskiwania tych danych pracodawcy mogą również naruszać godność, wolność, integralność oraz inne dobra osobiste pracowników. Przy korzystaniu przez pracodawcę z nowoczesnych technologii ustawodawca nie zawsze bowiem zapewnia w sposób wystarczający ochronę wolności i praw osób zatrudnionych. Przeprowadzona analiza pozwoli na ocenę polskich regulacji na tle prawa unijnego (Szabłowska, 2008, s. 47) oraz sformułowanie postulatów *de lege ferenda.* Od tego zależy stworzenie prawnych ram dla odpowiedniej i skutecznej ochrony osób zatrudnionych przed zagrożeniami w środowisku pracy. Można wstępnie założyć, iż stosowanie systemów biometrycznych w stosunkach pracy nie chroni dostatecznie praw i interesów pracowników. Gdy tymczasem istotne jest skuteczne przeciwdziałanie naruszeniu dóbr osobistych, mobbingowi i dyskryminacji osób zatrudnionych, zwłaszcza w ramach prewencji. Aby zweryfikować tę hipotezę należy dokonać analizy przedmiotowej regulacji posługując się przede wszystkim metodą dogmatyczno-językową oraz aksjologiczną, a także w ograniczonym zakresie prawno-porównawczą.

Pojęcie i istota danych biometrycznych a informacja biometryczna

Biometria jest nauką zajmującą się identyfikacją lub weryfikacją tożsamości osoby na podstawie jej cech fizjologicznych i behawioralnych (Bolle, 2008, s. 29). Te unikatowe cechy i umiejętności można zmierzyć i są to tzw. charakterystyki biometryczne. System biometryczny to aplikacja wykorzystująca technologie biometryczne, które umożliwiają automatyczną identyfikację lub weryfikację danej osoby (Jaroszewska-Choraś, 2016, s. 29). W piśmiennictwie przyjmuje się na ogół, że dane biometryczne pracownika to dane (informacje) o cechach życiowych (osobniczych) konkretnych ludzi, pozwalających na ich identyfikację. Indywidualizująca rola danych biometrycznych ma podstawę w tym, że każdy człowiek posiada szereg niepowtarzalnych, odróżniających go od innych cech, immanentnie związanych ze specyfiką i funkcjonowaniem jego organizmu. Dane biometryczne to unikalne cechy fizjologiczne i behawioralne ludzkiego organizmu (unikalne właściwości każdego indywidualnego człowieka), pozwalające odróżnić jedną osobę od drugiej (Korga, 2011, s. 620). Są one immamentnie przypisane (wyjątkowe) do danej osoby fizycznej i niezmienne w czasie. Cechy te, z wykorzystaniem odpowiednich technik oraz urządzeń, mogą być rozpoznawane („mierzone") i utrwalane w celach identyfikacyjnych, ale nie tylko, w bardzo wielu dziedzinach, m.in. w kryminalistyce (np. dla potrzeb ścigania sprawców przestępstw) czy w medycynie (np. pod kątem oceny ryzyka zapadalności

na różne choroby) (Golat, 2011, s. 14). Dane te są prezentowane najczęściej w podziale na dwie podstawowe grupy, tzn. dane odzwierciedlające cechy fizyczne, anatomiczne poszczególnych osób (pracowników) oraz dane charakteryzujące ich indywidualne sposoby zachowań, czyli tzw. cechy behawioralne. W praktyce największe znaczenie mają dane należące do pierwszej z tych grup, a zwłaszcza wizerunek twarzy i odciski palców, tęczówka oka, układ naczyń krwionośnych oraz kod genetyczny DNA. Natomiast jeżeli chodzi o dane biometryczne zaliczane do drugiej, behawioralnej grupy, to są nimi głos, sposób składania własnoręcznego podpisu czy indywidualny sposób chodzenia. Rzadziej wykorzystywane są kształt ucha, połysk skóry, termogram, ruch ust, EEG, EKG, styl pisma. Nie istnieje jednak pełny, wyczerpujący katalog danych biometrycznych ze względu na to, że dzięki doskonaleniu metod ich rozpoznawania oraz rejestracji wciąż ulega on rozszerzeniu w dobie rozwoju nowych technologii.

Dane biometryczne są szczególnym rodzajem danych osobowych. W piśmiennictwie uznaje się je za pozajęzykowe dane osobowe (Drozd, 2008, s. 45). Zgodnie z art. 4 ust. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, Dz.Urz. UE L 119 z 4.05.2016 (dalej: RODO) dane biometryczne to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Wymieniony w tym przepisie katalog sposobów pozyskiwania danych biometrycznych jest otwarty. Za szczególną kategorię danych osobowych dane biometryczne były ujmowane w poprzednio obowiązującej ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych[1], na co wskazywała definicja tych danych, zawarta w art. 6 ust. 2 tej ustawy. Zgodnie z tym przepisem danymi osobowymi były wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy czym osobą możliwą do zidentyfikowania była osoba, której tożsamość można było określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Wśród tych danych wskazane zostały m.in. dane o kodzie genetycznym oraz o stanie zdrowia, do oceny którego dane biometryczne są coraz częściej wykorzystywane. Zgodnie z art. 4 ust. 3 RODO dane dotyczące zdrowia to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia. Z kolei zgodnie z art. 4 ust. 13 RODO dane genetyczne to dane osobowe dotyczące odziedziczonych lub nabytych cech osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej. Zakaz gorszego traktowania osób ze względu na ich genotyp oraz zakaz stosowania testów genetycznych do celów stygmatyzacji i selekcji ludzi stanowi istotę zakazu dyskryminacji genetycznej (Kofin-Brończyk, 2023, s. 168–170).

Dane biometryczne to więc szczególna kategoria danych osobowych, które powstają w wyniku specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej i umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby i mogą być przetwarzane tylko w określonych, rygorystycznych warunkach. Z kolei termin „informacja biometryczna" ma szerszy, bardziej ogólny charakter i może odnosić się do samych cech fizycznych lub behawioralnych (np. odcisk palca, zdjęcie twarzy) przed ich przetworzeniem w celu identyfikacji. Można ją traktować jako surowe dane dotyczące cech fizycznych lub behawioralnych, które potencjalnie mogą stać się danymi biometrycznymi, jeśli zostaną poddane specjalistycznej analizie technicznej w celu identyfikacji osoby. Cel i sposób przetwarzania decyduje, czy dana informacja staje się „danymi biometrycznymi" w rozumieniu RODO. „Informacja biometryczna" to zatem ogólna cecha fizyczna lub behawioralna, natomiast „dane biometryczne" to informacja poddana specjalistycznemu, technicznemu przetwarzaniu w celu jednoznacznej identyfikacji osoby. W kontekście ochrony danych osobowych, istotne jest to drugie, węższe pojęcie, które podlega zaostrzonym rygorom prawnym.

Znaczenie rozróżnienia między ogólną informacją biometryczną a danymi biometrycznymi (w rozumieniu RODO) ma fundamentalne implikacje dla systemów sztucznej inteligencji (AI), wpływając na ich projektowanie, zgodność z prawem, etykę oraz techniczne aspekty działania. Jeśli system AI wykorzystuje specjalne techniki w celu jednoznacznej identyfikacji osoby, podlega on najbardziej rygorystycznym przepisom RODO (art. 9). Systemy AI wykorzystujące cechy biometryczne do innych celów (bez identyfikacji), np. do szacowania wieku, płci, mogą nie być traktowane jako przetwarzające dane biometryczne w sensie prawnym. Wymagają one standardowej ochrony danych osobowych, ale nie muszą spełniać wymogów z art. 9 RODO. Dopiero proces analizy tych informacji za pomocą algorytmów w celu stworzenia unikalnego szablonu (np. wzorca twarzy, szablonu głosu) sprawia, że stają się one danymi biometrycznymi w sensie prawnym.

Zdaniem M. Bąby „informacja biometryczna może być zatem rozumiana jako dane, które w wyniku procesu ich analizy zostały ukształtowane w istotną i użyteczną postać w drodze ich przetworzenia przez system biometryczny. Przetworzenie w przypadku identyfikacji oznacza wyłuskanie przez system biometryczny cech z surowych pomiarów, a następnie przeszukanie przez system całej bazy danych pod kątem zgodności wzorca z wyłuskanymi cechami biometrycznymi. Przetworzenie w przypadku weryfikacji oznacza wyłuskanie cech uzyskanych z pomiaru biometrycznego i porównanie cech wejściowych (pobranych w danym momencie) z cechami

zarejestrowanymi w systemowej bazie danych dla danego identyfikatora podmiotu. W wyniku porównania system ustala, że użytkownik jest tym, za kogo się podaje" (Bąba, 2016, s. 28–29). Na gruncie biometrii informacja i dane są zatem różnymi pojęciami, które nie są synonimami (pojęciami identycznymi), ale są ze sobą funkcjonalnie powiązane. Zdaniem tego autora „Dane biometryczne rozumiane jako pewne surowe fakty na temat zmierzonych cech fizycznych bądź behawioralnych danej osoby istnieją niezależnie od informacji biometrycznej, są nam dane, albowiem są zdeterminowanie przez genetykę lub fenotyp albo wykształcone nawyki" (Bąba, 2016, s.29). Informacja biometryczna to znaczenie, jakie nadaje surowej postaci danych na temat zmierzonych cech fizycznych bądź behawioralnych danej osoby biometryczny system rozpoznawania wzorca. Ogólne dane biometryczne zyskując indywidualną treść stają się informacją biometryczną. Jak zauważa M. Bąba przewaga infologiczna informacji biometrycznej pojawia się, gdy przechodzi się do szczegółu, tj. do procesu ustalania tożsamości konkretnej osoby. Informacja na poziomie infologicznym jest wnioskiem z danych przydatnym dla odbiorcy w pewnym określonym celu (Bąba, 2016, s. 28).

Przepisy kodeksu pracy regulują problematykę danych biometrycznych w sposób szczególny, ale regulację tę należy rozpatrywać w pierwszym rzędzie w świetle ogólnych unormowań dotyczących danych osobowych, a zwłaszcza art. 22^1 k.p. Ten ostatni przepis nie upoważnia pracodawcy do żądania od pracownika podania jego danych biometrycznych (Szewczyk, 2013, s. 93–107). Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania danych biometrycznych wyłącznie w przypadku, gdy przetwarzanie tych danych osobowych następuje z inicjatywy tych osób. Nie oznacza to jeszcze, że ich przetwarzanie będzie automatycznie dopuszczalne, czym innym jest bowiem przechowywanie danych, a czym innym ich udostępnienie na zewnątrz. Będzie to możliwe w sytuacjach wyjątkowych (bezwzględna konieczność), jeśli jest to niezbędne do osiągnięcia określonego celu gromadzenia i przetwarzania danych biometrycznych z uwzględnieniem ochrony podstawowych praw i wolności jednostek (Dörre-Kolasa, 2021, Legalis). Będziemy mieli z nimi do czynienia, gdy założonego celu nie da się osiągnąć w inny, mniej uciążliwy dla pracownika sposób, a wartość dobra chronionego przy użyciu narzędzi biometrycznych jest znaczna, np. ochrona zdrowia i życia pracownika.

Ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności 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 (Dörre-Kolasa, 2021, Legalis).

Podstawą przetwarzania danych biometrycznych pracowników jest niewątpliwie art. 9 ust. 2 lit. b i ust. 4 RODO w zw. z art. 22^{1b} § 2 k.p. Przetwarzanie danych biometrycznych pracownika jest dopuszczalne, gdy podanie tych danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę (technologiczne, produkcyjne), lub dostępu do pomieszczeń wymagających szczególnej ochrony (wymogi bezpieczeństwa, ochrona mienia szczególnej wartości, dzieł sztuki, tajemnica państwowa, itp.). Nie należy zapominać również o konieczności ich przetwarzania, gdy jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy. Przetwarzanie to powinno odbywać się na zasadzie wyjątku tylko wtedy, gdy jest to niezbędne do wypełnienia obowiązków i wykonania szczególnych praw w obszarze prawa pracy jako dozwolone prawem krajowym państwa członkowskiego. Uprawnienia pracodawców wynikające ze stosunku pracy nie mogą jednak naruszać dóbr osobistych osób zatrudnionych. Powinno się to zatem odbywać w warunkach pozwalających na respektowanie prawa pracownika do prywatności i innych dóbr osobistych. Dlatego tak ważne jest zachowanie zasady adekwatności (proporcjonalności) w stosunku do przetwarzania danych biometrycznych przez pracodawcę, aby nadmiernie nie uszczuplić praw i wolności osób zatrudnionych. Niezbędne jest zatem wyważenie wartości pozostających ze sobą w kolizji i ustalenie prymatu jednego z nich, któremu należy zapewnić ochronę. Pozyskiwanie danych o cechach biometrycznych pracownika jest bowiem przejawem głębokiej ingerencji w sferę prywatności pracownika (Kuba, 2013, s. 67–68). Istnieje również możliwość nielegalnego wykorzystania danych biometrycznych pracownika zdobytych niejawnie. Tylko zatem rygorystyczna ocena proporcjonalności wdrożonych przez pracodawców technik biometrycznych może przyczynić się do zwiększenia skuteczności w zakresie ochrony dóbr osobistych osób zatrudnionych, w tym również zakazu ich algorytmicznej dyskryminacji (Otto, 2022, s. 155–156).

Dane biometryczne jako szczególny rodzaj danych osobowych a dobra osobiste pracownika

Dane biometryczne umożliwiają niepodważalne potwierdzenie tożsamości danej osoby, ponieważ są jednostkowymi biologicznymi cechami (przymiotami), które mogą być przypisane tylko jednej osobie. W związku z tym pozwalają one na odróżnienie osoby, do której należą od pozostałych osób. Nie można jednak wykluczyć rzadkich przypadków modyfikacji tych danych w wyniku uszkodzeń oraz celowych zabiegów korekcyjnych. Przy pozyskiwaniu danych biometrycznych pracownika przez pracodawcę może zdarzyć się również, że niejako przy okazji dojdzie do przetwarzania niektórych danych wrażliwych (sensytywnych) pracownika, takich jak informacje o stanie jego zdrowia, genotypie oraz niektórych przebytych chorobach.

Przed nowelizacją kodeksu pracy odesłanie w art. 22^1 § 5 k.p. do przepisów o ochronie danych osobowych w zakresie nieuregulowanym w § 1–4 przesądziło o konieczności stosowania w prawie pracy ustawy o ochronie danych osobowych (Florek, 2017, s. 198–199; Kosmala,

2014, s. 337 i n.) w kontekście art. 47 i 51 Konstytucji RP. „Dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (art. 4 RODO). Dane o stanie zdrowia należą do szczególnej kategorii danych osobowych, tzw. danych wrażliwych, których przetwarzanie jest dopuszczalne tylko w przypadkach wskazanych w przepisach prawa. Przetwarzanie danych osobowych (wrażliwych) jest dopuszczalne w szczególności, jeśli osoba, której dane dotyczą, wyraziła na to zgodę na piśmie, oraz gdy przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w przepisach prawa (Szewczyk, 2022, s. 75–113). *De lege lata* musi istnieć wyraźny przepis prawny, na podstawie którego pracodawca może żądać od pracownika podania jego danych biometrycznych. Z kolei w świetle art. 22 RODO istnieje zakaz podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych (Sakowska-Baryła, 2018, s. 269).

Przepisy o ochronie danych osobowych stanowią istotne ograniczenie dla pracodawców zainteresowanych stosowaniem technologii biometrycznych. Prawo UE oraz polskie prawo pracy wraz z przepisami o ochronie danych osobowych, co do zasady, określają granice ochrony danych osobowych dotyczących stanu zdrowia pracowników. Tak ustalone granice chronią sferę prywatności i inne dobra osobiste pracownika oraz jego interesy, gwarantując jednak pracodawcy wypełnianie swoich podstawowych obowiązków związanych z zatrudnianiem pracowników. Od pracodawcy wymaga się w szczególności spełnienia podstawowego obowiązku ochrony zdrowia i życia osób zatrudnionych oraz ochrony ich prywatności. Zapewnienie bezpiecznych i higienicznych warunków pracy ma pierwszeństwo przed prawem do prywatności pracowników (Wyka, 2003, s. 161 i n.). Jak słusznie zauważył Sąd Najwyższy sfera zdrowia i życia pracowników jest jednak sferą wspólnych interesów stron stosunku pracy oraz interesu publicznego (wyrok SN z 16 listopadzie 2000, I PKN 44/00, OSNP 2002, nr 10, poz. 239). A więc działanie pracodawcy w granicach normatywnie ustalonych celów przetwarzania danych nie wymaga zgody pracownika, jednak przekraczanie tych celów przez przetwarzanie danych o stanie zdrowia, genetycznych i biometrycznych pracownika jest dopuszczalne tylko za zgodą tego ostatniego (Drozd, 2008, s. 180).

Ze względu na zindywidualizowany charakter danych biometrycznych korzystanie z nich, także przez pracodawców, powinno być postrzegane w kontekście ochrony dóbr osobistych osób pozostających w zatrudnieniu, których te dane dotyczą. Przepis art. 23 k.c. zawiera otwarte, przykładowe wyliczenie dóbr osobistych, wśród których bezpośredni związek z danymi biometrycznymi wykazuje jedynie wizerunek (Sieńczyło-Chlabicz, 2003, s. 17–24).

W tym kontekście dotyczy to prawa do prywatności, którego jest on przejawem. Wizerunek to nie tylko zwykła dana osobowa, lecz biometryczna dana osobowa, dla której z racji przyporządkowania jej do szczególnych kategorii danych osobowych została przewidziana odrębna forma przetwarzania (Jakubik, 2019, Legalis). W świetle ETPC pojęcie życia prywatnego obejmuje także prawo do tożsamości (Świerczyński, Więckowski, 2022, Legalis). Do najistotniejszych komponentów prawa do prywatności należy prawo do integracji psychofizycznej, autonomii, prywatności informacji oraz samostanowienia. Zastosowanie technik biometrycznych stanowi bowiem daleko idącą ingerencję w prywatność oraz godność osoby, której te dane dotyczą (Sutrop, 2010, s. 105). Pracownicy mają na ogół problemy ze zrozumieniem zakresu ingerencji i technicznych sposobów wykorzystania pobranych od nich materiałów w celu wyizolowania z nich danych biometrycznych (Wiewiórowski, 2012, s. 18).

Warunki korzystania z systemów biometrycznych

Zgoda jest ważną przesłanką wyłączającą bezprawność zachowania pracodawcy korzystającego z systemów biometrycznych. Dobra osobiste ze swej istoty są jednak powiązane z podmiotem, którego dotyczą. Silna więź łącząca osobę, w tym osobę pracownika z jej dobrem wyraża się między innymi w tym, że system prawny nie dopuszcza pełnej swobody w zakresie dysponowania dobrem przez osobę, której dane dobro osobiste przysługuje oraz prawami osobistymi opartymi na tych dobrach, a nawet zakaz jakiejkolwiek ingerencji w istotę niektórych dóbr osobistych. Jako przykład naruszeń dóbr osobistych, które nie podlegają autonomii podmiotu uprawnionego, podaje się życie, czy też ciężkie uszkodzenie ciała (Szpunar, 1990, s. 47). Zakres dopuszczalnej ingerencji naruszającej dobro osobiste jest z reguły ustalany odrębnie dla każdego rodzaju dobra (Wyrwiński, 2009, s. 204). Zgoda pracownika przynajmniej w niektórych sytuacjach nie uchyla więc bezprawności zachowania pracodawcy. Oceniając stan faktyczny oraz udzieloną zgodę, należy zawsze rozważyć, czy udzielenie zgody nie koliduje z szeroko rozumianym interesem publicznym oraz interesem uprawnionego. Dopiero negatywna odpowiedź na tak postawione pytanie umożliwiałaby wyłączenie bezprawności zachowania pracodawcy (Cisek, 1989, s. 95–97). Tym samym swoboda w zakresie dysponowania swoimi dobrami osobistymi musi podlegać ocenie z punktu widzenia ogólnych zasad prawa, a zwłaszcza zasad współżycia społecznego czy reguł o podobnym charakterze. Bez tej oceny działanie za zgodą uprawnionego jest więc co do zasady bezprawne (Zieliński, 1986, s. 193 i n.).

Użycie systemu biometrycznego rejestrującego czas pracy pracowników lub kontrolującego dostęp do tzw. tajnych pomieszczeń przez pracodawcę, może umożliwić mu przy okazji zapis ich stanu zdrowia (taka daną jest też wynik badania w zakresie trzeźwości oraz przebytych odwykach oraz wpływu nałogów na stan zdrowia) (Hołyst, 2011, s. 702 i n.). W związku z powyższym forma identyfikacji biometrycznej, zainstalowanej na potrzeby

ewidencji czasu pracy, nie jest dopuszczalna nawet w sytuacji, gdy pracownik oficjalnie wyrazi zgodę na udostępnienie omawianych danych osobowych. Po pierwsze ze względu na to, że dzięki rozwojowi medycyny nie tylko analiza kodu genetycznego czy krwi, ale inne dane biometryczne człowieka mogą dostarczyć pracodawcy danych o stanie zdrowia pracownika i jego chorobach, dlatego dane biometryczne należy zaliczyć do tzw. danych wrażliwych (sensytywnych), których przetwarzanie podlega rygorom ustawy o ochronie danych osobowych. Przetwarzanie danych wrażliwych dopuszczalne jest natomiast tylko na podstawie odrębnych przepisów, jeżeli w szczególności z przepisu tego wynika uprawnienie do przetwarzania danych wrażliwych bez zgody osoby, której one dotyczą oraz przepis ten stwarza pełne gwarancje ochrony tych danych (Litwiński, 2009, s. 151; Drozd, 2008, s. 165; Nerka, 2009, s. 76 i n.).

Przetwarzanie tych danych sensytywnych możliwe jest więc tylko na podstawie przepisów prawnych niezależnie od tego, czy osoba której dane są przetwarzane wyrazi na to zgodę. Zgoda pracownika w przypadku danych wrażliwych nie uchyla więc bezprawności przetwarzania tych danych bez podstawy prawnej. Po drugie w relacjach pracowniczego zatrudnienia z reguły trudno mówić o „dobrowolnym", „swobodnym" lub „nieskrępowanym" podjęciu przez pracownika (kandydata) decyzji i wyrażeniu woli w sprawie zgody (Sibiga, 2005, s. 70 i n.). W przypadku przetwarzania danych osobowych wrażliwych zgoda pracownika z reguły nie będzie więc stanowić podstawy prawnej dla przetwarzania danych wrażliwych pracownika. Przetwarzanie danych wrażliwych możliwe jest bowiem tylko na podstawie wyraźnego zezwolenia zawartego w przepisach prawa (Litwiński, 2008, s. 71; Barański, 2020, s. 26–32).

Trudno zatem było zaakceptować te stanowiska w piśmiennictwie, które przed wprowadzeniem art. 22^{1b} k.p. uznawały, iż przesłanki legalizujące przetwarzanie danych biometrycznych wymienione w art. 23 ust. 1 uchylonej ustawy o ochronie danych osobowych znajdują zastosowanie do przetwarzania danych biometrycznych pracowników uzyskiwanych na żądanie pracodawców od tych pierwszych (Spytek-Bandurska, 2009, s. 25 i n.; Malik 2008, s. 624–625; Korga, 2011, s. 620). Należało raczej zaakceptować poglądy, w świetle których w zakresie gromadzenia i przetwarzania danych osobowych (biometrycznych) pracowników i kandydatów do pracy otrzymanych od nich samych na żądanie pracodawcy kodeks pracy wyłączał stosowanie art. 23 ust. 1 oraz art. 27 uchylonej ustawy o ochronie danych osobowych, włącznie z przepisem, który przewiduje zgodę podmiotu danych jako podstawę przetwarzania jego danych osobowych (Sibiga, 2005, s. 69). W świetle tych poglądów pracodawca nie jest uprawniony do żądania od pracownika lub kandydata do pracy innych danych osobowych niż wymienione w art. 22^1 § 1–4 i § 4 k. p., nawet gdy powoła się na uzyskaną od niego zgodę na przetwarzanie danych (Sibiga, 2012, s. 125).

Warto jednakże zauważyć, że pierwszeństwo w stosowaniu art. 22^1 k.p. dotyczy jedynie wąskiego zakresu zagadnień związanych z dopuszczalnością przetwarzania i adekwatnością danych osobowych (m.in. biometrycznych), których pracodawca może żądać bezpośrednio od pracowników i kandydatów do pracy. W pozostałych przypadkach, np. gdy pracodawca gromadzi dane osobowe pracownika lub kandydata zdobyte z innych źródeł niż od samego pracownika lub kandydata przepisy o ochronie danych osobowych muszą znaleźć wprost zastosowanie (Sibiga, 2012, s. 125). Jednak te pozostałe przypadki rzadko znajdą zastosowanie w odniesieniu do pozyskiwania danych biometrycznych, ponieważ charakter tych ostatnich danych sprawia, iż muszą one być pozyskiwane od samych pracowników i kandydatów na pracowników. Natomiast pracodawcy nie są upoważnieni do zgłaszania takich żądań w odniesieniu do tych osób, z powołaniem się na udzieloną przez nich zgodę, jako na jedyną przesłankę legalizującą przetwarzanie danych biometrycznych (Kulesza, 2007, s. 139).

Przypisy/Notes

[1] Dz.U. z 2016 r., poz. 922 ze zm. (uchylona). Ustawa ta jeszcze obowiązuje w ograniczonym zakresie, m.in. w sprawach dotyczących postępowań wszczętych przed wejściem w życie nowych przepisów

Bibliografia/References

Barański, M. (2020). Ukryty monitoring w miejscu pracy. *Monitor Prawa Pracy*, 3. DOI: 10.32027/MOPR.20.3.5

Bąba, M. (2016). Próba wyznaczenia zakresu pojęcia danych biometrycznych. *Prawo Mediów Elektronicznych*, 2.

Bąba, M. (2024). Employment with the use of artificial intelligente: opportunities and risks. *Studia z Zakresu Prawa Pracy i Polityki Społecznej,* 3.

Bolle, R. M. (2008). *Biometria*. Wydawnictwo Naukowe PWN.

Cisek, A. (1989). *Dobra osobiste i ich niemajątkowa ochrona w kodeksie cywilnym*. Zakład Narodowy im. Ossolińskich.

Dörre-Kolasa, D. (2023). Przetwarzanie danych osobowych pracowników w ramach tzw. innych form monitoringu. *Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji*, t. 132.

Dörre-Kolasa, D. (2021). Komentarz do art. 22^1 k.p. W: P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Legalis.

Drozd, A. (2008). *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy.* LexisNexis.

Florek, L. (2017). *Kodeks pracy. Komentarz.* W: L. Florek (red.), Warszawa Wolters Kluwer Polska

Golat, R. (2011). Dane biometryczne w stosunkach pracowniczych. *Służba Pracownicza*, 11.

Golonka, A. (2010). Granice dopuszczalności monitoringu pracownika przy wykorzystaniu jego danych biometrycznych oraz audiowizualnych form nadzoru. W: Z. Góral (red.), *Kontrola pracownika. Możliwości techniczne i dylematy prawne*. Wolters Kluwer.

Hołyst, B. (2011). Biometria w procesie identyfikacji. W: T. Grzegorczyk (red.), *Funkcje procesu karnego. Księga jubileuszowa Profesora Janusza Tylmana*. Wolters Kluwer.
Jabłoński, M. (2023). Stosowanie wobec pracowników ukrytego monitoringu wizyjnego: kwestie sporne i niejednoznaczne. *Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji,* t. 132, DOI: 10.19195/0137-1134.132.2
Jakubik, M. (2019). *Wizerunek na gruncie Rodo*. Legalis.
Jaroszewska-Choraś, D. (2016). *Biometria. Aspekty prawne*. Gdańsk Wydawnictwo Uniwersytetu Gdańskiego.
Kofin-Brończyk, K. (2023). Zakaz dyskryminacji genetycznej w prawie międzynarodowym publicznym. *Studia Prawnicze KUL*, 1.
Korga, M. (2011). Dane biometryczne i ich wykorzystywanie na gruncie stosunku pracy. *Monitor Prawa Pracy,* 12.
Kosmala, K. (2014). *Dobra osobiste.* W: I. Lewandowska-Malec (red.). C.H.Beck.
Kuba, M. (2013). Prawne uwarunkowania zastosowania technik biometrycznych w procesie kontroli pracownika. W: Z. Góral (red.), *Gdańsko-Łódzkie Roczniki Prawa Pracy i Prawa Socjalnego*. Gdańsk–Łódź, 3.
Kulesza, E. (2007). Kilka uwag o zakresie danych osobowych pracownika przetwarzanych przez pracodawcę. *Gdańskie Studia Prawnicze*, t. XVII.
Litwiński, P. (2008). Monitoring pracownika w miejscu pracy a ochrona danych osobowych pracownika. *Monitor Prawa Pracy*, 2.
Litwiński, P. (2009). *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*. Wolters Kluwer Polska.
Malik, K. (2008). Problematyka przetwarzania danych biometrycznych pracowników. *Monitor Prawniczy*, 12.
Nerka, A. (2009). Problematyka zgody pracownika na przetwarzanie danych osobowych. W: T. Wyka, A. Nerka (red.), *Granice ochrony danych osobowych w stosunkach pracy*. Wolters Kluwer.
Otto, M. (2022). A step towards digital self-& co-determination in the context of algorithmic management systems. *Italian Labour Law e-Journal* 15 (1).
Sakowska-Baryła, M. (2018). W: M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. C.H.Beck.
Sibiga, G. (2005). Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy. *Radca Prawny*, 2.
Sibiga, G. (2012). Zakres stosowania ustawy o ochronie danych osobowych do przetwarzania danych pracowników i osób ubiegających się o zatrudnienia. *Monitor Prawa Pracy*, 3.
Sieńczyło – Chlabicz, J. (2003). Przedmiot, podmiot i charakter prawa do wizerunku, *Przegląd Ustawodawstwa Gospodarczego,* 8.
Spytek-Bandurska, G. (2009). Wybrane problemy pracodawców ze stosowaniem przepisów o ochronie danych osobowych. W: T. Wyka, A. Nerka. (red.), *Granice ochrony danych osobowych w stosunkach pracy*. Wolters Kluwer.
Sutrop, M. (2010). Ethisal Isssues in Goering Biometrics Technologies. W: A. Kumar, D. Zhang (red.), *Ethics and Policy of Biometrics*. Springer.
Szabłowska, M. (2008). Ochrona danych osobowych pracownika w Polsce na tle europejskich standardów – wybrane zagadnienia. W: G. Goździewicz, M. Szabłowska. (red.), *Prawna ochrona danych osobowych w Polsce na tle standardów Europejskich*. TNOiK „Dom Organizatora".
Szewczyk, H. (2013). Dopuszczalność wykorzystywania danych biometrycznych pracowników i kandydatów do pracy w stosunkach pracy. W: B. Ćwiertniak (red.), *Aktualne zagadnienia prawa pracy i polityki socjalne zbiór studiów. T. 2.* Sosnowiec, Oficyna Wydawnicza Humanitas.
Szewczyk, H. (2022). Glosa do wyroku Sądu Najwyższego z dnia 4 lutego 2021 r., II PSKP 7/21, *Orzecznictwo Sądów Polskich,* 10.
Szpunar, A. (1990). Zgoda uprawnionego w zakresie dóbr osobistych. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 1.
Szpunar, M. (2019). *Kultura algorytmów*. Wydawnictwo Uniwersytetu Jagiellońskiego.
Świerczyński, M., Więckowski, Z. (2022). Identyfikacja na podstawie danych biometrycznych (wizerunku) w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka. W: J. Gołaczyński (red.), *Prawo Nowych Technologii. Księga z okazji jubileuszu 20-lecia działalności Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego – Blok Prawa Komputerowego*, C.H.Beck.
Wiewiórowski, W. (2012). Ochrona danych osobowych podmiotów objętych indywidualnym prawem pracy. W: T. Wyka, A. Nerka, *Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych: stan obecny i perspektywy zmian.* Wolters Kluwer.
Wyka, T. (2003). *Ochrona zdrowia i życia pracownika jako element treści stosunku pracy*. Difin.
Wyrwiński, M. (2009). Zgoda na naruszenie dobra osobistego. W: J. Barta, R. Markiewicz, *Media a dobra osobiste*. Wolters Kluwer.
Zieliński, T. (1986). *Prawo pracy. Zarys systemu*. *Cz. I. Ogólna*. Państwowe Wydawnictwo Naukowe.

Helena Szewczyk, adiunkt w Instytucie Nauk Prawnych na Wydziale Prawa i Administracji Uniwersytetu Śląskiego w Katowicach. Jest absolwentką Uniwersytetu Ekonomicznego w Katowicach oraz Uniwersytetu Śląskiego. Jej zainteresowania naukowe związane są z prawem pracy, prawem urzędniczym oraz europejskim prawem pracy. Jest autorką wielu publikacji naukowych (książek, studiów, artykułów, glos itp.).Wykonuje zawód radcy prawnego.

Helena Szewczyk is an assistant professor at the Institute of Legal Studies at the Faculty of Law and Administration of the University of Silesia in Katowice. She is a graduate of the University of Economics in Katowice and the University of Silesia. Her research interests include labor law, civil service law, and European labor law. She is the author of numerous academic publications (books, studies, articles, commentaries, etc.). She practices as a legal counsel.