POLSKA AKADEMIA NAUK
INSTYTUT NAUK PRAWNYCH

PL ISSN 0039-3312

Studia
PRAWNICZE

Zeszyt 1(187) 2011
Warszawa 2011

*Magdalena Korga* ■

# PRZETWARZANIE DANYCH BIOMETRYCZNYCH PRACOWNIKÓW W ŚWIETLE ORZECZENIA NSA Z DNIA 1 GRUDNIA 2009R. (I OSK 249/09)

## 1. Wstęp

Wielu przedsiębiorców wykorzystuje w praktyce systemy weryfikacji swoich pracowników oparte na ich liniach papilarnych, obrazie tęczówki oka czy kształcie dłoni (czyli danych biometrycznych – szczególnym rodzaju danych osobowych). Dane biometryczne pozwalają na jednoznaczną identyfikację osoby, bez konieczności wykorzystywania przedmiotów powierzonych pracownikowi przez pracodawcę (np. kart chipowych, magnetycznych, legitymacji) oraz niezależną od wiedzy osoby rozpoznawanej (np. znajomości kodu czy hasła). Jest to niewątpliwą zaletą technologii wykorzystującej dane biometryczne bazującej na informacjach pochodzących bezpośrednio od pracownika. Orzeczenie Naczelnego Sądu Administracyjnego (dalej jako NSA) z dnia 1 grudnia 2009r. (I OSK 249/09, LEX 553777) jest pierwszym wyrokiem poruszającym kwestię przetwarzania przez pracodawcę danych biometrycznych pracownika na gruncie polskiego prawa, stąd jego doniosłość i potrzeba dogłębnej analizy.

Przetwarzanie danych osobowych w przedsiębiorstwie jest koniecznością – nie dotyczy jedynie podmiotów prowadzących jednoosobową działalność gospodarczą. Pracodawcy muszą przetwarzać dane osobowe pracowników, m.in. zbierając je i wykorzystując celem realizacji nakładanych na nich obowiązków wynikających z przepisów prawa pracy, ubezpieczeń społecznych oraz związanych

ze świadczeniami na rzecz pracowników. Sama specyfika prowadzonej przez przedsiębiorstwo działalności wymusza niejednokrotnie konieczność ujawniania informacji o pracownikach. Dane osobowe są umieszczane np. na identyfikatorach noszonych przez pracowników, by poprawić jakość obsługi klientów czy też podawane są na firmowej stronie internetowej lub w korespondencji emailowej.

Postępujący na przestrzeni ostatnich lat rozwój nowych technologii i środków komunikacji, jak również praktyk związanych ze świadczeniem pracy, spowodował, iż obowiązujące przepisy prawne dotyczące przetwarzania danych osobowych w stosunkach pracy nie przystają do wymagań rzeczywistości. Nie tylko stwarzają poważne trudności interpretacyjne, ale również ograniczają pracodawcy możliwości prowadzenia przedsiębiorstwa, jednocześnie nie zapewniając należytej ochrony pracownikom, jako dysponentom danych. Przykładem rozdźwięku między realiami istniejącymi w zakładach pracy a przepisami prawnymi jest m.in. brak uregulowania prawnego dotyczącego kwestii monitoringu w miejscu pracy, a także ograniczony i skrajnie restrykcyjny katalog danych osobowych, których przedstawienia pracodawca może żądać od pracownika oraz kandydata do pracy.

## 2. Przetwarzanie i ochrona danych osobowych pracowników

Zgodnie z art. 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej[1] „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby". Odzwierciedleniem i doprecyzowaniem treści art. 51 Konstytucji na gruncie prawa pracy jest art. $22^1$ Kodeksu pracy[2], obowiązujący od 1 stycznia 2004r[3]. Praktycy wskazują, że wprowadzenie tego przepisu stanowiło przełom w uregulowaniu sytuacji prawnej pracowników dotyczącej ochrony ich prywatności[4]. Nadmienić w tym miejscu należy, iż artykuł $22^1$ k.p. kształtuje prawa i obowiązki pracodawcy zarówno w odniesieniu do pracowników jak i kandydatów do pracy. W niniejszym artykule omówiona zostanie tematyka przetwarzania danych osobowych osób już zatrudnionych.

---

[1] Ustawa z dnia 2 kwietnia 1997r. – Konstytucja Rzeczypospolitej Polskiej (Dz. U. Nr 78, poz. 483 z późn. zm.).

[2] Ustawa z dnia 26 kwietnia 1974r. – Kodeks pracy (Dz. U. z 1998r. Nr 21, poz. 94 z późn. zm.). – dalej jako k.p.

[3] Wprowadzony ustawą z dnia 14 listopada 2003 r. o zmianie ustawy - Kodeks pracy oraz o zmianie niektórych innych ustaw (Dz. U. Nr 213, poz. 2081).

[4] Zob. szerzej M. Gersdorf [w:] M. Gersdorf, K. Rączka, M. Raczkowski *Kodeks pracy. Komentarz*, Warszawa 2010, s. 149; zob. także http://26konferencja.giodo.gov.pl/data/resources/GersdorfM _paper.pdf.

Ustawodawca w art. 22[1] k.p. wskazał na prawo pracodawcy do żądania od pracownika podania danych osobowych obejmujących:

1) imię (imiona) i nazwisko,
2) imiona rodziców,
3) datę urodzenia,
4) miejsce zamieszkania (adres do korespondencji),
5) wykształcenie,
6) przebieg dotychczasowego zatrudnienia,
7) numer PESEL,
8) inne niż ww. dane osobowe pracownika, a także imiona i nazwiska oraz daty urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

Katalog powyższy jest katalogiem zamkniętym. Sam jednak art. 22[1] k.p. „otwiera" go niejako wskazując w treści § 4, że pracodawca może żądać podania innych danych osobowych niż określone powyżej, jeżeli wynika to z odrębnych przepisów prawa. Warto zauważyć, że na dzień przygotowywania artykułu nie istnieją przepisy, które zezwalałaby pracodawcy na żądanie od pracownika podania jego danych osobowych innych niż wymienione w art. 22[1] § 1 i 2 k.p. Podsumowując, art. 22[1] k.p. nie tyle przyznaje pracodawcy prawo, ale raczej ogranicza zakres danych, których może on żądać od pracownika[5].

Art. 22[1] § 5 k.p. w zakresie nieuregulowanym w Kodeksie pracy odsyła bezpośrednio do przepisów o ochronie danych osobowych. Przede wszystkim odesłanie to dotyczy ustawy o ochronie danych osobowych[6], ale trzeba mieć także na uwadze przepisy innych aktów normatywnych odnoszące się do kwestii przetwarzania i ochrony danych[7]. Są to przepisy szczególne („sektorowe", „specjalne") normujące poszczególne dziedziny życia społecznego[8], np. Prawo prasowe[9], Prawo o aktach stanu cywilnego[10], Prawo bankowe[11].

---

[5] A. Drozd., *Ochrona danych osobowych pracownika (kandydata) po nowelizacji kodeksu pracy*, Prawo i Zabezpieczenie Społeczne 2004, nr 1, s. 25.

[6] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) – dalej jako u.o.d.o.

[7] Szerzej na temat pojęcia „przepisów o ochronie danych osobowych" zob. G. Sibiga *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 26-27.

[8] J. Barta, P. Fajgielski, R. Markiewicz *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 124.

[9] Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. Nr 5, poz. 24 z późn. zm.)

[10] Ustawa z dnia 29 września 1986 r. – Prawo o aktach stanu cywilnego (Dz. U. z 2004 r. Nr 161, poz. 1688 z późn. zm.).

[11] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002r. Nr 72, poz. 665 z późn. zm.).

Ustawa o ochronie danych osobowych wyróżnia dwie kategorie danych: dane zwykłe („pospolite", „neutralne") oraz dane wrażliwe („delikatne", „sensytywne"). Dane wrażliwe, zgodnie z art. 27 ust. 1 u.o.d.o., dotyczą m.in. poglądów politycznych, przynależności wyznaniowej, partyjnej i związkowej, stanu zdrowia. Szczególnym rodzajem danych osobowych, niewyodrębnionym w ustawie o ochronie danych osobowych, są dane biometryczne. Jak zauważa Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych[12] w „Dokumencie roboczym w sprawie biometrii"[13] dane biometryczne mają „szczególny charakter, ponieważ mają związek z charakterystyką zachowań i fizjologią danej osoby oraz mogą umożliwiać identyfikację bez pozostawiania wątpliwości". Danymi biometrycznymi są m.in. linie papilarne, obraz tęczówki i siatkówki oka, geometria dłoni, barwa i ton głosu, wizerunek twarzy. W aktualnym polskim stanie prawnym brak jest powszechnie obowiązujących, kompleksowych przepisów dotyczących biometrii. Do przetwarzania danych biometrycznych zastosowanie znajduje oczywiście ustawa o ochronie danych osobowych, jednakże bezpośrednio do danych biometrycznych i do prawa ich pozyskiwania od dysponenta danych odnoszą się jedynie szczególne przepisy „branżowe". Są nimi m.in. ustawa o dokumentach paszportowych[14], ustawa o Policji[15], ustawa o cudzoziemcach[16], ustawa o Straży Granicznej[17]. Dla przykładu w dokumentach paszportowych zamieszczane są w formie elektronicznej wizerunek twarzy i odciski palców. Te same rodzaje danych biometrycznych mogą być przetwarzane w postępowaniach oraz rejestrach prowadzonych na podstawie ustawy o cudzoziemcach.

---

[12] Grupa robocza artykułu 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (dalej jako Grupa Robocza) została powołana na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L Nr 281, s. 31) - dalej jako Dyrektywa 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prawa do prywatności. Składa się z przedstawicieli krajowych organów ochrony danych państw członkowskich UE oraz przedstawicieli Komisji Europejskiej. Więcej informacji o Grupie Roboczej oraz ochronie danych osobowych w Unii Europejskiej znaleźć można na stronie internetowej: http://www.europa.eu.int oraz http://www.giodo.gov.pl.

[13] Przyjęty w dniu 1 sierpnia 2003 r. „Working document on biometrics" (12168/02/EN WP 80).

[14] Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych (Dz. U. Nr 143, poz. 1027 z późn. zm.).

[15] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2007r. Nr 43, poz. 277 z późn. zm.).

[16] Ustawa z dnia 13 czerwca 2003 r. o cudzoziemcach (Dz. U. z 2006r. Nr 234, poz. 1694 z późn. zm.).

[17] Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2005 r. Nr 234, poz. 1997 z późn. zm.).

W przepisach prawa pracy nie istnieje natomiast żaden przepis, na podstawie którego pracodawca mógłby żądać pod pracownika podania jego danych biometrycznych.

## 3. Wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009r. oraz jego wpływ na praktykę

Wzajemny stosunek przepisów Kodeksu pracy i ustawy o ochronie danych osobowych w połączeniu z zagadnieniem danych biometrycznych oraz kwestią pozycji stron w stosunku pracy stały się przedmiotem rozstrzygnięcia Naczelnego Sądu Administracyjnego. W wyroku z dnia 1 grudnia 2009r. (I OSK 249/09, LEX 553777) NSA wypowiedział się na temat zbierania przez pracodawców danych biometrycznych (w postaci linii papilarnych) pracowników, za ich uprzednią zgodą wyrażoną na piśmie. Celem przetwarzania danych biometrycznych w omawianym przypadku było ewidencjonowanie czasu pracy w zakładzie pracy.

W przedmiotowej sprawie ustalono następujący stan faktyczny. Spółka L. wprowadziła system czytników linii papilarnych, zainstalowany przy wejściach do budynków i za ich pomocą rejestrowała czas pracy pracowników. Ewidencja czasu pracy odbywała się zarówno przy użyciu kart radiowych jak i za pomocą wyżej opisanych czytników, przy czym każdy pracownik mógł wybrać sposób rejestracji. Pracodawca skanował linie papilarne palców dłoni pracowników, po to by móc ewidencjonować ich czas pracy. Zeskanowany obraz (charakterystyczne punkty linii papilarnych) był następnie przetwarzany na zapis cyfrowy (kod cyfrowy). Linie papilarne palca przyłożonego przez pracownika do czytnika były porównywane z zapisanym kodem w celu ewidencji wejść i wyjść z pracy. Dane biometryczne zbierane były na podstawie pisemnej zgody pracowników na przetwarzanie wzoru linii papilarnych.

Na podstawie ustalonego stanu faktycznego Generalny Inspektor Danych Osobowych (dalej jako Generalny Inspektor) wydał, a następnie podtrzymał decyzję, nakazującą Spółce L. usunięcie uchybień w procesie przetwarzania danych osobowych. Generalny Inspektor zobowiązał Spółkę do usunięcia danych dotyczących układu linii papilarnych pracowników i nakazał zaprzestać ich zbierania.

Z decyzją Generalnego Inspektora nie zgodził się Wojewódzki Sąd Administracyjny w Warszawie. W wyroku z dnia 27 listopada 2008r. (II SA/Wa 903/08) Wojewódzki Sąd Administracyjny uznał, że przesłanki legalizujące przetwarzanie danych osobowych wymienione w art. 23 ust. 1 u.o.d.o. mają charakter autonomiczny i niezależny w stosunku do przepisów Kodeksu pracy. W przypadku wyrażenia przez dysponenta danych (pracownika) zgody na przetwarzanie

swoich danych biometrycznych (czyli innych danych pracowniczych niż wymienione w art. $22^1$ § 1-4 k.p.), nie ma konieczności „poszukiwania" innej podstawy dla zgodnego z prawem ich przetwarzania. Poprzez art. $22^1$ § 5 k.p. pracodawca może pobierać i gromadzić, czyli przetwarzać dane biometryczne pracowników, o ile spełniona zostanie chociażby jedna z przesłanek legalizujących ich przetwarzanie przewidziana w ustawie o ochronie danych osobowych. Z treści przepisu art. $22^1$ § 5 k.p. sąd wywiódł wniosek, że w odniesieniu do danych biometrycznych z zasady nie jest zabronione ich przetwarzanie, lecz musi się ono odbywać z poszanowaniem przepisów ustawy o ochronie danych osobowych.

Skargę kasacyjną od powyższego wyroku wniósł Generalny Inspektor podnosząc, iż art. $22^1$ § 1-2 i § 4 k.p. wskazuje jakich danych osobowych pracodawca ma prawo żądać od pracownika (pozyskiwać i dalej przetwarzać). Kasator zauważył, że z brzmienia tych przepisów wynika prawo pracodawcy do przetwarzania wyłącznie tych danych osobowych, które są wymienione w art. $22^1$ k.p. Użyte w nim słowo „żądać" odnosi się do czynności pozyskania danych osobowych, a co za tym idzie, do dalszego ich przetwarzania. Wobec tego niedopuszczalne jest usankcjonowanie w oparciu o inne przesłanki, tj. wymienione w art. 23 ust. 1 u.o.d.o., przetwarzania przez pracodawcę danych biometrycznych. Generalny Inspektor podkreślił ponadto, że warunkiem uznania zgody za przesłankę legalizującą przetwarzanie danych osobowych jest jej dobrowolność. Okoliczności wpływające na brak równowagi w relacji pomiędzy pracodawcą a pracownikiem sprzyjają wymuszeniu zgody, a co się z tym wiąże pozbawiają ją przymiotu dobrowolności.

Argumenty Generalnego Inspektora zostały uwzględnione i zaaprobowane przez Naczelny Sąd Administracyjny, co skutkowało uchyleniem zaskarżonego wyroku i oddaleniem skargi Spółki na decyzję Generalnego Inspektora.

Wydaje się, że podstawową kwestią mającą znaczenie przy rozstrzyganiu referowanej sprawy było przyjęcie przez NSA, iż pracownik proszony o zgodę na przetwarzanie jego danych osobowych (w tym przypadku danych biometrycznych), znajduje się w sytuacji niekomfortowej. Wie on, że niewyrażenie zgody wobec pracodawcy może wpłynąć na jego sytuację jako pracownika. Strony stosunku pracy – pracodawca i pracownik – znajdują się w położeniu nierównorzędnym, inaczej niż ma się to przykładowo w przypadku banku i jego klienta[18]. Pracownik jest zależny od pracodawcy, jako podmiotu, któremu zgoda ma być udzielona.

[18] Pomimo, jak się wydaje, w miarę komfortowej sytuacji klienta w stosunku do banku, Przewodnicząca Komisji Nadzoru Bankowego wystosowała do prezesów banków pismo odnoszące się do warunków wyrażonej przez klientów zgody na przetwarzanie ich danych osobowych – zob. szerzej P. Babiarz „Udostępnianie przez bank danych osobowych klientów", Monitor Prawniczy 2001, nr 5, s. 327.

Swoboda wyrażenia zgody przez pracownika jest zatem z zasady wątpliwa[19]. Jak stwierdził NSA, z powyższych względów katalog danych, których pracodawca może żądać od pracownika, został ograniczony w Kodeksie pracy (art. $22^1$ k.p.). W uzasadnieniu prawnym wyroku NSA konstatuje, że „uznanie faktu wyrażenia zgody przez pracownika, jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. $22^1$ Kodeksu pracy, stanowiłoby obejście tego przepisu".

Należy w tym miejscu wskazać pogląd wyrażony przez Grupę Roboczą już w dokumencie z dnia 13 września 2001r. pt. „Opinia Grupy Roboczej w sprawie przetwarzania danych osobowych w kontekście zatrudnienia"[20]. Grupa Robocza wskazała w nim, iż udzielona przez pracownika zgoda na przetwarzanie jego danych osobowych jest „misleading" (zwodnicza, myląca)[21]. Grupa Robocza argumentuje w Opinii, że „pracodawca musi przetwarzać dane osobowe pracowników – jest to nieuniknioną i konieczną konsekwencją stosunku pracy – jednak legitymizacja procesu przetwarzania danych przez pracodawcę na podstawie zgody wyrażonej przez pracownika jest zwodnicza. Uzależnienie od zgody pracownika winno zostać ograniczone do przypadków, w których pracownik ma całkowitą swobodę jej udzielenia i jest w stanie odmówić wyrażenia zgody bez narażania się na szkodę"[22].

Naczelny Sąd Administracyjny stwierdził ponadto w uzasadnieniu wyroku, że praktyka rozszerzania katalogu danych osobowych określonych w art. $22^1$ k.p. poprzez zastosowanie art. 23 ust. 1 pkt 1 u.o.d.o. jest sprzeczna z zasadą adekwatności (proporcjonalności), implementowaną do u.o.d.o. z postanowień Dyrektywy 95/46/WE. NSA podkreślił, że „zasada proporcjonalności wyraża się w obowiązku przetwarzania prawidłowych danych przez administratorów w sposób odpowiedni do celów, dla jakich zostały zgromadzone." Powołując się na wydany przez Grupę Roboczą „Dokument roboczy w sprawie biometrii", sąd zwrócił uwagę, iż podstawowym kryterium dotyczącym przetwarzania danych bio-

---

[19] Tak m.in. P. Fajgielski *Zgoda na przetwarzanie danych osobowych* (w:) G. Sibiga, X. Konarski (red.) *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Warszawa 2007, s. 47.

[20] Oryginalny tytuł „Opinion 8/2001 on the processing of personal data in the employment context".

[21] *Wielki słownik angielsko – polski*, red. J. Linde – Usiekniewicz, Warszawa 2002, s. 755.

[22] Tłum. z jęz. angielskiego – M.K. W oryginale *where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.*

metrycznych jest właśnie zasada proporcjonalności. Cel, jakim jest kontrolowanie czasu pracy pracowników, w referowanej sprawie uznany został za nieadekwatny, nieusprawiedliwiający przetwarzania danych biometrycznych. Sąd stwierdził m.in., że „ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. (…) wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania".

W związku z zapadłym orzeczeniem pojawia się pytanie o konsekwencje praktyczne stanowiska zaprezentowanego przez Naczelny Sąd Administracyjny.

Z wyroku NSA z dnia 1 grudnia 2009r. nie można wywodzić, że poszukiwanie przesłanek legalizujących przetwarzanie danych biometrycznych pracowników w art. 23 ust. 1 u.o.d.o. jest zawsze błędne i sprzeczne z prawem. Sąd nie stwierdził bowiem, że pracodawca w żadnym przypadku nie ma prawa pozyskiwać innych danych osobowych pracownika niż wymienione w Kodeksie pracy. Z referowanego orzeczenia nie można wywieść generalnego wniosku, że przesłanki wymienione w art. 23 ust. 1 u.o.d.o. nie znajdują zastosowania do przetwarzania danych osobowych w stosunkach pracy. Wyrażenie zgody przez dysponenta danych to tylko jedna z okoliczności legalizujących przetwarzanie danych, określonych w art. 23 ust. 1 u.o.d.o. Prócz zgody dysponenta danych administrator może powoływać się na niezbędność przetwarzania ze względu na realizowanie uprawnienia lub spełnianie obowiązku wynikającego z przepisu prawa (ust. 1 pkt 2), realizowanie umowy lub podjęcie działań przed jej zawarciem z dysponentem danych (ust. 1 pkt 3), realizowanie prawem określonych zadań dla dobra publicznego (ust. 1 pkt 4) oraz usprawiedliwiony cel administratora danych (ust. 1 pkt 5). Wymaga podkreślenia fakt, iż przesłanki wymienione w u.o.d.o. są równoprawne[23], a każda z nich jest autonomiczna i niezależna[24]. Wystarczy wystąpienie jednej z nich, by przetwarzanie danych mogło być uznane za usprawiedliwione.

Jak wynika z przedstawionego wyżej rozstrzygnięcia NSA, wyrażona na prośbę pracodawcy zgoda pracownika na przetwarzanie jego danych biometrycznych może zostać oceniona jako niedobrowolna i udzielona w sytuacji braku faktycznej swobody podjęcia autonomicznej decyzji. W świetle omawianego orzeczenia wydaje się, że możliwym rozwiązaniem legalizującym przetwarzanie przez pracodawcę danych biometrycznych pracowników (a więc przetwarzanie w zakresie szerszym niż przewidziany w Kodeksie pracy) jest powołanie się na pozostałe przesłanki wymienione w art. 23 ust. 1 zawarte w treści punktów 2-3

[23] Tak J. Barta, P. Fajgielski, R. Markiewicz *Ochrona …….*, s. 433.

[24] Wyrok WSA w Warszawie z dnia 19 lipca 2007r., II SA/Wa 678/07, LEX nr 368229; wyrok WSA w Warszawie z dnia 1 grudnia 2005r., II SA/Wa 917/05, LEX nr 189823.

i 5 u.o.do. Jedną z nich może być usprawiedliwiony cel zakładu pracy (pod warunkiem jednak, iż przetwarzanie nie narusza praw i wolności pracownika). Pracodawca musiałby każdorazowo ocenić, czy w konkretnych okolicznościach jego interes jest rzeczywiście usprawiedliwiony, jednocześnie konfrontując go z interesem podmiotu danych w zachowaniu jego podstawowych praw i wolności[25]. Wydaje się zatem, że zasadnym mogłoby więc być podnoszenie jako argumentów uzasadniających przetwarzanie danych biometrycznych m.in. zapewnienie bezpieczeństwa pracy, kontrola dostępu do tajnych informacji lub niebezpiecznych materiałów[26] (czyli zapewnienie ochrony szczególnie wrażliwych miejsc na terenie zakładu pracy) czy zapobieganie zachowaniom mogącym powodować groźne w swych skutkach wypadki na terenie zakładu pracy.

Warto nadmienić, że do dnia wydania omawianego wyroku, dokonując wykładni art. $22^1$ k.p. w związku z art. 23 ust. 1 u.o.d.o. i badając wzajemne relacje powyższych przepisów, komentatorzy dochodzili do odmiennych wniosków. Pierwsze stanowisko dowodziło tezy, iż przesłanki legalizujące przetwarzanie danych osobowych wymienione w art. 23 ust. 1 u.o.d.o. znajdują zastosowanie w odniesieniu do przetwarzania danych osobowych pracowników[27]. Przeciwny pogląd reprezentował m.in. Generalny Inspektor argumentując, że pracodawca może żądać od pracownika podania danych tylko w takim zakresie, jaki został wskazany w treści art. $22^1$ k.p. Kwestia udostępnienia pracodawcy innych danych niż określone w tym przepisie musi być uregulowana w odrębnym przepisie prawa. Jeśli tak nie jest, pracodawca nie może żądać od pracownika ich podania. Artykułu 23 ust 1 u.o.d.o. nie stosuje się ze względu na treść art. $22^1$ § 5 k.p., dotyczącego dopuszczalności przetwarzania danych. Innymi słowy Kodeks pracy wyłącza możliwość przetwarzania danych osobowych z powołaniem się na przesłanki legalizujące określone w ustawie o ochronie danych osobowych, a zatem art. 23 ust. 1 u.o.d.o. w całości nie znajduje zastosowania do przetwarzania danych pracowniczych[28].

---

[25] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 85-87.

[26] Wypowiedź Generalnego Inspektora z wywiadu przeprowadzonego przez Ł. Guzę *Wariograf w firmie zakazany*, Gazeta Prawna z 12 sierpnia 2010r., nr 156.

[27] G. Spytek – Bandurska, *Wybrane problemy pracodawców ze stosowaniem przepisów o ochronie danych osobowych* [w:] T. Wyka, A. Nerka (red.) *Granice ochrony danych osobowych w stosunkach pracy*, Warszawa 2009, s. 25, 39; w odniesieniu do samej zgody legalizującej pozyskiwanie od kandydatów na pracowników danych osobowych podobnie wypowiadają się A. Patulski, G. Orłowski, *Informacja o karalności kandydata na pracownika*, Monitor Prawa Pracy 2004, nr 7, s. 195.

[28] Podobnie G. Sibiga, *Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy*, Radca Prawny 2005, nr 2, s. 69; I. Walencik *Sprawdzanie niekaralności. Ochrona pracownika ponad interesem pracodawcy*, Rzeczpospolita z 10 maja 2004r., nr 108.

Jak się wydaje, w referowanym wyroku Naczelny Sąd Administracyjny zajął pośrednie stanowisko. Opiera się ono na stwierdzeniu, że w relacji pomiędzy pracodawcą a pracownikiem zgoda wyrażona przez pracownika generalnie nie legalizuje przetwarzania (w tym również pozyskiwania) danych osobowych. Analizując stan faktyczny sprawy sąd orzekł, iż w tej konkretnej sytuacji zgoda pracowników nie może stanowić podstawy do zgodnego z prawem przetwarzania przez pracodawcę danych biometrycznych. Z uzasadnienia wyroku wywieść można następujący wniosek – pozostałe przesłanki z art. 23 ust. 1 u.o.d.o., pod warunkiem uwzględnienia zasady adekwatności, mogą legalizować pozyskiwanie danych od pracownika.

W świetle omawianego orzeczenia warto zastanowić się, czy w niektórych sytuacjach faktycznych zgoda pracownika mogłaby zostać uznana za legalizującą przetwarzanie danych biometrycznych przez pracodawcę? Na tak postawione pytanie można byłoby udzielić odpowiedzi twierdzącej w konkretnych sytuacjach, w których pracodawca jest w stanie bezsprzecznie wykazać, że zgoda udzielona przez pracownika była w zupełności dobrowolna i niewymuszona. Jednym z warunków uznania takiej zgody za stanowiącą podstawę przetwarzania danych byłaby również okoliczność, iż pracownik może ją odwołać w każdym czasie bez niebezpieczeństwa powstania niekorzystnych dla siebie skutków w zakresie stosunku pracy łączącego go z pracodawcą[29].

Idąc dalej w kierunku rozstrzygania analogicznych spraw w praktyce, wydaje się, że decydująca mogłaby być reakcja pracodawcy w sytuacji, gdy pracownik proszony o wyrażenie zgody na pobranie i przetwarzanie jego danych biometrycznych faktycznie jej nie udzieli. Powyższe sprowadza się do pytania, czy pracodawca mógłby potraktować takie zachowanie pracownika jako przyczynę uzasadniającą utratę zaufania względem niego i wypowiedzieć temu pracownikowi umowę o pracę? Jeśli praktyka orzecznicza wypracowałaby pogląd, iż nie wyrażenie przez pracownika zgody na przetwarzanie jego danych osobowych (nie tylko biometrycznych), nie może stanowić podstawy do rozwiązania stosunku pracy przez pracodawcę, zasadne byłoby twierdzenie o dobrowolności oświadczenia woli w tym przedmiocie. Nieuzasadnione w takiej sytuacji byłyby argumenty o braku swobody przy wyrażaniu zgody przez pracownika czy jego niekomfortowej sytuacji względem pracodawcy. Wtedy też próby podważania zgody udzielonej przez pracownika, jako przesłanki legalizującej przetwarzanie jego danych biometrycznych, miałyby niewielkie szanse powodzenia.

[29] Więcej na temat problematyki zgody osoby, której dane dotyczą zob. M. Jagielski, *Prawo do …*, s. 103 i n.

Należy zwrócić uwagę, że dotychczasowe podejście reprezentowane przez Generalnego Inspektora w kwestii, której dotyczy referowany wyrok było dalej idące niż stanowisko przedstawione przez NSA. Generalny Inspektor w decyzji z dnia 19 maja 2006r. (GI-DEC-DIS-163/06/481) stwierdził, że „żądanie podania danych jest możliwe wyłącznie na podstawie regulacji kodeksowej, nie znajdują zastosowania przesłanki wymienione w art. 23 ust. 1 u.o.d.o., w tym zgoda osoby, której dane dotyczą na przetwarzanie danych osobowych". Na podstawie omawianego rozstrzygnięcia NSA, można stwierdzić, że opinia Generalnego Inspektora nie została w całości podzielona przez sąd.

Aktualne natomiast w świetle analizowanego orzeczenia NSA pozostaje stanowisko doktryny, poddające w wątpliwość sens ustawowego ograniczenia zakresu danych, które administrator ma prawo przetwarzać w sytuacji, gdy możliwe byłoby rozszerzenie tego katalogu na podstawie zgody dysponenta danych. „Wydaje się, że dopuszczenie przetwarzania danych na podstawie zgody w sytuacji, gdy przepisy ograniczają zakres przetwarzania danych, pozbawia sensu wspomniane ograniczenie, w szczególności wówczas, gdy osoba, której dane dotyczą, pozostaje w układzie podległości względem podmiotu, któremu zgoda ma być udzielona"[30].

Zgodnie z uzasadnieniem wyroku, dla oceny konkretnego stanu faktycznego, prócz dopuszczalnych warunków przetwarzania danych osobowych (w tym również ich pozyskiwania) określonych w art. 23 ust. 1 u.o.d.o., za każdym razem zbadać należy także cel, jakiemu służyć ma przetwarzanie danych. Ponieważ te dwa czynniki (przesłanka przetwarzania danych oraz cel przetwarzania), pozostające we wzajemnym związku, decydować będą w danej sytuacji o uprawnieniu administratora do zbierania i przetwarzania danych biometrycznych, koniecznym jest przybliżenie zasady adekwatności.

## 4. Zasada adekwatności przy przetwarzaniu biometrycznych danych osobowych

Mając na uwadze powyższe rozważania, uzasadnione jest omówienie zasady adekwatności, która odgrywa znaczącą rolę przy ocenie prawidłowości przetwarzania danych biometrycznych.

Obowiązek przetwarzania danych adekwatnych w stosunku do celów, w jakich są przetwarzane, to nakaz wynikający z zasady proporcjonalności (adekwatności, relewantności) wyrażonej w art. 26 ust. 1 pkt 3 u.o.d.o. Jest ona jedną

[30] P. Fajgielski *Zgoda na przetwarzanie danych osobowych* [w:] G. Sibiga, X. Konarski (red.) *Ochrona .....*, s. 47; podobnie G. Sibiga *Przetwarzanie i ochrona...*, s. 70-71.

z pięciu zasad przetwarzania danych osobowych opisanych w Rozdziale 3 ustawy o ochronie danych osobowych, stanowiących jednocześnie obowiązki administratora, których musi on zawsze przestrzegać[31]. Zgodnie z zasadą adekwatności administrator danych winien przetwarzać w zgodzie z obowiązującym prawem tylko tego rodzaju dane i o takiej treści, które są konieczne ze względu na cel ich zbierania. Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy dobrem dysponenta danych a interesem administratora danych, który dane te przetwarza. Powyższe oznacza, że administrator nie może przetwarzać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym niż uzasadniony tym celem stopniu szczegółowości. „Równowaga będzie zachowana, jeśli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne dla osiągnięcia celu, w jakim dane są przez niego przetwarzane" (wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005r., sygn. akt II SA/Wa 917/2005, LEX 189823). Jeśli administrator danych domaga się więcej praw aniżeli przewidują obowiązujące przepisy prawa, następuje zachwianie równowagi na korzyść administratora, a zatem następuje bezpodstawne ograniczenie praw osoby, której dane dotyczą.

Warto odwołać się w tym miejscu do poglądu Grupy Roboczej wyrażonego w „Dokumencie roboczym w sprawie biometrii", traktującego o zasadzie adekwatności. „Ocena poszanowania zasady proporcjonalności jest niezbędna i musi być wykonywana z uwzględnieniem ryzyka dotyczącego swobód i fundamentalnych praw obywatelskich, chodzi zwłaszcza o ustalenie, czy poszukiwany cel nie mógł być osiągnięty w sposób mniej inwazyjny". Jak wynika z powyższego, zasada proporcjonalności nakazuje, by cel przetwarzania danych przez administratora był proporcjonalny do uciążliwości wobec dysponenta danych, spowodowanych przez przetwarzanie jego danych[32]. Konsekwencją zasady adekwatności jest obowiązek odrzucenia celów przetwarzania, które mogą zostać osiągnięte wyłącznie w sposób nadmiernie uciążliwy do wartości realizowanego celu[33]. Należy zaznaczyć, iż podobnie na gruncie polskiego ustawodawstwa wypowiedział się Trybunał Konstytucyjny w wyroku z dnia 12 grudnia 2005r. (sygn. K 32/2004, OTK-A 2005, nr 11, poz. 132). Stwierdził on, iż „konieczność w demokratycznym państwie prawnym to zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób lub stopniu, który nie mógłby być

[31] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona ……*, s. 501.

[32] A. Drozd, *Prawo podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, Warszawa 2004, s. 120.

[33] K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999r, s. 152.

osiągnięty przy zastosowaniu innych środków, a jednocześnie winny być to środki jak najmniej uciążliwie dla podmiotów, których prawo lub wolność ograniczają".

W ustawie o ochronie danych osobowych ustawodawca użył zwrotu niedookreślonego, zgodnie z którym przetwarzane dane winny być „adekwatne w stosunku do celów". Brak jest jednak jakichkolwiek wskazówek, jak „adekwatność" ustalać. W praktyce powoduje to wiele wątpliwości interpretacyjnych odnoszących się do istniejących stanów faktycznych. Odniesieniem dla administratorów danych mogą być jedynie decyzje, oceny i wypowiedzi Generalnego Inspektora bądź też wyroki sądów traktujące o konkretnych okolicznościach i możliwości zakwalifikowania ich jako adekwatne bądź nieadekwatne zbieranie danych. Dla przykładu za sprzeczne z zasadą adekwatności uznane zostało: zbieranie danych w zakresie wizerunku, rysopisu, imion rodziców, miejsca urodzenia, poprzednich adresów zameldowania, informacji o dzieciach oraz kategorii i dacie nadania uprawnienia do prowadzenia pojazdów dla celów zawarcia i realizacji umowy leasingu (cytowany wyżej wyrok WSA w Warszawie z dnia 1 grudnia 2005r., sygn. akt II SA/Wa 917/2005) oraz zbieranie danych o wykształceniu i stanie cywilnym przy zawieraniu umów odpowiedzialności cywilnej posiadacza pojazdu mechanicznego (wyrok NSA z dnia 5 lutego 2003r., sygn. akt II SA 3505/01, Gazeta Prawna 2002, nr 27, s. 16). Za adekwatne do celu i prawidłowe uznane natomiast zostało odnotowywanie imienia, nazwiska oraz numeru dokumentu (podstawowych danych służących identyfikacji osoby), po to, by poprawić bezpieczeństwo budynku (wyrok WSA w Warszawie z dnia 12 maja 2005r., II SA/Wa 2499/04, niepubl.).

Każdorazowo administrator samodzielnie musi podejmować decyzję, czy wyznaczony cel jest adekwatny i usprawiedliwia w jego przypadku przetwarzanie danych. Jak konstatuje NSA w wyroku z dnia 27 listopada 2003r. (II SA 209/03, niepubl.), w każdym wypadku należy oceniać czy w konkretnym stosunku, w związku z którym administrator danych przetwarza dane, przetwarzanie danych osobowych następuje z uwzględnieniem art. 26 ust. 1 pkt 3, a więc w sposób zgodny z zasadą adekwatności. Administrator winien przeprowadzić ocenę stanu faktycznego odwołującą się do wartości usprawiedliwiających jego interesy i uwzględniającą jednocześnie konieczność dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Podmiot decydujący o celach i środkach przetwarzana danych musi przy tym pamiętać, iż naraża się na odmienną interpretację sądu oraz Generalnego Inspektora.

Koniecznym jest podkreślenie, iż zasada proporcjonalności, jako najważniejsza z zasad ochrony danych w odniesieniu do danych biometrycznych, w praktyce oceniana jest odmiennie w różnych krajach. I tak np. w Danii posługiwanie się danymi biometrycznymi przy nabyciu biletów na prom jest zasadne, a w Grecji nie

wyrażono zgody na używanie systemu identyfikacji biometrycznej przy odprawie pasażerów na lotnisku[34].

Reasumując – cel, jakim jest przykładowo ochrona tajemnicy państwowej, bezpieczeństwo państwa czy obywateli (ochrona dostępu do urządzeń nuklearnych lub do tajemnicy produkcji państwowego sprzętu wojskowego), niewątpliwie ocenić można jako nadrzędny, zezwalający na przetwarzanie danych biometrycznych pracowników. Niejednokrotnie jednak ocena danej sytuacji występującej w praktyce, np. ochrona szczególnie wrażliwych miejsc w zakładzie pracy (serwerowni, sejfów, czy miejsc, w których znajdują się tajne dokumenty), będzie problematyczna. Zasada adekwatności opiera się bowiem na każdorazowym wartościowaniu i subiektywnej ocenie, odnosząc się do niezbyt ścisłych kryteriów[35]. Jedynym poziomem oceny jest „adekwatność" zakresu przetwarzanych danych w stosunku do celu ich przetwarzania. Na podstawie omawianego wyroku jedno jest bezsporne – przetwarzanie danych biometrycznych pracowników, na podstawie ich zgody, celem ewidencjonowania czasu pracy, jest sprzeczne z prawem.

Na chwilę obecną zauważyć należy, iż w praktyce istotnymi wytycznymi w sprawie przetwarzania przez pracodawców danych biometrycznych pracowników są wypowiedzi Generalnego Inspektora, wskazujące na występowanie w praktyce sytuacji usprawiedliwiających przetwarzanie danych biometrycznych pracowników. Zgodnie z opinią Generalnego Inspektora są nimi np. ochrona miejsc, w których przechowywane są materiały niebezpieczne, wybuchowe, radioaktywne, wirusy, bakterie, tajemnice prawnie chronione, tajemnice przemysłowe, czy know-how przedsiębiorstwa[36]. W takich okolicznościach dane biometryczne pracowników mogą być przetwarzane z uwagi na uzasadniony interes przedsiębiorstwa i bezpieczeństwo zakładu pracy, a Generalny Inspektor aprobuje ich wykorzystanie biorąc pod uwagę celowość przetwarzania tych danych.

---

[34] Za J.P. Walter, *Niektóre aspekty ochrony danych przy posługiwaniu się danymi biometrycznymi w sektorze prywatnym*, [w:] *Prawo do prywatności – prawo do godności*: 26 Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych, 14-16 września 2004 Polska, Wrocław/ zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych", Warszawa 2006, s. 269.

[35] J. Barta, P. Fajgielski, R. Markiewicz *Ochrona ……*, s. 508.

[36] Opinia Generalnego Inspektora Wojciecha R. Wiewiórowskiego wygłoszona podczas wykładu wprowadzającego do IX Forum ADO/ABI odbywającego się w Warszawie w dniu 16 listopada 2010 r.

## 5. Podsumowanie

Bezsprzecznym pozostaje, iż konieczne jest pogodzenie w praktyce interesów pracodawcy, jako administratora danych osobowych i ochrony prywatności pracownika – dysponenta danych. Winno to nastąpić poprzez dostosowanie przepisów prawnych związanych z zatrudnieniem do potrzeb dyktowanych przez rynek pracy oraz możliwości rozwoju technologicznego przedsiębiorstw.

Analiza omówionego orzeczenia NSA, jak również treści art. $22^1$ k.p., skłaniają do wniosku, że postulowany przez środowiska pracodawców mniejszy rygoryzm w określeniu możliwości pozyskiwania przez pracodawcę danych o pracownikach może wywołać zarówno dobre, jak i złe skutki. Mógłby przyczynić się do lepszego dopasowania profilu osób zatrudnionych do potrzeb przedsiębiorstwa, z drugiej jednak strony spowodować np. większe bezrobocie wśród osób skazanych (przy wprowadzeniu możliwości pozyskiwania przez wszystkich pracodawców informacji o niekaralności pracowników i kandydatów do pracy). Warunkiem wprowadzanych zmian, prócz wcześniejszej rzetelnej ich analizy i konsultacji m.in. z kryminologami, socjologami, czy psychologami, powinna być dbałość o przestrzeganie przez administratorów danych - pracodawców, zasad celowości i adekwatności, tak by nie wkraczać zbyt głęboko w sferę prywatności pracownika. Wypada również zwrócić uwagę na należyte zabezpieczenie przetwarzanych danych, w szczególności danych biometrycznych, oraz jak najlepsze przygotowanie merytoryczne osób upoważnionych do przetwarzania danych osobowych w przedsiębiorstwach.

Miejmy nadzieję, że w niedalekiej przyszłości odpowiedzi na pojawiające się z biegiem czasu pytania będziemy mogli szukać również w orzecznictwie, którego dorobek w omawianej w niniejszym opracowaniu materii jest obecnie niewielki. Wymaga w tym miejscu podkreślenia, że postulat zmiany przepisów prawnych dotyczących przetwarzania danych osobowych pracowników, nie dotyczy jedynie przepisów Kodeksu pracy, lecz odnosi się również do innych aktów prawnych. Są nimi m.in. ustawa o Krajowym Rejestrze Karnym[37] oraz ustawy będące pragmatykami służbowymi (np. ustawa o pracownikach samorządowych[38], ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[39]).

---

[37] Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2008r. Nr 50, poz. 292 z późn. zm.).

[38] Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz. U. z 2008 r. Nr 223, poz. 1458 z późn. zm.).

[39] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154).

Anachroniczna treść art. 22[1] Kodeksu pracy stała się przyczyną sporu zakończonego przedstawionym w niniejszej publikacji wyrokiem NSA, a także wystąpienia Generalnego Inspektora skierowanego do Ministra Pracy i Polityki Społecznej[40]. Generalny Inspektor w swoim piśmie zasugerował konieczność wprowadzenia jednoznacznych uregulowań prawnych dotyczących spraw dostępu pracodawcy do informacji na temat pracownika. Stanowiska Generalnego Inspektora nie podzieliła jednak Minister Pracy[41], argumentując, iż Kodeks pracy zawiera regulacje stanowiące podstawowe prawa i obowiązki w dziedzinie zatrudnienia odnoszące się, co do zasady, do wszystkich pracowników. Natomiast w przepisach innych ustaw zawarte są szczegółowe rozwiązania dotyczące konkretnych sfer działalności oraz regulujące specyficzne prawa i obowiązki pracownicze (np. ustawa o transporcie drogowym[42], ustawa o służbie cywilnej[43]). Według Minister Pracy zakres danych osobowych zawarty w Kodeksie pracy jest wystarczający, a w innych przepisach niemożliwe jest dokładne określenie procedur związanych z pozyskiwaniem od pracownika jego danych osobowych.

Omówiony w niniejszym opracowaniu wyrok Naczelnego Sądu Administracyjnego doprowadził do podjęcia debaty w przedmiocie wprowadzenia zmian w przepisach prawa związanych z zatrudnieniem, a dotyczących danych osobowych, w tym danych biometrycznych. Dostrzeżono konieczność dyskusji na temat wprowadzenia rozwiązań mających na celu dostosowanie ustawodawstwa do realnych zjawisk społecznych związanych ze świadczeniem pracy, w którą aktywnie włączył się Generalny Inspektor wybrany na IV kadencję[44].

[40] Pan Michał Serzycki w styczniu 2010 r. wystąpił do Ministra Pracy i Polityki Społecznej – Pani Jolanty Fedak o podjęcie prac legislacyjnych nad zmianą przepisów regulujących przetwarzanie danych osobowych pracowników (kandydatów do pracy) przez pracodawców (DOLiS-035-416/09), http://www.giodo.gov.pl/575 /id_art/3299/j/pl.

[41] Odpowiedź Pani Jolanty Fedak z dnia 9 marca 2010 r. (DPR-I-4102-119-JS/MK/BL/10), http://www.giodo. gov.pl/575 /id_art/3299/j/pl.

[42] Ustawa z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2007r. Nr 125, poz. 874 z późn. zm.).

[43] Ustawa z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2008r. Nr 227, poz. 1505 z późn. zm.).

[44] Od 4 sierpnia 2010 r. funkcję Generalnego Inspektora pełni Pan Wojciech R. Wiewiórowski.

# PROCESSING OF BIOMETRIC INFORMATION OF EMPLOYEES IN THE LIGHT OF THE DECISION OF THE SUPREME ADMINISTRATIVE COURT DATED DECEMBER 1, 2009 (I OSK 249/09)

The decision of the Supreme Administrative Court1 dated December 1, 2009 ( I OSK 249/09, LEX 553777) is the first ruling which raises the issue of processing biometric information of an employee by the employer in regard to Polish law. It is, therefore, of profound significance and calls for thorough analysis.

As a result of advancement in new technologies and means of communications over the past few years, as well as progress in the development of practices of work performance, the provisions of law in force applicable to personal data processing in employment relationships (Article 221 of Labour Code, in particular) have been out of touch with the demands of the contemporary world.

The decision of the Supreme Administrative Court (hereinafter referred to as "SAC") dealt with the relation between the provisions of Labour Code and Personal Data Protection Act, combined with the issue of biometric information and the positions of respective parties in the employment relationship. In its decision of December 1, 2009, SAC ruled on collection of biometric information of employees (employee fingerprints) by employers upon prior written consent of the employees in question. In the case concerned biometric information was being processed for the purpose of working time registration at the workplace. It seems that SAC assumption that an employee who was asked to give consent for processing his personal data (biometric information in this specific case) was in an inconvenient situation was fundamental to the decision on the case in question. Employee is dependent on his employer as an entity to which consent shall be given. Therefore, the employee's freedom to give consent or not is questionable in principle. SAC concluded that for the aforementioned reasons, the catalogue of data that employer was allowed to require from the employee was limited in the Labour Code. Furthermore, the Supreme Administrative Court stated in the justification for the decision that the practice of invoking the consent given by an employee in order to support extension of the scope of personal data catalogue defined in the Labour Code was in conflict with the principle of appropriateness (proportionality). The Court pointed out that it was the principle of proportionality that represented the essential criterion applicable to biometric information processing. In the presented case the purpose, namely, control over employee

[1] Naczelny Sąd Administracyjny – NSA.

working time was deemed inappropriate and failing to justify biometric information processing.

It follows from the decision of SAC that employee's consent to process his biometric information which is given upon employer's request may be assessed as being involuntary and given in the circumstances of actual lack of freedom to take an independent decision. It seems, in the light of the presented decision, that invoking these prerequisites listed in the Personal Data Protection Act which are other than consent of biometric information holder is a solution possible for validating the processing of biometric information of employees - thus processing it to a more extensive degree than it is allowed based on the Labour Code. A justified purpose of the workplace may be one of such prerequisites, on condition, however, that data processing neither violates employee rights, nor employee freedom.

As provided in the justification for the Court decision, for the purpose of assessing specific state of affairs, each time the purpose that data processing is supposed to serve should be investigated in addition to the permissible conditions of personal data processing (as well as personal data collection) that are defined in the Personal Data Protection Act. The prerequisite which legitimizes data processing and the purpose of data processing are interrelated and are decisive in a given situation for the right of data administrator to collect and process biometric information.

Presently, it should be pointed out that the statements of Inspector General for Personal Data Protection2 in practice constitute important guidelines for processing biometric information of employees by employers. These guidelines indicate that there actually are situations which justify processing of biometric information of employees. In accordance with Inspector General's opinion these situations include, for example, the need to protect places in which hazardous materials, explosive materials, radioactive materials, viruses, bacteria, legally protected secrets, industrial secrets or know-how of a company are stored. Biometric information of employees may be processed in such circumstances because of justified interest of the company and safety at the workplace and the Inspector General approves the use of biometric information considering the advisability of processing the said information.

[2] Generalny Inspektor Ochrony Danych Osobowych (also referred to as Information Commissioner).