Zeszyty Naukowe Towarzystwa Doktorantów UJ
Nauki Ścisłe, Numer 17 (2/2018), s. 45–60
e-ISSN 2082-3827 | p-ISSN 2084-977X
www.doktoranci.uj.edu.pl/zeszyty/nauki-scisle
DOI: 10.26361/ZNTDSc.09.2018.17.02

Weronika Kupny

Uniwersytet Jagielloński
Wydział Prawa i Administracji
Katedra Prawa Pracy i Polityki Społecznej
e-mail: weronika.kupny@gmail.com

Ochrona prywatności w miejscu pracy w erze dynamicznie rozwijających się technologii

Streszczenie

Prawo do prywatności zaliczane jest do podstawowych praw człowieka i jako takie jest przedmiotem większości współczesnych ustawodawstw. Systemy prawne rozbudowują w znaczącym zakresie instrumenty prawa ochrony prywatności, ale jednocześnie znajdują powody, aby w tę sferę mocno ingerować. Z pewnością dynamiczny rozwój nowoczesnych technologii nie ułatwia prawodawcy znalezienia kompleksowego rozwiązania. Artykuł podejmuje tematykę ochrony prywatności w ramach stosunku pracy w kontekście innowacyjności i rozwoju technologii. W niniejszym opracowaniu autorka dokonała porównania wpływu nowoczesnych technologii w miejscu pracy dziś, w świetle obowiązujących przepisów, i jutro – wobec uchwalonego rozporządzenia (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz zniesienia dyrektywy 95/46 / WE (ogólne rozporządzenie o ochronie danych).

Słowa kluczowe

przetwarzanie danych osobowych, prawo do prywatności, ochrona danych osobowych, ogólne rozporządzenie o ochronie danych, zatrudnienie pracownicze

I

Z danych osobowych płynie szereg ochronnych praw dla osób fizycznych od chwili urodzenia aż do śmierci. Dotyczy to praw, które często są realizowane wraz z brakiem wiedzy administratorów, wykorzystujących swoją pozycję rynkową albo fakt pewnych ułomności prawnych. Życie prywatne to życie osobiste i rodzinne, możliwość wyrażania własnych myśli i opinii czy przynależność do określonej grupy wyznaniowej. Prywatność tak rozumiana różni się od prywatności, z którą spotykamy się w miejscu pracy. Ta z reguły jest bardzo mocno ograniczona. Wynika to bowiem z charakteru i organizacji pracy. W dobie cyfryzacji i coraz powszechniejszego wykorzystywania *Big Data* technologicznie możliwe jest większe wykorzystywanie danych osobowych przez pracodawców. Przedsiębiorcy coraz częściej sięgają po cyfrowe urządzenia pomagające im unowocześnić model zarządzania. Oferują one wiele dodatkowych „udogodnień", jak możliwość zlokalizowania miejsca pobytu pracownika, kontrolowania i monitorowania aktywności pracownika czy jego poczty służbowej. Z drugiej strony urządzenia te pozwalają na zapewnienie bezpieczeństwa i ochrony mienia (pomieszczeń i urządzeń) czy wykrycie wszelkiego rodzaju naruszeń obowiązku zachowania w tajemnicy informacji stanowiących część kapitału przedsiębiorcy[1]. Jednakże często pracodawcy, decydując się na stosowanie technologii, zapominają o konieczności przestrzegania zasad legalności i adekwatności w stosunku do celu przetwarzania danych[2].

W historii ochrony danych osobowych w Polsce rok 2017 był okresem szczególnym. To nie tylko czas jubileuszu 20-lecia prawa do ochrony danych osobowych, ale też okres przygotowań naszego kraju do rozpoczęcia stosowania ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[3]. Od 25 maja rozporządzenie to stanowi wyjściowy akt regulujący ochronę danych osobowych na terenie Unii Europejskiej, w tym w Polsce. Jednocześnie polski ustawodawca dokonał zmian w ponad 130 aktach prawnych, które w swojej treści traktują o danych osobowych, w tym także w Kodeksie pracy[4].

Autor niniejszego artykułu w dalszej części podejmuje się zarówno analizy, czy i w jakim zakresie uchwalone przepisy w powiązaniu z przepisami RODO

---

[1] D. Dörre-Kolasa, *Monitoring w miejscu pracy a prawo do prywatności*, „Praca i Zabezpieczenie Społeczne" 2004, nr 9, s. 10–12.

[2] M. Barański, M. Giermak, *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego (uwagi de lege ferenda)*, „Państwo i Prawo" 2017, nr 9, s. 90–91.

[3] Rozporządzenie 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 (RODO), Dz. Urz. UE L 119, s. 1.

[4] M. Frąckowiak, T. Świeboda, *Ochrona danych osobowych pracownika w perspektywie RODO i przepisów dotyczących monitoringu wizyjnego stosowanego przez pracodawcę*, „MOPR" 2018, nr 7, s. 8 i n.

uwzględniają zasadnicze zgłoszone przez doktrynę postulaty co do zmiany przepisów dotyczących przetwarzania danych pracowników, jak i poddaje przeglądowi nowe przepisy z zakresu nowoczesnych technologii.

II

Czy kiedykolwiek spróbowaliśmy dokonać analizy, w świetle obowiązujących przepisów, w jaki sposób zarządzamy własnymi danymi osobowymi? Dane osobowe przynależne jednostce są niezwykle cenną własnością. Często z własnością identyfikujemy samochód, dom, mieszkanie czy komputer, a zapominamy, że każdy z nas jest właścicielem bardzo cennego towaru. To coś nazywa się prywatnością. Prawo do prywatności jest wyspecjalizowaną postacią ochrony danych osobowych. Za ojczyznę prawa do prywatności powszechnie uważa się Stany Zjednoczone. Dwaj amerykańscy profesorowie prawa – Samuel D. Warren i Louis D. Brandeis – uznali, że prawo do prywatności to prawo do bycia pozostawionym w spokoju, uprawnienie do wyłączności, odrębności, tajemnicy i samotności (*the right to be let alone*)[5]. O tym, jak bardzo ważne jest to prawo, przekonuje nas szereg regulacji międzynarodowych, europejskich i prawa krajowego.

Z regulacji europejskich najistotniejszą rolę odgrywa art. 16 Traktatu o funkcjonowaniu UE[6], bowiem elementarnym prawem każdej osoby w ramach UE jest prawo do ochrony danych osobowych. Prawo to wpisuje się w prawo do prywatności, które zagwarantowane jest również w konwencji praw człowieka[7], deklaracji praw człowieka[8], a także w szeregu innych aktów[9]. Na płaszczyźnie polskiego porządku prawnego prawo do prywatności i jego atrybut: prawo do ochrony danych osobowych, podniesione zostały do rangi praw konstytucyjnych. Wynikające z art. 47 Konstytucji[10] prawo do ochrony prawnej życia prywatnego zapewnione jest w zakresie prawa do ochrony danych osobowych przez art. 51[11] ustawy zasadniczej. Przepis ten gwarantuje ochronę danych, opierając się na zasadzie

---

[5] S. D. Warren, L. Brandeis, *The Right to Privacy*, "Harvard Law Review" 1890, Vol. IV, s. 193–220.

[6] Dz. Urz. UE C 326, 26/10/2012 P. 0001–0390.

[7] Art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności z 4 listopada 1950 r., zmienionej następnie Protokołami 3, 5 i 8 oraz uzupełnionej Protokołem nr 2, DzU z 1993 r., nr 61, poz. 284 ze zmianami.

[8] Art. 12. Powszechnej Deklaracji Praw Człowieka z 10 grudnia 1948 r.

[9] Art. 16 i 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych ONZ z 16 grudnia 1966 r., DzU z 1997 r., nr 38, poz. 167; art. 1 Konwencji Nr 108 Rady Europy z 28 stycznia 1981 r., DzU nr 5, poz. 24 ze zmianami; art. 12 Międzynarodowego Paktu Praw Gospodarczych, Społecznych i Kulturalnych z 16 grudnia 1966 r.

[10] DzU nr 78, poz. 483 ze zmianami.

[11] M. Wujczyk, *Prawo pracownika do ochrony prywatności*, Warszawa 2012, s. 159.

autonomii informacyjnej, a więc zasadzie nakładającej na każdą jednostkę obowiązek ujawniania informacji jej dotyczących w zakresie wynikającym z przepisów prawa. Musi to być jednocześnie przepis kształtowany z poszanowaniem odpowiednich wartościami[12]. Na gruncie ochrony danych osobowych do dnia 24 maja 2018 roku stosownymi przepisami była ustawa z 29 sierpnia 1997 roku[13], uzupełniana przez inne akty prawne. Ustawa ta, będąca implementacją dyrektywy 95/46/WE[14], spowodowała, że polski porządek prawny w zakresie przetwarzania danych osobowych odpowiadał standardom europejskim.

W perspektywie czasu harmonizacja dotychczasowych przepisów o ochronie danych osobowych okazała się, z punktu widzenia prawodawcy europejskiego, niewystarczająca. Dyskusja o konieczności zmiany przepisów o ochronie danych osobowych trwała od kilku lat, a od 2012 roku rozpoczęła się debata, jakie brzmienie będą miały przepisy rozporządzenia. Rzeczywistość, kiedy powstawała dyrektywa unijna, i rzeczywistość dzisiejsza to dwie różne perspektywy, a już na pewno inne rzeczywistości wirtualne. Mamy świat nowoczesnych technologii, świat przede wszystkim Internetu. Dyrektywa nie była w stanie odpowiedzieć na szereg pytań o stosowanie prawideł ochrony danych osobowych w kontekście właśnie użycia nowoczesnych narzędzi komunikacyjnych, nowoczesnych rozwiązań technicznych, informatycznych, ale też organizacyjnych. Zmieniła się organizacja pracy, modele zarządzania. To wszystko generuje ryzyko, które jeszcze w 1995 roku nie było do przewidzenia. Nastąpiła konieczność stworzenia regulacji, które będą zapewniać wyższy stopień ochrony, w szczególności przepisów o odpowiedzialności za naruszenie ochrony danych osobowych[15]. W ten oto sposób Komisja Europejska rozpoczęła prace legislacyjne nad wprowadzeniem nowych regulacji prawnych, co zostało osiągnięte dzięki powołaniu do życia RODO. Dodatkowo, polski ustawodawca uchwalił 10 maja 2018 roku ustawę o ochronie danych osobowych[16], mającą na celu zapewnienie skutecznego stosowania przepisów RODO.

---

[12] M. Siwicki, *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych (uwagi w związku z projektem rozporządzenia Parlamentu Europejskiego i Rady)*, „Państwo i Prawo" 2016, nr 3, s. 80.

[13] DzU z 2016 r. poz. 922 ze zm.

[14] Dyrektywa Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz. Urz. UE L 281, s. 31.

[15] M. Barański, M Giermak, op. cit., s. 95–96.

[16] DzU z 2018 r., poz. 1000.

III

Problematyka ochrony danych osobowych osób ubiegających się o pracę i pracowników jest uregulowana w art. 22^1 Kodeku pracy[17]. Celem wprowadzenia do polskiego systemu prawnego przepisu było nie tylko określenie podstawy żądania udostępnienia danych przez pracodawcę, lecz także ustanowienie wyraźnych granic w przetwarzaniu danych osobowych pracownika, uniemożliwiających ewentualne nadużycia. Artykuł ten, w brzmieniu sprzed nowelizacji, pełni nie tylko funkcję gwarancyjną dla kandydata do pracy/pracownika, ale w istocie mówi o prawach pracodawcy. Stosownie do art. 22^1§4 k.p. pracodawca uprawniony jest do żądania również innych danych niż określone w §1 i §2, pod warunkiem, że obowiązek ich wskazania wynika wprost z przepisów szczególnych. Przepis ten określa trzy grupy danych osobowych, których może żądać pracodawca[18]. Pierwsza grupa danych (dane dotyczące kandydata na pracownika) ujęta jest w postaci zamkniętego katalogu. Może ona zostać rozszerzona na podstawie przepisów szczególnych. Zakres danych osobowych objętych drugą grupą (dane dotyczące pracownika) zależy od indywidualnych okoliczności leżących po stronie pracownika oraz od rodzaju wykonywanej pracy, względnie od okoliczności związanych z pracodawcą. Trzecia grupa (dane dotyczące zarówno kandydata do pracy, jak i pracownika), otwarta, obejmuje dane osobowe, co do których obowiązek ich podania wynika „z odrębnych przepisów". Co więcej, pomimo że prawodawca nie dookreślił tego wyrażenia, w doktrynie przyjmuje się, że oznacza ono ustawy oraz rozporządzenia[19]. Nie podlega dyskusji, iż podmiot zatrudniający może żądać udostępnienia tylko tych informacji i danych, które zostały ujęte w komentowanym przepisie. Sporna jest jednak kwestia zgody kandydata do pracy lub pracownika jako przesłanki legalizującej czynności podejmowane przez pracodawcę. Udzielenie zgody przez pracownika w zakresie jego danych budzi liczne kontrowersje zarówno w doktrynie, jak i judykaturze, w szczególności, jeśli następuje ona z inicjatywy pracodawcy. Zgoda pracownika na przetwarzanie danych powinna być dobrowolna, a w relacji pracownik – pracodawca bywa rożnie z zachowaniem tej dobrowolności. W szczególności jej brak nie może powodować zmniejszenia uprawnień pracowniczych wynikających z obowiązujących przepisów[20]. Czynnikiem dominującym w uznaniu zgody za wyrażoną wbrew przepisom jest okoliczność faktycznego podporządkowania pracownika pracodawcy i nierówności stron. Pracownik, mając więc świadomość ewentualnych negatywnych następstw odmowy udzielania zgody na przetwarzanie danych osobowych, takiej zgodę udzieli[21].

---

[17] DzU z 2018 r., poz. 917.

[18] K. Jaśkowski, *Uwagi do art. 22^1 k.p.*, [w:] K. Jaśkowski, E. Maniewska, *Komentarz aktualizowany do Kodeksu pracy*, LEX 2018, s. 424–425.

[19] A. Sobczyk, *Kodeks pracy. Komentarz*, Warszawa 2018.

[20] A. M. Świątkowski, *Kodeks pracy. Komentarz*, Warszawa 2018.

[21] K. Jaśkowski, op. cit., s. 424–425.

Polski ustawodawca w projekcie ustawy zapewniającej bezpośrednie stosowanie RODO przewidział wprowadzenie dodatkowych regulacji w stosunku zatrudnienia. Głównym celem zmian było dostosowanie brzmienia przepisów prawa pracy do art. 6 ust. 1 lit. c RODO, który to przepis wprowadza przesłankę istnienia obowiązku prawnego jako podstawy uzyskiwania i przetwarzania danych osobowych. Nowelizacja ustawy przewidywała wzmocnienie pozycji pracodawcy. Artykuł 22^1 k.p. miał otrzymać nowe brzmienie. Postulowano rezygnację z zamkniętego katalogu danych osobowych na rzecz określenia danych, których przetwarzanie byłoby niedozwolone. Inne dane, niewymienione w katalogu danych obligatoryjnych, miałby być pobierane tylko wtedy, gdy byłoby to niezbędne do wypełnienia obowiązku pracodawcy nałożonego przepisami prawa[22]. Projekt wskazywał również, że przetwarzanie przez podmiot zatrudniający innych danych osobowych i informacji byłoby dopuszczalne tylko i wyłącznie za zgodą osoby ubiegającej się o zatrudnienie/pracownika i tylko wtedy, gdy jest to dla nich korzystne[23]. Nowelizacja ta nie miała jednak przesądzać o formie udzielonej zgody. W tym zakresie prawodawca odsyłał bezpośrednio do RODO. Dodatkowo, zgodnie z założeniami projektu, brak zgody, a także też jej wycofanie nie mogły oznaczać dla pracownika negatywnych skutków w zakresie stosunku pracy. Jednocześnie projektowane przepisy Kodeksu pracy zakładały możliwość uzyskania zgody od pracownika wyłącznie w przypadku przetwarzania danych biometrycznych – znowu jeżeli dotyczą one stosunku pracy. Sposób gromadzenia danych biometrycznych miał zostać określony przez odpowiednie rozporządzenie wykonawcze. Ostatecznie część projektowanych przepisów w zakresie katalogu danych osobowych, do żądania których uprawniony został pracodawca, regulacji w postaci monitoringu wizyjnego i skrzynki elektronicznej, znalazła się w ustawie z 10 maja 2018 roku zmieniającej Kodeks pracy[24].

IV

Kamery przemysłowe w zakładach pracy nie są niczym nowym. Zwłaszcza u większych pracodawców monitoring jest stosowny na porządku dziennym. Brakowało jednak konkretnej regulacji, w oparciu o którą nagrywanie w zakładzie pracy można było stosować. Nie było również przepisów, które wskazałyby podmiotom zatrudniającym, jak to zrobić. Monitoring aktywności pracownika jest szczególną formą kontrolowania jego zachowań. Poprzez monitoring rozumie się czynności

[22] Uzasadnienie do projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, s. 6.

[23] I. Baranowska, *Ochrona danych osobowych kandydatów do pracy i pracowników po wejściu w życie RODO. Komentarz praktyczny*, LEX/el. 2018.

[24] K. W. Baran, *Kodeks pracy. Komentarz*, Warszawa 2018.

przedsięwzięte w celu gromadzenia informacji o pracownikach, poddając ich obserwacji bezpośredniej lub z użyciem urządzeń elektronicznych[25]. Do form kontrolowania pracownika w miejscu pracy możemy zaliczyć: monitorowanie za pośrednictwem kamer z rejestracją głosu, kontrolowanie wykazów połączeń telefonicznych czy aktywności pracownika w Internecie, nagrywanie rozmów telefonicznych oraz geolokalizację[26]. Najczęściej monitoringowi poddawani są pracownicy, których narzędziem pracy jest komputer czy telefon, bowiem właśnie za pomocą systemów informatycznych umieszczonych w tych urządzeniach można najłatwiej i najpoważniej zaszkodzić pracodawcy[27]. W nowych przepisach Kodeks pracy wprost reguluje cele, sposoby wprowadzenia i zastosowania monitoringu wizyjnego, a także monitoringu poczty elektronicznej czy innych form kontrolowania.

Do monitoringu wizyjnego odnosi się nowy art. 22^2 Kodeksu pracy. Co więcej, niedopełnienie obowiązków wynikających z tych regulacji może rodzić odpowiedzialność za naruszenie przepisów o ochronie danych osobowych, tj. nałożenie administracyjnych kar pieniężnych, cywilnoprawną odpowiedzialność odszkodowawczą czy też odpowiedzialność wykroczeniową[28]. Przepisy Kodeksu pracy mówią, że pracodawca ma obowiązek organizować pracę w sposób zapewniający pełne wykorzystanie czasu pracy, jak również osiąganie przez pracowników przy wykorzystywaniu ich uzdolnień i kwalifikacji wysokiej wydajności i należytej jakości pracy oraz dbać o dobro zakładu pracy i chronić jego mienie[29]. Zgodnie z jedną z podstawowych zasad wynikających z RODO – zasadą ograniczenia celu – dane osobowe można zbierać wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach. Zatem zainstalowanie kamer w zakładzie pracy musi służyć konkretnemu celowi[30]. Regulacja przyjęta w art. 22^2 k.p. pozwala na zainstalowanie kamer, jeśli jest to niezbędne do zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji czy zachowania w tajemnicy informacji, które mogłyby narazić pracodawcę na szkodę. Kamery przemysłowe mogą się znajdować zarówno w zakładzie pracy, jak i obejmować teren wokół zakładu pracy. To ostatnie będzie szczególnie istotne, jeżeli celem pracodawcy jest zapewnienie ochrony mienia na przykład przed kradzieżą[31]. Jest jednak kilka miejsc, w których kamery nie powinny się znaleźć. Mowa tutaj o pomieszczeniach, w których toczy się życie społeczne pracowników, takich jak szatnie,

[25] K. Jaśkowski, E. Maniewska, *Komentarz aktualizowany do Kodeksu pracy*, Warszawa, LEX/el 2018.

[26] H. Szewczyk, *Ochrona dóbr osobistych w zatrudnieniu*, Warszawa 2007, s. 422 i n.

[27] D. Dörre-Kolasa, *Monitoring w miejscu pracy...*, op. cit., s. 10–12.

[28] M. Frąckowiak, T. Świeboda, op. cit., s. 8 i n.

[29] D. Dörre-Kolasa, *Monitoring pracowników*, LEX/el. 2018, komentarz praktyczny.

[30] Uzasadnienie do projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, s. 6.

[31] K. W. Baran, op. cit.

stołówka, pomieszczenia sanitarne, palarnie czy pomieszczenia udostępniane zakładowej organizacji związkowej. Wyjątkowo we wskazanych wyżej miejscach monitoring może być stosowany na przykład ze względu na kradzież czy przemoc fizyczną. Jednakże każdorazowo pracodawca powinien dołożyć należytej staranności, aby monitoring w takich miejscach nie doprowadził do naruszenia godności ani innych dóbr osobistych pracownika. Regulacje dotyczące monitoringu wizyjnego powinny się znaleźć w wewnątrzzakładowych źródłach prawa pracy, a dokładniej w układzie zbiorowym pracy lub w regulaminie pracy. Jeśli pracodawca nie jest związany żadnym PUZP ani ZUZP i nie jest zobowiązany do wydania regulaminu pracy (to znaczy gdy zatrudnia mniej niż 50 pracowników), kwestie te powinny znaleźć się w obwieszczeniu. W dokumentach tych powinny się znaleźć trzy główne kwestie: cel, zakres i sposób stosowania monitoringu[32]. Wprowadzenie odpowiednich regulacji wewnątrzzakładowych to jeszcze nie wszystko. Dodatkowo pracodawca zobowiązany jest poinformować pracowników o wprowadzeniu nagrywania w sposób przyjęty u niego (wywieszenie na tablicy ogłoszeń czy umieszczenie informacji na firmowym intranecie) nie później niż dwa tygodnie przed rozpoczęciem monitorowania. Nowo zatrudniani pracownicy powinni być informowani o tym przed dopuszczeniem do pracy. Ostatnim obowiązkiem pracodawcy, który powinien być wypełniony nie później niż jeden dzień przed rozpoczęciem monitorowania, jest odpowiednie oznaczenie pomieszczeń i terenu, na których zostały zainstalowane kamery. Oznaczenie powinno być widoczne i czytelne, przy użyciu odpowiednich znaków, infografik lub ogłoszeń dźwiękowych[33]. Choć pomiędzy opublikowaniem nowej ustawy a jej wejściem w życie minęło jedynie kilkanaście godzin, do przepisów odnoszących się do monitoringu nie przygotowano ani nie wprowadzono żadnych przepisów przejściowych. Wiadomo jednak, że od dawna pracodawcy stosują monitoring. Problem ten został ostatecznie zauważony przez Prezesa Urzędu Ochrony Danych Osobowych. W komunikacie wskazał on, że obecne systemy monitorowania powinny zostać poddane aktualizacji i dostosowane do wymogów określonych nowymi przepisami do końca września 2018 roku[34].

Kwestie monitoringu reguluje jeszcze jeden przepis, a mianowicie art. 22^3 k.p. Daje on pracodawcy możliwość kontrolowania służbowej poczty elektronicznej w celu zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi. Kontrola ta nie może jednak naruszać tajemnicy korespondencji ani innych dóbr osobistych pracownika. Szkoda, że ustawodawca nie uwzględnił regulacji

[32] E. Bielak-Jomaa, D. Lubasz, *Ogólne rozporządzenie o ochrony danych osobowych. Komentarz*, Warszawa 2018.

[33] M. Gawroński, K. Kloc, *Monitoring jako jedna z kluczowych zmian wprowadzonych przez ustawę o ochronie danych osobowych*, LEX/el. 2018.

[34] *Prezes UODO przedstawia wskazówki dotyczące monitoringu wizyjnego i zaprasza do konsultacji*, [online] https://uodo.gov.pl/pl/138/354 [dostęp: 30.06.2018].

prawnych w odniesieniu do sytuacji, gdy pracodawca będzie zezwalał na korzystanie z poczty elektronicznej do celów prywatnych czy odwrotnie – skrzynki prywatnej do celów służbowych[35]. Z pewnością taka kontrola musi być ograniczona za pośrednictwem odpowiednich narzędzi, które umożliwią wyodrębnienie części służbowej, nie naruszając w ten sposób prawa do prywatności i tajemnicy korespondencji. W świetle art. 22^3 §4 k.p. przepisy art. 22^3 §1–3 k.p. znajdują zastosowanie do innych form monitoringu niż kontrola służbowej poczty elektronicznej, z zastrzeżeniem, że ich zastosowanie jest konieczne do realizacji celów określonych w §1. Należy przyjąć, że wskazane regulacje mają zastosowanie do takich form kontroli pracownika, jak kontrola trzeźwości, monitorowanie floty GPS, odwiedzanie stron internetowych czy wysyłanie SMS-ów. Obowiązki informacyjne pracodawcy są tożsame z obowiązkami, jakie będą na pracodawcę nałożone w przypadku wprowadzenia monitoringu wizyjnego[36].

Najważniejszą zmianą, która została wprowadzona przepisami RODO, jest zakwalifikowanie danych biometrycznych do szczególnej kategorii danych osobowych. Dotychczas w brzmieniu ustawy o ochronie danych osobowych z 1997 roku dane biometryczne nie zostały wymienione wprost w art. 27 ust. 1, który definiuje zamknięty katalog danych osobowych wrażliwych, a więc takich, których przetwarzanie jest zabronione. Ustawodawca w projekcie ustawy zawarł regulację dotyczącą danych biometrycznych. Treść nowego artykułu 22^2 §1–3, który ostatecznie nie znalazł się w Kodeksie pracy, zakładała możliwość przetwarzania przez pracodawcę danych biometrycznych tylko pracowników i tylko za ich uprzednią zgodą udzieloną w formie pisemnej lub elektronicznie. Ustawa z 1997 roku nie klasyfikowała danych biometrycznych do danych wrażliwych, mimo iż w istocie dotyczą cech fizycznych, fizjologicznych lub behawioralnych, a więc powinny podlegać silniejszej ochronie"[37]. W ustawodawstwie krajowym do przetwarzania danych biometrycznych uprawnione są organy państwowe wykonujące zadania publiczne, a także organy paszportowe. Natomiast w stosunku pracy polem do wykorzystywania biometrii przez pracodawców jest kontrola dostępu do chronionych obszarów, pomieszczeń oraz autoryzacja użytkowników korzystających z określonych danych, programów czy urządzeń. W takich okolicznościach powodem zbierania danych biometrycznych jest uzasadniony interes pracodawcy i bezpieczeństwo mienia. Mimo to wielu pracodawców wykorzystuje dane biometryczne do ewidencjonowania czasu pracy pracowników czy innych czynności, które nie odpowiadają przesłankom legalności i adekwatności

[35] M. Gawroński, K. Kloc, op. cit.

[36] D. Dörre-Kolasa, *Monitoring pracowników*, op. cit.

[37] M. Korga, *Dane biometryczne i ich wykorzystywanie na gruncie stosunku pracy*, „MOPR" 2011, nr 12, s. 19.

przetwarzania danych[38]. Odczyt linii papilarnych przez system informatyczny w celu ewidencji czasu pracy pracowników niewątpliwie jest rozwiązaniem łatwym, ale niekoniecznie zgodnym z literą prawa. Jak zauważa Andrzej Drozd, zasada adekwatności nakazuje, by cel przetwarzania danych przez administratora był proporcjonalny do uciążliwości doświadczanych przez ich dysponenta, spowodowanych przez przetwarzanie jego danych w określonych okolicznościach[39]. Zagadnienie to było przedmiotem analizy Naczelnego Sąd Administracyjny i Urzędu Ochrony Danych Osobowych. NSA uznał, że „wykorzystywanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania"[40]. W odniesieniu do przetwarzania informacji biometrycznych pracowników jednoznacznie stwierdzić należy, że wśród szeroko pojętej interpretacji przepisów prawa pracy nie istnieje jasny przepis, zgodnie z którym pracodawca uprawniony jest do żądania od pracownika podania danych biometrycznych. Sam Prezes Urzędu Ochrony Danych Osobowych w decyzji z 15 grudnia 2009 roku jednoznacznie stwierdził, że „czas pracy pracownika może być przez pracodawcę kontrolowany za pomocą innych środków, mniej ingerujących w prywatność osoby zatrudnionej"[41]. Dodał również, że „złożenie przez pracownika oświadczenia, którego treścią jest wyrażenie zgody na przetwarzanie danych osobowych w postaci linii papilarnych, nie stanowi przesłanki legalizującej przetwarzanie danych osobowych pracowników"[42].

Reforma unijna wprowadziła wiele zmian w zakresie danych biometrycznych, nadając im status danych wrażliwych, zakazując ich wykorzystywania oraz dopuszczając ich przetwarzanie tylko w określonych przypadkach. W art. 4 punkt 14 RODO zdefiniowano dane biometryczne, jednak jest to katalog otwarty, gdyż z uwagi na dynamiczny rozwój metod technicznych przetwarzania danych identyfikujących jednostkę katalog możliwości wykorzystywania danych biometrycznych stale się powiększa. Dane biometryczne oznaczają 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. Zatem obok wizerunku twarzy można wskazać także

[38] M. Gersdorf, *Nowe techniki gromadzenia i przetwarzania danych osobowych pracowników a ochrona ich prywatności*, referat wygłoszony na 26. Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych, 14 września 2004 roku, [online] http://26konferencja.giodo.gov.p1/program/j/pl/ [dostęp: 18.02.2016].

[39] A. Drozd, *Prawo podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, Warszawa 2004, s. 120, 123–124.

[40] Wyrok NSA z 1 grudnia 2009 r. I OSK 249/09, LEX nr 785755.

[41] Decyzja nr DIS/DEC-1261/46988/09, [online] https://giodo.gov.pl/pl/289/3336 [dostęp: 24.05.2018].

[42] Ibidem.

na takie dane biometryczne, jak: odcisk palca, cechy tęczówki oka, układ naczyń krwionośnych, głos, kształt małżowiny usznej, podpis uwzględniający nacisk i poziom nachylenia pisma, dynamika pisania na klawiaturze. Coraz szerszy zakres danych biometrycznych wykorzystywanych przez wiele podmiotów niesie z sobą duże ryzyko nadużyć[43]. Dostosowanie w tym zakresie prawa polskiego do unijnego będzie lepiej chroniło prywatność obywateli. Chociaż zasady dotyczące zakazu przetwarzania danych biometrycznych nie znalazły się w Kodeksie pracy, to w pewnych okolicznościach będzie miał zastosowanie art. 22^2 k.p. Jest to wyjątek związany z monitoringiem wizyjnym obejmującym przetwarzanie danych biometrycznych pracowników. Wizerunek pracowników utrwalany za pośrednictwem monitoringu może być bowiem w określonych przypadkach ich danymi biometrycznymi. Przetwarzanie danych biometrycznych jest dopuszczalne wyłącznie za wyraźną zgodą, w ściśle określonym celu. To, czy mamy do czynienia z danymi biometrycznymi, zależy od technologii przetwarzania wizerunku. Istotne jest więc, czy stosowane są specjalne metody techniczne, umożliwiające jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości[44]. Pracodawcy powinni więc zwrócić uwagę, na jak dokładne i szczegółowe rejestrowanie obrazu pozwala zainstalowany w zakładzie pracy monitoring oraz czy przy jego wykorzystaniu dokonywana jest szczegółowa analiza i identyfikacja nagranych osób fizycznych. Wizerunek pracowników utrwalony przez tak zwany zwykły monitoring nie będzie bowiem uznany za dane biometryczne. Jeśli jednak zastosowana jest specjalna technika pozwalająca na jednoznaczną identyfikację pracownika, wówczas tak utrwalony wizerunek pracownika będzie jego daną biometryczną[45].

W procesach naboru pojawiły się kolejne ograniczenia. Z dniem wdrożenia przepisów RODO zmianom uległy regulacje dotyczące czynności sprawdzających kandydata/pracownika. Na przestrzeni ostatnich kilkunastu lat na polskim rynku pracy popularnymi metodami stały się: weryfikowanie informacji przedstawionych przez kandydatów w procesie rekrutacyjnym, w tym rekomendacji poprzednich pracodawców (*background screening*, *background check*), poddawanie testom w celu uzyskiwania dodatkowych informacji o kandydatach/pracownikach (badania psychologiczne). *Background check* to proces polegający na weryfikacji prawdziwości informacji wskazanych przez kandydata do pracy. Proces taki może być wykonywany bądź to przez pracodawców, bądź przez podmioty rekrutujące pracowników i inne profesjonalne podmioty oferujące takie usługi.

[43] R. Jezierski, *Przetwarzanie danych osobowych podczas czynności sprawdzających kandydata: background screening, testy psychologiczne, dane o karalności, rekomendacj*e, [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dörre-Kolasa, Seria „Zarządzanie", 2017, s. 60–75.

[44] Uzasadnienie do projektu ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych, s. 6.

[45] E. Bielak-Jomaa, D. Lubasz, op. cit.

Zaś przedmiotem procesu są przede wszystkim informacje wskazane w CV oraz innych dokumentach przedkładanych podczas ubiegania się o pracę, jak kwestionariusze osobowe, certyfikaty czy rekomendacje[46]. W praktyce jednak weryfikowanie informacji dotyczy niemalże każdej dziedziny życia, która ma bezpośredni lub pośredni związek z pracą. Sprawdzanie danych kandydatów i pracowników jest uznawane za niedopuszczalną praktykę szczególnie wtedy, gdy dokonywana jest bez zgody i wiedzy kandydata/pracownika, a w wyniku weryfikacji pracodawca uzyskuje dostęp do wrażliwych informacji, które nie powinny być przetwarzane w procesie rekrutacji oraz w okresie zatrudnienia. Na podstawie przepisów obowiązujących do dnia 24 maja 2018 roku weryfikowanie informacji przedstawionych przez kandydatów w procesie rekrutacyjnym budziło spore wątpliwości w związku z możliwością uzyskania dostępu do danych osobowych kandydata/pracownika, które nie zostały ujęte w art. 22^1 k.p. W praktyce odwoływano się do regulacji zamieszczonej w art. 22^1 §3 k.p., zgodnie z którą pracodawca mógł żądać dostępu do innych danych, nieujętych w katalogu danych osobowych, w oparciu o złożone przez kandydata/pracownika oświadczenie. Brakowało jednak jasnych zasad w przepisach umożliwiających weryfikację kont osoby na portalach społecznościowych, kontaktu z byłymi pracodawcami czy certyfikatów i rekomendacji.

Próżno było szukać regulacji odnośnie do innej, bardzo popularnej metody, jaką jest poddawanie kandydatów/pracowników testom psychologicznym. Jednym z kluczowych elementów procesu zarządzania zasobami ludzkimi jest ocenianie kandydatów do pracy oraz pracowników[47]. Badania tego typu z pewnością mogą stanowić alternatywę dla wariografu, gdyż unikają stresującej atmosfery, która towarzyszy badaniu poligraficznemu. Jednakże naruszenie prywatności osoby ubiegającej się o pracę czy pracownika może mieć również miejsce przy przeprowadzaniu różnego rodzaju testów, badań czy podczas przeszukiwania portali społecznościowych[48]. Decyzja o poddaniu osoby obowiązkowi wzięcia udziału w badaniu może wynikać z dwóch przyczyn – z wymogów określonych przepisami prawa lub z własnej inicjatywy pracodawcy. W pierwszym przypadku wymóg sprawdzenia kandydata i przeprowadzenia badań psychologicznych bądź testów umiejętności przewidują niektóre przepisy prawne[49]. Psychometryczna ocena kandydatów w pełni znajduje uzasadnie-

[46] H. Szewczyk, op. cit., s. 415 i n.

[47] Z. Ciekanowski, *Proces oceniania pracowników w nowoczesnej organizacji*, „Nauki Humanistyczne i Społeczne na rzecz Bezpieczeństwa", [online] http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BGPK-3625-4017/c/httpwww_bg_utp_edu_plartbtp3201203_12ciekanowski.pdf [dostęp: 21.05.2018 r.]

[48] R. Jezierski, op. cit., s. 60–75.

[49] Rozporządzenie Ministra Spraw Wewnętrznych z dnia 18 kwietnia 2012 r. w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w policji (DzU z 2012 r., poz. 432); Rozporządzenie Ministra Sprawiedliwości

nie w obowiązujących przepisach prawa, jeżeli mamy do czynienia z naborem do zawodów niebezpiecznych czy związanych z pewnym rodzajem lub warunkami pracy. W pozostałym zakresie weryfikacja oraz testy psychologiczne powinny być ograniczone. Testy powinny być bowiem przeprowadzane tylko w zakresie niezbędnym przy rekrutacji na stanowiska, na których cechy osobowościowe odgrywają istotną rolę[50]. Nie powinny one nakazywać pracownikowi zamieszczania informacji, które mogą posiadać znamiona potencjalnie dyskryminujące czy uwłaczające. Kandydat winien być poinformowany, jakie cechy osobowości oraz zakres umiejętności będą sprawdzone, a także o wynikach i sposobie ich udostępniania. Podmiot zatrudniający zobowiązany jest do uzyskania pisemnej zgody na przeprowadzenie badań[51].

W celu zminimalizowania ryzyka związanego z możliwym naruszeniem zasad ochrony danych osobowych oraz uczynienia zadość wymogom RODO w zakresie *background screeningu* i poddawania osób testom psychologicznym polski ustawodawca odwołuje się do nowego brzmienia art. 22^1 §3 k.p. Zgodnie z jego treścią przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w tym artykule jest dopuszczalne tylko wtedy, gdy dotyczą one stosunku pracy i kandydat wyrazi na to swobodną zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej. Tak więc pracodawca powinien odebrać uprzednio wyraźną zgodę na przeprowadzenie weryfikacji od kandydata/pracownika. W praktyce będzie to oznaczało, że pracodawca powinien zapewnić kandydatów i pracowników, iż brak zgody nie będzie miał negatywnego wpływu na wynik rekrutacji ani nie stanie się podstawą jakiejkolwiek decyzji dotyczącej ich zatrudnienia. W przypadku uzyskania odpowiedniej zgody wydaje się, że pracodawca lub wspierająca go firma zewnętrzna będą uprawnieni do kontaktu z poprzednimi pracodawcami. Niemniej jednak w takim przypadku weryfikacja powinna zostać ograniczona wyłącznie do informacji przedstawionych przez kandydata/pracownika i nie może obejmować innych danych osobowych[52]. Jeżeli kandydat zgodzi się na przedłożenie referencji, wówczas pracodawca może włączyć je do dokumentów rekrutacyjnych. Warto jednak zadbać o to, aby w dokumentacji znalazła się zgoda pracownika na przedłożenie tych dokumentów.

---

z 19 września 2014 r. w sprawie badań lekarskich i psychologicznych kandydatów do objęcia urzędu sędziego (DzU z 2014 r., poz. 1293); Ustawa z dnia 12 października 1990 r. o straży granicznej (DzU z 2017 r., poz. 2365).

[50] H. Szewczyk, op. cit., s. 420 i n.

[51] D. Dörre-Kolasa, *Współczesne przykłady naruszeń obowiązku pracodawcy szanowania godności i innych dóbr osobistych pracownika – art.111 k.p.*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej. Rocznik" 2001/2002, s. 227.

[52] M. Barański, M. Giermak, op. cit., s. 92.

V

Przyjęty zakres przedmiotowego opracowania z pewnością nie pozwala w sposób pełny odnieść się do problemu związanego z ochroną danych osobowych. Problematyka ochrony danych w zatrudnieniu, mimo wielu zmian, które weszły w życie 25 maja 2018 roku, wciąż budzi wiele kontrowersji. Ścierają się tu przeciwstawne interesy dwóch grup: grupy pracowników, oczekujących od współczesnego państwa ochrony sfery życia prywatnego i wszelkich swoich danych, oraz grupy pracodawców, dążących do kontrolowania pracowników.

Rozwój cywilizacyjny wymaga, aby na prawo pracy, w szczególności na prawo do prywatności jednostki w kontekście zatrudnienia, spoglądać inaczej, uwzględniając warunki, w których musi być ono respektowane. Należy również zauważyć, że omawiane zagadnienie stanowi doskonały przykład na wskazany w literaturze przedmiotu związek prawa pracy z nauką i techniką, wypływ owej nauki i nowych rozwiązań technicznych na dynamiczny rozwój norm ochronnych prawa pracy i ich wykładni[53]. Nowoczesne techniki nadzoru stanowią drastyczną ingerencję w sferę prywatności pracownika i rodzą zagrożenia, z których istnienia nie tylko pracownik, lecz także współczesne społeczeństwo nie zdaje sobie sprawy. Techniki te otwierają przedsiębiorcom możliwości analizy danych na każdym etapie i w każdej sferze życia. Ostatnie lata to również wzrost wielu zagrożeń odnoszących się do prawidłowego przetwarzania i ochrony danych osobowych. Mają miejsce coraz częstsze włamania do systemów informatycznych czy wycieki danych.

Ustawa z 10 maja 2018 roku, która wprowadza do Kodeksu pracy przepisy dotyczące stosowania nowoczesnych technologii, wywołuje wiele kontrowersji i problemów. Czy nowe przepisy sprawiły, że kwestia ochrony danych osobowych stała się bardziej jednoznaczna i prosta? Minęło zaledwie kilka miesięcy od wprowadzenia bezpośredniego stosowania RODO. Z drugiej strony pracodawcy korzystający z monitoringu wizyjnego są w fazie dostosowywania się do nowych regulacji. To za krótko, aby mówić o tym, czy zmiany idą w dobrym kierunku, czy w złym. Na pewno wiemy, że zgodnie z nowym art. 22^2 §1 k.p. przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 22^1 k.p. jest dopuszczalne za zgodą kandydata do pracy, która może być wyrażona także elektronicznie. Brak takiej zgody nie może być przyczyną, dla której kandydat miałby mniejsze szanse na zatrudnienie. Jednocześnie każdy pracodawca przed zastosowaniem nowoczesnych technologii będzie musiał pamiętać o przestrzeganiu art. 35 rozporządzenia, który obliguje administratora do dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych przed ich rozpoczęciem w przypadku, w którym dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować ryzyko naruszenia praw lub wolności osób fizycznych. Śmiało można powiedzieć, że RODO to nie rewolucja, lecz ewolucja.

[53] M. Gersdorf, op. cit.

Protection of the Right to Privacy at Work in the Period of Dynamically Developing Technologies – Today and Tomorrow

Abstract

The protection of the right to privacy is one of the basic human rights and as a fundamental subject in most modern laws. Legal systems extend the privacy protection instruments to a significant extent, but at the same time they find reasons to strongly interfere in this area. Certainly, the dynamic development of modern technologies does not help the legislator to find a comprehensive solution. The article deals with the subject of privacy protection in the employment relationship on the area of innovation, technology development. In this study, the author also compares the impact of the use of modern technologies in the workplace today - in the light of the applicable regulations and tomorrow – taking into account enactment of Regulation (EU) 2016/679 of European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Keywords

processing of personal data, the right to privacy, protection of personal data, General Data Protection Regulation, employment relationship

Bibliografia

1. Baran K. W., *Kodeks pracy. Komentarz*, Warszawa 2018.
2. Baranowska I., *Ochrona danych osobowych kandydatów do pracy i pracowników po wejściu w życie RODO. Komentarz praktyczny*, LEX/el. 2018.
3. Barański M., Giermak M., *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego (uwagi de lege ferenda)*, „Państwo i Prawo" 2017, nr 9.
4. Bielak-Jomaa E., Lubasz D., *Ogólne rozporządzenie o ochrony danych osobowych. Komentarz*, Warszawa 2018.
5. Ciekanowski Z., *Proces oceniania pracowników w nowoczesnej organizacji*, „Nauki Humanistyczne i Społeczne na rzecz Bezpieczeństwa", [online] http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BGPK-3625-4017/c/httpwww_bg_utp_edu_plartbtp3201203_12ciekanowski.pdf [dostęp: 21.05.2018].
6. Dörre-Kolasa D., *Monitoring w miejscu pracy a prawo do prywatności*, „Praca i Zabezpieczenie Społeczne" 2004, nr 9.
7. Dörre-Kolasa D., *Monitoring pracowników*, LEX/el. 2018, komentarz praktyczny.
8. Dörre-Kolasa D., *Współczesne przykłady naruszeń obowiązku pracodawcy szanowania godności i innych dóbr osobistych pracownika – art.111 k.p.*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej. Rocznik" 2001/2002.
9. Drozd A., *Prawo podmiotu zatrudniającego do pozyskiwania informacji o kandydacie na pracownika*, Warszawa 2004.
10. Frąckowiak M., Świeboda T., *Ochrona danych osobowych pracownika w perspektywie RODO i przepisów dotyczących monitoringu wizyjnego stosowanego przez pracodawcę*, „MOPR" 2018, nr 7.

11. Gawroński M., Kloc K., *Monitoring jako jedna z kluczowych zmian wprowadzonych przez ustawę o ochronie danych osobowych*, LEX/el. 2018.
12. Gersdorf M., *Nowe techniki gromadzenia i przetwarzania danych osobowych pracowników a ochrona ich prywatności*, referat wygłoszony na 26. Międzynarodowej Konferencji Ochrony Prywatności i Danych Osobowych, 14 września 2004 roku, [online] http://26konferencja.giodo.gov.p1/program/j/pl/ [dostęp: 18.02.2016].
13. Jaśkowski K., *Uwagi do art. 22[1] k.p.*, [w:] K. Jaśkowski, E. Maniewska, *Komentarz aktualizowany do Kodeksu pracy*, LEX 2018.
14. Jaworski R., *Badania poligraficzne a prawa pracownicze*, [w:] *Granice ochrony danych osobowych w stosunkach pracy*, red. T. Wyka, A. Nerka, Warszawa 2009.
15. Jezierski R., *Przetwarzanie danych osobowych podczas czynności sprawdzających kandydata: background screening, testy psychologiczne, dane o karalności, rekomendacj*e, [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dörre-Kolasa, Seria „Zarządzanie", 2017.
16. Korga M., *Dane biometryczne i ich wykorzystywanie na gruncie stosunku pracy*, „MOPR" 2011, nr 12.
17. Krzysztofek M., *Zgoda pracownika jako podstawa przetwarzania danych biometrycznych w RODO i w projekcie Przepisów wprowadzających ustawę o ochronie danych osobowych*, „IAP" 2017, nr 4.
18. Litwiński P., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa, Legalis/el 2018.
19. Siwicki M., *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych (uwagi w związku z projektem rozporządzenia Parlamentu Europejskiego i Rady)*, „Państwo i Prawo" 2016, nr 3.
20. Sobczyk A., *Kodeks pracy. Komentarz*, Warszawa 2018.
21. Szewczyk H., *Ochrona dóbr osobistych w zatrudnieniu*, Warszawa 2007.
22. Świątkowski A. M., *Kodeks pracy. Komentarz*, Warszawa 2018.
23. Warren S. D., Brandeis L., *The Right to Privacy*, "Harvard Law Review" 1890, Vol. IV.
24. Wujczyk M., *Prawo pracownika do ochrony prywatności*, Warszawa 2012.
25. Wujczyk M., *Podstawy prawne przetwarzania danych osobowych kandydatów do pracy i pracowników, ze szczególnym uwzględnieniem zgody jako przesłanki uchylającej zakaz przetwarzania danych. Z problematyki wykładni art. 22[1] k.p.*, [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dörre-Kolasa, Seria „Zarządzanie", 2017.
26. Wyrok Naczelnego Sądu Administracyjnego z 1 grudnia 2009 r. I OSK 249/09, LEX nr 785755.