Acta Universitatis Wratislaviensis No 3082
PRAWO CCCVII Wrocław 2009

JACEK BOROWICZ
Uniwersytet Wrocławski

Sytuacja prawna pracownika przetwarzającego dane osobowe w ramach wykonywania obowiązków ze stosunku pracy

1. Uwagi wstępne

Wykonywanie obowiązków pracowniczych związanych z przetwarzaniem informacji prawem chronionych podlega wielu specyficznym, prawnym uwarunkowaniom. Wpływają one w przekonaniu autora w sposób dość istotny na sytuację prawną pracownika przetwarzającego te informacje. Zakres tego wpływu jest jednak różny w zależności od szczegółowości unormowań prawnych statuujących zasady ochrony informacji danego rodzaju i wynikającego z nich stopnia ingerencji ustawodawcy w kształtowanie reguł wykonywania zatrudnienia związanego z ich przetwarzaniem. Na przykład w odniesieniu do pracowników mających dostęp do tzw. tajemnicy pracodawcy źródłem obowiązku zapewnienia ochrony informacjom objętym tą formą tajemnicy jest przepis powszechnego prawa pracy a zakres formalizacji szczegółowych obowiązków stron stosunku pracy z tym związanych – nieokreślony bezpośrednio przez ustawę[1]. „Obowiązek przestrzegania tajemnicy [pracodawcy – J.B.] ma charakter bezwarunkowy w tym znaczeniu, że pracodawca nie musi podejmować określonych kroków w celu zachowania poufności informacji, których ujawnienie mogłoby go narazić na szkodę"[2]. W przypadku zaś na

[1] Art. 100 § 2 pkt 4 k.p. O tajemnicy pracodawcy szerzej J. Borowicz, *Przestrzeganie tajemnicy pracodawcy a inne pracownicze obowiązki przestrzegania tajemnicy – zagadnienia pojęciowe*, PiZS 10/1998, s. 2–9.

[2] Do udowodnienia winy pracownika niezbędne jest jednak poinformowanie przez pracodawcę o zakresie poufności informacji – *Kodeks pracy*. *Komentarz*, red. W. Muszalski, Warszawa 2004, s. 294.

przykład pracownika przetwarzającego informacje niejawne w rozumieniu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych[3] mamy do czynienia z całym zespołem szczegółowych unormowań ustawowych formujących, zdaniem autora, wyraźnie odrębny status prawny tego pracownika[4].

Również przepisy zawarte w ustawie z dn. 29 sierpnia 1997 r. o ochronie danych osobowych[5] (dalej: jako ustawa o.d.o.) wraz ze sformułowanym w nich szerokim katalogiem obowiązków przypisywanych podmiotom przetwarzającym te dane wpływają kształtująco na sytuację prawną osób zatrudnionych u tych podmiotów na zasadach pracowniczych. Do rozważenia pozostaje zakres tego wpływu, a tym samym odpowiedź na pytanie o zakres odrębności sytuacji prawnej osób przetwarzających dane osobowe w ramach wykonywania obowiązków z zakresu stosunku pracy.

Specyfika sytuacji prawnej pracownika przetwarzającego informacje chronione może znajdować swoje najwyraźniejsze odzwierciedlenie przede wszystkim w sferach: 1) wymogów, które spełnić ma osoba aspirująca do wykonywania pracy związanej z dostępem do informacji chronionych, 2) jej obowiązków związanych z przetwarzaniem tych informacji, 3) jej odpowiedzialności za naruszenie reguł ich ochrony. Ustawodawca może zatem formułować wymogi dopuszczalności zatrudnienia danej osoby na stanowisku związanym z dostępem do informacji chronionych określonej kategorii, jak również wprowadzać specyficzne procedury naboru lub sprawdzenia kompetencji kandydatów na stanowiska związane z ich przetwarzaniem. Najbardziej wyrazistym przykładem sygnalizowanych rozwiązań prawnych mogą być prawnie określone postępowania sprawdzające przed dopuszczeniem do wykonywania pracy związanej z dostępem do informacji niejawnych[6] czy też normy określające przesłanki, które musi spełniać osoba zatrudniana w pionie ochrony informacji niejawnych[7], lub też przepisy wprowadzające wymóg odbycia odpowiednich szkoleń przed rozpoczęciem przetwarzania informacji chronionych[8]. Analiza przepisów chroniących daną kategorię informacji pozwala także na wskazanie pewnych specyficznych, wynikających z tych przepisów powinności ciążących na pracowniku je przetwarzającym

[3] Tekst jedn. Dz.U. 5.196.1631.

[4] Szerzej: J. Borowicz, *Status prawny pracownika przetwarzającego informacje niejawne. Zagadnienia wybrane*, PiZS 9/2001, s. 2–13; także J. Borowicz, *Ochrona informacji niejawnych w stosunkach pracy – zagadnienia wybrane*, Przegląd Prawa i Administracji, t. LVIII, Wrocław 2004, s. 51–68.

[5] Tekst jedn. Dz.U. 2.101.926 z późn. zm.

[6] Zgodnie z art. 27 ust. 1 Ustawy o ochronie informacji niejawnych dopuszczenie do pracy lub pełnienia służby na stanowisku albo zlecenie prac związanych z dostępem do informacji niejawnych może nastąpić do zasady dopiero po przeprowadzeniu postępowania sprawdzającego.

[7] J. Borowicz, *Status prawny*..., s. 4–7.

[8] Zgodnie z art. 54 ust. 1 Ustawy o ochronie informacji niejawnych dopuszczenie do pracy lub służby, z którymi łączy się dostęp do informacji niejawnych, poprzedza szkolenie w zakresie ochrony informacji niejawnych.

(np. obowiązek złożenia ślubowań wyrażających przyjęcie powinności ochrony tajemnicy danej kategorii, jak dzieje się na przykład w przypadku tajemnicy statystycznej czy skarbowej[9]) lub na odczytanie treści powszechnych, kodeksowych obowiązków pracowniczych (np. obowiązku sumienności i staranności przestrzegania tajemnicy określonej w odrębnych przepisach – art. 100. 1 i § 2 pkt 5 k.p.) w kontekście powinności ochrony danej kategorii informacji. Unormowania chroniące daną kategorię informacji mogą również zawierać bezpośrednie odniesienia co do reżimów odpowiedzialności prawnej, które znajdą zastosowanie w sytuacji naruszenia zasad ochrony tych informacji (np. przez sformułowanie katalogu przestępstw przeciwko tym informacjom, jak w przypadku ustawy o.d.o.). Formalnym wyrazem szczególnej sytuacji prawnej pracownika przetwarzającego dane chronione jest specyficzna dokumentacja osobowa i organizacyjna opisująca ją oraz konkretyzująca obowiązki związane z przetwarzaniem tych danych (np. poświadczenia bezpieczeństwa, upoważnienia do dostępu do danych osobowych, akty wewnętrzne typu instrukcyjnego opisujące techniki i procedury postępowania z informacjami chronionymi).

2. Pracownik jako podmiot administrujący danymi osobowymi

Ustawa o ochronie danych osobowych od początków swego funkcjonowania w polskim systemie prawnym wskazywała podmioty zaangażowane w proces przetwarzania danych osobowych jako adresatów jej norm ustalających ich szczegółowe powinności związane z ochroną tych danych. Do określenia tych podmiotów w pierwotnym tekście tej ustawy[10] stosowana była dość rozbudowana terminologia. Można było wskazać np. na pojęcia: administratora danych osobowych (dalej: ADO; było to i jest nadal jedyne pojęcie definiowane ustawowo

[9] Zgodnie np. z art. 12 Ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz.U. 95.88.439 z późn. zm.) pracownicy służb statystyki publicznej, rachmistrze spisowi, ankieterzy statystyczni oraz inne osoby wykonujące czynności w imieniu i na rzecz statystyki publicznej, mający bezpośredni dostęp do danych indywidualnych i danych osobowych, są obowiązani do bezwzględnego przestrzegania tajemnicy statystycznej i mogą być dopuszczeni do wykonywania tych czynności po złożeniu w urzędzie statystycznym albo innej jednostce organizacyjnej służb statystyki publicznej pisemnego przyrzeczenia następującej treści: „Przyrzekam, że będę wykonywać swoje prace na rzecz statystyki publicznej z całą rzetelnością, zgodnie z etyką zawodową statystyka, a poznane w czasie ich wykonywania dane jednostkowe zachowam w tajemnicy wobec osób trzecich". Podobnie zgodnie z art. 294 § 2. ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (tekst jedn. Dz.U. 05.8.60 z późn. zm.) m.in. pracownicy urzędów skarbowych oraz izb skarbowych są obowiązani do złożenia na piśmie przyrzeczenia następującej treści: „Przyrzekam, że będę przestrzegał tajemnicy skarbowej. Oświadczam, że są mi znane przepisy o odpowiedzialności karnej za ujawnienie tajemnicy skarbowej".

[10] Np. tekst pierwotny tej ustawy opublikowany w Dz.U. 97.133.883.

– J.B.), osoby dopuszczonej na podstawie upoważnienia administratora danych osobowych do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych (art. 37 ustawy o.d.o.), osoby zatrudnionej przy przetwarzaniu danych (art. 39 ustawy o.d.o; podkreślenie – J.B.), administrującego zbiorem danych (art. 50, 51, 54 ustawy o.d.o.), administrującego danymi (art. 52 ustawy o.d.o.), obowiązanego do ochrony danych osobowych (art. 51 ustawy o.d.o.)[11]. Z kolei powoływana ustawa w wersji obecnie obowiązującej charakteryzuje się ujednoliceniem i uproszczeniem terminologii stosowanej do określenia podmiotów zaangażowanych w rozmaite aspekty procesu przetwarzania danych osobowych. Ustawodawca, w dalszym ciągu posługując się jako jedną z głównych (i nadal konsekwentnie zdefiniowanych ustawowo) ustawowych kategorii pojęciowych terminem administratora danych osobowych, wyróżnił także pojęcia: osoby upoważnionej do przetwarzania danych (art. 7 pkt 6 ppkt b, art. 39 ust. 1 i 2 ustawy o.d.o.), osoby posiadającej upoważnienie nadane przez administratora danych (art. 37 ustawy o.d.o.), administratora bezpieczeństwa informacji (art. 36 ust. 3. ustawy o.d.o.)[12]. Z kolei w przepisach karnych ustawy o.d.o. rozróżnia się współcześnie tego, kto przetwarza w zbiorze dane osobowe (art. 49 ust. 1), tego, kto administruje zbiorem danych (art. 51 ust. 1, art. 52, art. 54); tego, kto będąc do tego obowiązany, nie zgłasza do rejestracji zbioru danych (art. 53)[13]. We wskazanych przypadkach (z wyjątkiem

[11] Podobne, aczkolwiek znacznie bardziej szczegółowe rozróżnienie podmiotów zaangażowanych w proces przetwarzania danych osobowych występuje na gruncie obowiązujących w przeszłości przepisów wykonawczych do ustawy o.d.o. W rozporządzeniu MSWiA z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DZ.U. z 1998 r., Nr 80, poz. 521 z późn. zm.), rozróżniano ADO oraz: *administratora bezpieczeństwa informacji* (par. 3), *osoby zatrudnione przy przetwarzaniu danych osobowych* (par. 4, 6 ust. 1, 7 ust. 2), *osoby dopuszczone do pracy przy przetwarzaniu danych osobowych* (par. 4), *osoby przetwarzające dane osobowe* (par. 6 ust. 3), *osobę użytkującą przenośny komputer, służący do przetwarzania danych osobowych* (par. 9), *osobę upoważnioną przez ADO do nadzoru nad naprawą urządzeń, dysków lub innych informatycznych nośników danych* (par. 10 ust. 3), *użytkownika systemu informatycznego, w którym przetwarza się dane osobowe danych* (par. 14 ust. 3). W przypadku tego aktu prawnego brakowało także definicji poszczególnych tych pojęć.

[12] Poprzednio pojęcie *administratora bezpieczeństwa informacji* występowało w przepisach wykonawczych do ustawy o.d.o. (przypis 16), obecnie uchylonych i zastąpionych przez nowe (przypis kolejny).

[13] Należy nadmienić, że nowe przepisy wykonawcze zawarte w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 04.100.1024), podobnie jak w przypadku uchylonych przepisów wykonawczych, poszerzają paletę terminologiczną, wprowadzając do tekstu prawnego m.in. typowo informatyczne pojęcie użytkownika (§ 2 pkt 2), a także pojęcia: *osoby upoważnionej do przetwarzania danych osobowych w systemie informatycznym* (§ 2 pkt 2 *in fine*), *osoby uprawnionej do pracy w systemie informatycznym* (§ 2 pkt 3). Z kolei w załączniku do tego rozporządzenia odnaleźć można zarówno terminologię zbli-

ADO) brakuje jednak definicji ustawowych. Jak można zauważyć, ustawodawca, wskazując na podmioty zaangażowane w proces przetwarzania danych osobowych, nie posługiwał się nigdy wprost pojęciem pracownika, rezygnując z czasem także z szerszego pojęciowo określenia „osoby zatrudnionej przy przetwarzaniu danych osobowych", znanego z wcześniejszych wersji ustawy, a mogącego być powiązanym z kategorią zatrudnienia pracowniczego. Wskazuje to, że dla ustawodawcy głównym kryterium wyodrębnienia podmiotów zaangażowanych w przetwarzanie danych osobowych u konkretnego administratora danych osobowych jest właśnie fakt przetwarzania tych danych przez te osoby na podstawie otrzymanego od ADO upoważnienia, a nie np. podstawa prawna, na której wykonywana jest praca na rzecz danego ADO. W konsekwencji mogą to być zarówno pracownicy w rozumieniu art. 2 k.p., jak i osoby zatrudnione na innych podstawach prawnych – o ile legitymują się one stosownym upoważnieniem ADO – i jako takie zostały ujęte w ewidencji osób upoważnionych (a nie jak w pierwotnej wersji ustawy o.d.o. – zatrudnionych przy przetwarzaniu danych – J.B.) do przetwarzania danych osobowych.

Przedstawiony przegląd terminologii ustawowej stanowić może podstawę przede wszystkim do podniesienia jeszcze jednej istotnej kwestii, a mianowicie relacji między wskazanymi pojęciami określającymi podmioty zaangażowane w proces przetwarzania danych osobowych u ADO a samym pojęciem ADO. W szczególności rozważyć należy, czy pojęcie ADO określa podmiot od nich odrębny, czy też zakresy pojęciowe poszczególnych terminów ustawowych określających te podmioty mogą się na siebie nakładać.

Zgodnie z definicją zawartą obecnie w art. 7 pkt 4 ustawy o.d.o administratorem danych osobowych jest organ, instytucja, jednostka organizacyjna, podmiot lub osoba, będące organem państwowym, organem samorządu terytorialnego, państwową lub komunalną jednostką organizacyjną, podmiotem niepaństwowym realizującym zadania publiczne, osobą fizyczną lub prawną albo jednostką organizacyjną – jeżeli przetwarzają one dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych i w związku z tym decydują o celach i środkach przetwarzania tych danych. Jak wynika z przedstawionej definicji, pojęcie ADO jest bardzo pojemne. Status ten może zatem służyć podmiotom przyjmującym bardzo różną, dopuszczoną przez prawo formę prawną i organizacyjną. W szczególności status ten nie jest powiązany z posiadaniem

żoną do znanej z ustawy o.d.o. (jego zapisy odnoszą się m.in. do osób *upoważnionych do przetwarzania danych osobowych* – część A, pkt I, ppkt 1 i 2 załącznika czy też osób mających *dostęp do danych przetwarzanych w systemie informatycznym* – część A, pkt II załącznika), jak i specyficzne określenia kazuistycznie wskazujące na podmioty uwikłane w pewne szczególne sytuacje związane z przetwarzaniem danych osobowych (np. *użytkownik, który utracił uprawnienia do przetwarzania danych* – część A, pkt IV załącznika; *osoba użytkująca komputer przenośny zawierający dane osobowe* – część A, pkt V załącznika; *osoba upoważniona przez administratora danych do nadzoru nad naprawą urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe* – część A, pkt VI, ppkt 3 załącznika).

osobowości prawnej przez dany podmiot. Można nawet postawić tezę, że elementy te (tzn. forma prawna, forma organizacyjna) mają drugorzędne znaczenie w przypadku identyfikacji ADO. W literaturze i orzecznictwie sformułowany został pogląd, zgodnie z którym podstawowe znaczenie do zakwalifikowania danego podmiotu jako ADO będzie mieć ustalenie, czy ma on kompetencje decyzyjne, pozwalające rozstrzygać w sposób wiążący o celach i środkach zbierania, gromadzenia i przechowywania w zbiorach, udostępniania, przekazywania, niszczenia oraz każdego innego przetwarzania danych osobowych w związku ze swoją działalnością zarobkową, zawodową lub do realizacji swoich celów statutowych[14]. Podkreśla się przy tym, iż pojęcie ADO nie powinno być zawężone wyłącznie do kręgu tych podmiotów, których kompetencje decyzyjne obejmują wykonywanie wszystkich operacji składających się na pojęcie przetwarzania danych w rozumieniu art. 7 pkt 2 ustawy o.d.o.[15] W literaturze wyraża się także pogląd o możliwości funkcjonowania kilku ADO w ramach jednej jednostki organizacyjnej o złożonej strukturze[16]. Istotne natomiast wydaje się zaakcentowanie, że ADO jest podmiotem samodzielnym w podejmowaniu decyzji we wskazanej sferze[17]. Uwagi te mogą być bezpośrednio odniesione do podmiotów wskazanych w art. 3 k.p. jako pracodawcy – strony stosunków pracy. Ponadto w literaturze zwraca się uwagę, że już samo określenie zakresu stosowania ustawy o.d.o., zwłaszcza przez jego odniesienie do wszelkich podmiotów przetwarzających dane osobowe w związku z działalnością zarobkową i zawodową, jest dostatecznie szerokie, by objąć nim także kategorię pracodawców w rozumieniu art. 3 k.p. Świadczyć mają o tym inne regulacje ustawy o.d.o. wprost łączące przetwarzanie danych osobowych ze stosunkami zatrudnienia (np. art. 27 ust. 6, art. 43 ust. 1 i 4), a co istotne w obowiązującym stanie prawnym – przepisy k.p. (art. 22^1)[18].

[14] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2001, s. 306; J. Borowicz, *Odpowiedzialność pracodawcy jako administratora danych osobowych*, Nowe Zeszyty Samorządowe nr 5/2002, s. 59; A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 17–18; A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2004, s. 61; wyrok NSA w Warszawie z dn. 30 stycznia 2002 r., II SA 1098/01, Wokanda 2002/7–8/70; postanowienie SN z dnia 11 grudnia 2000 r., II KKN 438/00, OSNKW 2001/3–4/33.

[15] Za ADO uznać należy także te podmioty, które samodzielnie prowadzą jedynie np. zbieranie i przechowywanie danych czy też zajmują się jedynie ich opracowywaniem bądź udostępnianiem; J. Barta, R. Markiewicz, *op. cit.*, s. 305.

[16] J. Borowicz, *Pracodawca samorządowy jako administrator pracowniczych danych osobowych*, Nowe Zeszyty Samorządowe nr 1/2006, s. 23–24.

[17] A. Drozd, *Ustawa o ochronie*..., s. 62.

[18] Wprowadzony do kodeksu pracy w ramach nowelizacji z 17 listopada 2003 r., określając zakres uprawnień pracodawcy związanych z przetwarzaniem danych osobowych w związku z zatrudnieniem, formę udostępniania danych osobowych przez pracownika oraz normując relację między przepisami k.p. a przepisami ustawy z dn. 29 sierpnia 1997 r. o ochronie danych osobowych (Art. 1 pkt 7 ustawy z dn. 14 listopada 2003 r. o zmianie ustawy – Kodeks pracy, oraz o zmianie niektórych innych ustaw, Dz.U. Nr 213, poz. 2081).

Tak więc w myśl obowiązujących przepisów pracodawca, przetwarzając dane osobowe zatrudnionych pracowników zarówno w aktach osobowych, różnego rodzaju wykazach i skorowidzach, jak i w systemach informatycznych, staje się administratorem tych danych, którego zasadniczo dotyczą ustawowe reguły ich przetwarzania[19]. Pracodawca w rozumieniu art. 3 k.p. może w konkretnej sytuacji występować w pozycji strony stosunku pracy, którego przedmiotem będzie wykonywanie przez pracownika pracy określonego rodzaju. Jej elementem składowym będzie przetwarzanie danych osobowych w zakresie funkcjonalnie i treściowo powiązanym z tym rodzajem pracy. Pracownik ten będzie zatem przetwarzał u danego pracodawcy dane osobowe w ramach wykonywania obowiązków ze stosunku pracy.

Istotnych ustaleń w zakresie rozróżnienia pojęć administratora danych osobowych i administrującego danymi osobowymi (określanego także jako dysponent danych osobowych) dokonano w orzecznictwie. Przymiot „administrującego" przysługiwać ma zatem podmiotowi, który w odróżnieniu od ADO, będącego podmiotem decydującym o celach i środkach przetwarzania danych osobowych, jedynie „zarządza, zawiaduje zbiorem danych lub danymi". Jednocześnie, w nawiązaniu do wypowiedzi doktryny, wskazuje się, że pojęcie administrującego ma szersze znaczenie. Administrującym może być więc zarówno ADO, jak i ten, kto takiej roli nie odgrywa. Odpowiednio administratorem danych osobowych nie jest każdy dysponent danych osobowych[20].

Należy zaaprobować ten pogląd. Analiza językowa powoływanych przepisów w związku z nieostrością stosowanych w nim pojęć nie pozwala co prawda – moim zdaniem – na postawienie radykalnej tezy, iż ustawodawca przeciwstawia decydowanie o celach i środkach przetwarzania danych osobowych działaniom polegającym na obsłudze systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, wykonywaniu zatrudnienia przy przetwarzaniu danych, administrowaniu zbiorem danych czy danymi, ochranianiu danych osobowych, jednak pozwala na wskazanie szerokiego spektrum działań wykonawczych funkcjonalnie podporządkowanych kompetencjom o charakterze decyzyjnym. W konsekwencji należy uznać, że o ile pracodawcom służyć będzie przymiot administratorów danych osobowych w odniesieniu do danych pracowników przez siebie zatrudnianych oraz danych osobowych przetwarzanych w ścisłym związku z przedmiotem działalności danego pracodawcy (np. dane osobowe klientów – indywidualnych osób fizycznych), o tyle pracownicy zatrudniani przy przetwarzaniu tych danych (np. w szeroko rozumianych komórkach kadrowych), dysponujący odpowiednim upoważnieniem (patrz dalej) powinni być identyfikowani co do zasady jako „administrujący danymi osobowymi" w ramach wykonywania obowiązków ze stosunku pracy.

[19] T. Kuczyński, *Ochrona danych osobowych w stosunkach zatrudnienia*, Przegląd Sądowy nr 11–12/98, s. 122.

[20] Zob. orzecznictwo w przyp. 13; J. Barta, R. Markiewicz, *op. cit*., s. 307.

3. Nawiązanie stosunku pracy z pracownikiem przetwarzającym dane osobowe

Przepisy ustawy o.d.o. oraz związane z nią przepisy wykonawcze (zarówno u początków swojego funkcjonowania w polskim systemie prawnym, jak i obecnie) zawierają niewielki zakres unormowań, które mogą być odniesione do kwestii doboru, nawiązania stosunku pracy i wdrożenia do pracy osób przetwarzających dane osobowe. W szczególności zaś obowiązujące w tym zakresie prawo nie przewiduje szczególnej procedury kwalifikowania i oceny kandydatów do pracy związanej z danymi osobowymi – procedury, której przedmiotem byłoby ustalenie, czy kandydaci ci dają rękojmię prawidłowego wykonywania obowiązków związanych z ochroną przetwarzanych przez siebie informacji (tak jak np. w przypadku wykonywania pracy na stanowiskach związanych z dostępem do informacji niejawnych – J.B.[21]). Pewne działania mogące mieć znaczenie przy ocenie kandydata na pracownika przetwarzającego dane osobowe mogą zatem wynikać albo z własnej inicjatywy pracodawcy, albo też z przepisów prawa formułujących wymagania, których spełnienie – w sposób pośredni – może wpływać także na ocenę przydatności kandydata do pracy związanej z przetwarzaniem tych danych (np. taką funkcję mogą spełnić niejako „przy okazji" ustawowe wymogi niekaralności, odbycie szkoleń, aplikacji, stażów, zdania egzaminów i inne podnoszone w pragmatykach). Przepisy dotyczące ochrony danych osobowych nie formułują również żadnych wymogów formalnych i merytorycznych, które miałyby spełniać osoby mające być zatrudnione na stanowiskach związanych z przetwarzaniem danych osobowych. Ocena kwalifikacji konkretnej osoby i jej przydatności do pracy związanej z ich przetwarzaniem zostaje więc pozostawiona pracodawcy. Należy jednak przyjąć, iż pracodawca, działając jako administrator danych osobowych w rozumieniu art. 7 pkt. 4 ustawy o.d.o., przez staranny dobór i przygotowanie kandydatów do pracy na stanowiskach związanych z przetwarzaniem danych osobowych, wykonuje swój obowiązek prawidłowego zabezpieczenia tych danych[22].

3.1. Przygotowanie pracownika do pracy związanej z przetwarzaniem danych osobowych

Uchylone Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3.06.1998 r. w sprawie określania podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informa-

[21] Na temat tych procedur szerzej J. Borowicz, *Status prawny*..., s. 4–10.

[22] Na konieczność dołożenia szczególnej staranności w wyborze osób odpowiedzialnych za prawidłowość przetwarzania danych osobowych w odniesieniu do wskazania przez administratora danych osobowych tzw. administratora bezpieczeństwa informacji zwraca uwagę A. Drozd, *Ustawa o ochronie*..., Warszawa 2004, s. 253.

tyczne służące do przetwarzania danych osobowych[23] (dalej: rozp. MSWiA z dn. 3.06. 1998 r.), nakazywało w swoim § 5 zaznajomienie pracowników przetwarzających dane osobowe z przepisami normującymi to zagadnienie „przed przystąpieniem do pracy" przy przetwarzaniu tych danych. Nie określano przy tym metody tego „zaznajomienia się". Brakowało także wyraźnie sformułowanej powinności dokumentowania realizacji tego obowiązku[24]. Aktualnie obowiązujące Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[25] (dalej: rozp. MSWiA z dnia 29 kwietnia 2004 r.), odstąpiło od tego typu wymogu. Zdaniem autora, ze względu na wagę i złożoność problemu ochrony danych osobowych, zmianę tę należy ocenić krytycznie. Znajomość unormowań prawa wydaje się zarówno kwestią podstawową i punktem wyjścia do budowania odpowiedniej świadomości prawnej pracowników, jak i warunkiem niezbędnym do właściwego realizowania obowiązków pracowniczych związanych z ochroną tych danych u konkretnego pracodawcy.

W obowiązującym stanie prawnym pracownik mający w związku z wykonywaniem pracy umówionej przetwarzać dane osobowe może być zobowiązany przez pracodawcę realizującego własną powinność wynikającą z art. 94 pkt. 1 k.p. do uczestniczenia w szkoleniu z zakresu ich ochrony. Pracodawca zaznajamia tym samym tego pracownika m.in. z zakresem obowiązków związanych z ochroną tej kategorii danych oraz sposobami pracy zapewniającymi ich bezpieczne przetwarzanie na wyznaczonym stanowisku. Należy przyjąć, że istotnym elementem takiego szkolenia byłoby – oprócz zapoznania się z przepisami prawa oraz procedurami i technikami ochrony informacji – zaznajomienie pracownika z takimi elementami dokumentacji organizacyjnej z zakresu ochrony danych osobowych, jak „Polityka bezpieczeństwa" oraz „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" uszczegóławiającymi zasady ochrony tych danych u danego pracodawcy[26]. Byłoby to również

[23] Dz.U. nr 80, poz. 521.

[24] W literaturze zwrócono wówczas uwagę, że ponieważ w trakcie czynności kontrolnych realizacja tego obowiązku (zaznajomienia z przepisami dotyczącymi ochrony danych osobowych – J.B.) może być badana przez inspektora ochrony danych osobowych, w interesie pracodawcy leży więc właściwe udokumentowanie spełnienia wszystkich wymogów prawnych ochrony tych danych. Waga, jaką przykłada ustawodawca do ochrony danych osobowych, nakazuje, aby pracownik potwierdził na piśmie odbycie przeszkolenia, instruktażu czy innej formy zaznajomienia się z odpowiednimi przepisami (ustawodawca nie precyzuje formy realizacji tego obowiązku). Potwierdzenie to należy przechowywać w aktach osobowych, w części B; J. Borowicz, *Obowiązek prowadzenia przez pracodawcę dokumentacji osobowej i organizacyjnej z zakresu ochrony danych osobowych*, PiZS 3/2001, s. 5.

[25] Dz.U. 04.100.1024.

[26] Obowiązek prowadzenia tej dokumentacji wynikający z art. 36 ust. 2 ustawy o ochronie danych osobowych precyzuje rozp. MSWiA z dnia 29 kwietnia 2004 r. – zob. § 1 pkt 1, § 3, § 4.

przejawem wykonania powinności wdrożenia tej dokumentacji (§ 3 ust. 1. rozp. MSWiA z dnia 29 kwietnia 2004 r.)[27].

3.2. Złożenie oświadczenia pracownika o zapoznaniu się z prawami przysługującymi mu w związku z ochroną jego danych osobowych

Ustawodawca nakłada na ADO obowiązek poinformowania osoby fizycznej, której dane są przez nią zbierane, o swojej „tożsamości" (w przypadku zatrudnienia pracowniczego będzie to nazwa i siedziba pracodawcy), celu zbierania danych oraz prawie wglądu do swoich danych oraz ich poprawiania (art. 24 ustawy o.d.o.). Obserwacje praktyki stosowania unormowań chroniących dane osobowe poczynione przez autora wskazują, że jest to powinność powszechnie ignorowana przez pracodawców. Tymczasem, jak wynika z literatury, udzielenie tych informacji pracownikowi warunkuje legalność zbierania danych osobowych przez pracodawcę[28]. A zatem w interesie prawnym pracodawcy, który spełnił wskazaną powinność przy zatrudnieniu pracownika, jest zapewnienie sobie możliwości wykazania się faktem realizacji ustawowej powinności w odniesieniu do każdej z zatrudnianych przez siebie osób fizycznych. Oznaczać to może składanie przez pracowników pisemnych oświadczeń o zapoznaniu się z przysługującymi im na mocy przepisów ustawy o.d.o uprawnieniami. Należy przypomnieć, że konstrukcja obowiązku określonego w art. 24 ustawy o.d.o. wyklucza jego realizację przez działania skierowane do ogółu uprawnionych (np. wywieszenie w miejscu ogólnie dostępnym dla pracowników informacji o prawach osób fizycznych związanych z ochroną ich danych osobowych)[29].

3.3. Zaznajomienie pracownika z zakresem informacji objętych tajemnicą na zasadzie art. 39 ust. 2 ustawy o.d.o.

Zgodnie z § 3 Rozporządzenia MPiPS z dnia 28.05.1996 r. w sprawie zakresu prowadzenia przez pracodawcę dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika[30] pracodawca „przed dopuszczeniem pracownika do pracy uzyskuje jego pisem-

[27] A. Drozd, *Ustawa o ochronie*..., s. 241.

[28] A. Drozd, *Zasady przetwarzania danych osobowych w aktach osobowych pracowników*, PiZS 3/2005, s. 12–13.

[29] Oświadczenie tego typu powinno być przechowywane w aktach osobowych pracownika, w ich części B; J. Borowicz, *Obowiązek prowadzenia*...

[30] Dz.U. 96.62.286 z późn. zm.

ne potwierdzenie zapoznania się z [...] zakresem informacji objętych tajemnicą określoną w obowiązujących ustawach dla umówionego z pracownikiem rodzaju pracy". Zgodnie zaś z aktualnym brzmieniem art. 39 ust. 2 ustawy o.d.o. osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Pracodawca powinien zatem przed dopuszczeniem pracownika do pracy wskazać mu wyraźnie: 1) zakres objętych tajemnicą danych osobowych, z jakim pracownik ten będzie miał do czynienia w ramach wykonywania pracy umówionej, 2) objęte tajemnicą sposoby ich zabezpieczenia. Pracownik powinien zaś potwierdzić pisemnie zapoznanie się z tymi informacjami[31].

3.4. Nadanie pracownikowi upoważnienia do przetwarzania danych osobowych

Wymóg nadania takiego upoważnienia pracownikowi zatrudnionemu przy przetwarzaniu danych osobowych, znany z poprzednich wersji ustawy o.d.o., wynika także z aktualnego brzmienia jej art. 37. Upoważnienie to powinno być nadane pracownikowi przed rozpoczęciem wykonywania pracy związanej z przetwarzaniem tych danych i tylko pracownik legitymujący się takim upoważnieniem może legalnie przetwarzać dane osobowe u danego pracodawcy. Należy w związku z tym przyjąć, że nie można domniemywać istnienia upoważnienia do przetwarzania danych osobowych na podstawie rodzaju pracy umówionej (jako takiego, z którym z istoty rzeczy wiąże się konieczność przetwarzania tych danych) albo wykazu obowiązków/zakresu czynności przedstawionego pracownikowi przez pracodawcę. Jak wskazuje się w literaturze, w obecnym stanie prawnym nie ma wątpliwości, że zakresem tego upoważnienia objęty jest każdy przypadek przetwarzania danych osobowych w zbiorze – w szczególności bez względu na to, czy zbiór jest prowadzony w systemie informatycznym[32]. Nadawania upoważnienia, o którym mowa w art. 37 ustawy o.d.o., nie należy zatem mylić z przypadkiem nadawania uprawnień do przetwarzania danych w systemie informatycznym, o którym mowa np. w rozp. MSWiA z dnia 29 kwietnia 2004 r. (§ 5 pkt 1). Nadanie określonej osobie uprawnień do przetwarzania danych w systemie informatycznym jest czynnością techniczną wynikającą z faktu wcześniejszego nadania upoważnienia do przetwarzania danych osobowych jako takich.

Ustawodawca nie określa formy ani treści takiego upoważnienia. Ze względów dowodowych należy przyjąć, że powinno ono być wydane na piśmie. Upoważnienie to powinno mieć charakter imienny – w jego treści należy wyraź-

[31] Potwierdzenie to powinno być przechowywane w jego aktach osobowych (część B).

[32] A. Drozd, *Ustawa o ochronie*..., s. 254; wcześniej na konieczność objęcia zakresem upoważnienia do przetwarzania danych osobowych metodami „tradycyjnymi" zwracał uwagę także J. Borowicz, *Obowiązek prowadzenia*..., s. 4–5.

nie wskazać osobę dysponującą tym upoważnieniem oraz zakres przetwarzania danych osobowych realizowany na jego podstawie. Należałoby przyjąć, iż upoważnienie takie powinno być wydane w dwóch egzemplarzach – jeden z nich pozostawałby, na wypadek kontroli, w dyspozycji pracownika, a drugi w jego aktach osobowych, w ich części B[33].

3.5. Ujęcie informacji dotyczących pracownika przetwarzającego dane osobowe w „Ewidencji osób upoważnionych do przetwarzania danych osobowych"

Art. 39 ust. 1 ustawy o.d.o. formułuje ciążącą na administratorze danych osobowych powinność ewidencjonowania osób przetwarzających dane osobowe na podstawie nadanych im przez niego upoważnień. Obejmuje ona zatem swoim zakresem podmiotowym nie tylko pracowników zatrudnionych przy przetwarzaniu danych osobowych, lecz także wszystkie inne osoby, którym konkretny pracodawca takie upoważnienia nadał. Ewidencja ta stanowi element dokumentacji osobowej związanej z przetwarzaniem danych osobowych[34]. W ewidencji takiej należy uwzględnić następujące informacje: imię i nazwisko pracownika, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych przez danego pracownika, a także identyfikator tego pracownika funkcjonujący w systemie informatycznym. Wskazanie w ewidencji zakresu upoważnienia do przetwarzania danych osobowych może być dokonane na przykład przez nazwanie poszczególnych kategorii danych osobowych i określenie stanowiska zajmowanego przez pracownika podlegającego wpisowi do ewidencji lub wskazanie rodzaju pracy umówionej, z której wykonywaniem łączy się przetwarzanie danych osobowych.

Ustawodawca nie przesądza, w jakiej formie ma być prowadzona ewidencja pracowników przetwarzających dane osobowe. W literaturze wyrażono w związku z tym pogląd, iż posługiwanie się pojęciem ewidencji może, w świetle przepisu art. 2 ust. 2 ustawy o.d.o. wprowadzającego rozróżnienie danych przetwarzanych w systemach informatycznych oraz „kartotekach [...] i innych zbiorach ewidencyjnych" sugerować, iż ewidencja ta ma mieć formę „tradycyjną" – pisemną (nieinformatyczną)[35].

---

[33] J. Borowicz, *Obowiązek prowadzenia*...

[34] „Za włączeniem ewidencji osób przetwarzających dane osobowe do dokumentacji osobowej przemawia odniesienie jej do mogącego zmieniać się w czasie zbioru konkretnych, upoważnionych do przetwarzania danych osobowych osób fizycznych, a nie względnie ustalonego w ramach struktury organizacyjnej zakładu pracy zbioru stanowisk pracy lub komórek organizacyjnych związanych z przetwarzaniem danych osobowych", J. Borowicz, *Obowiązek prowadzenia*..., s. 5–6.

[35] A. Drozd, *Ustawa o ochronie*..., s. 260, J. Borowicz, *Obowiązek prowadzenia*...

4. Obowiązki pracownika przetwarzającego dane osobowe

4.1. Obowiązek stosowania obowiązujących u danego pracodawcy sposobów zabezpieczenia danych osobowych

Przepisy ustawy o.d.o. nakładają na pracodawcę – administratora danych osobowych wiele obowiązków związanych ze stosowaniem technicznych i organizacyjnych środków ochrony tych danych odpowiednio do zagrożeń oraz kategorii danych osobowych objętych ochroną. Środki te powinny być opisane w prowadzonej przez pracodawcę dokumentacji. Ustawodawca nakłada również na pracodawcę powinność wyznaczenia administratora bezpieczeństwa informacji sprawującego nadzór nad przestrzeganiem zasad ochrony danych osobowych (art. 36. ust. 1–3 ustawy o.d.o.)[36]. Szczegółowe zasady stosowania środków technicznych i organizacyjnych określa rozp. MSWiA z dnia 29 kwietnia 2004 r. Ogół tych unormowań wyznacza zestaw oczekiwanych z punktu widzenia bezpieczeństwa danych, zróżnicowanych zachowań pracownika. Objęte one mogą być opisowym określeniem „obowiązku stosowania obowiązujących u danego pracodawcy sposobów zabezpieczenia danych osobowych". Zachowania polegające na zawinionym niestosowaniu lub zawinionym błędnym stosowaniu tych sposobów mogą być interpretowane jako naruszenie obowiązków pracowniczych związanych z przetwarzaniem danych osobowych. Stosowane u danego pracodawcy sposoby zabezpieczenia danych osobowych wyznaczają również – w sensie technicznym – metodykę wykonywania pracy umówionej z uwzględnieniem wymogów bezpieczeństwa informacji. Zachowania zgodne z tą metodyką pozwalają uznać, iż praca wykonywana jest sumiennie i starannie, z poszanowaniem ustalonego porządku pracy, dobra zakładu pracy i tajemnicy pracodawcy oraz danych osobowych. Przyjęta u danego pracodawcy organizacyjna i techniczna (a w szczególności informatyczna) metodologia ochrony danych osobowych może być zatem źródłem danych umożliwiających ustalenie norm o charakterze pozaprawnym, pozwalających pracodawcy na ocenę wykonywania niektórych podstawowych obowiązków pracowniczych opisanych w art. 100 k.p.

[36] W literaturze zwraca się uwagę, że w związku z tym, iż ustawa o.d.o. nie określa, w ramach jakiego stosunku prawnego administrator bezpieczeństwa informacji ma wykonywać swoje obowiązki, należy więc przyjąć, że może on to czynić w ramach rozmaitych stosunków zatrudnienia (stosunek pracy, stosunki cywilnoprawne czy też administracyjnoprawne) lub w ramach samozatrudnienia, A. Drozd, *Ustawa o ochronie*..., s. 252–253.

4.2. Obowiązek zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia

Pracownik na mocy art. 100 § 2 pkt 5 k.p. zobowiązany jest do przestrzegania tajemnicy danych osobowych jak jednej z tajemnic określonych w odrębnych przepisach. Tak więc zachowując tajemnice tych danych, spełnia on wyrażoną w tym przepisie k.p. powinność pracowniczą. Nie wydaje się jednak, aby uzasadniało to określenie samej tajemnicy danych osobowych z art. 39 ust. 2 ustawy o.d.o. jako „tajemnicy pracowniczej", jak czyni to G. Sibiga, ponieważ zgodnie z przepisem ustawy o.d.o. adresatem tej powinności są osoby upoważnione do przetwarzania danych (co jest szerokim ujęciem grupy adresatów tej powinności) – a nie wyłącznie upoważnione osoby przetwarzające te dane w ramach wykonywania obowiązków ze stosunku pracy[37] (czy nawet szerzej – w ramach zatrudnienia). Należy dodać, że obowiązek zachowania tajemnicy danych osobowych przez pracownika przetwarzającego te dane w ramach wykonywania obowiązków ze stosunku pracy nie zależy od tego, czy i jaką szkodę ujawnienie tych danych podmiotom nieuprawnionym mogłoby wyrządzić pracodawcy[38].

Jak już wspomniano, zgodnie z aktualnym brzmieniem art. 39 ust. 2 ustawy o.d.o. osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować w tajemnicy zarówno te dane, jak i sposoby ich zabezpieczenia. Wcześniejsza wersja tego przepisu zawężała tę powinność do zachowania w tajemnicy samych tylko danych osobowych. Wyrażając aprobatę dla obecnego brzmienia tego przepisu, należy zgodzić się, że zachowanie w poufności sposobów (metod, technik, narzędzi, procedur) zabezpieczenia danych osobowych, szczególnie w przypadku przetwarzania tych danych w systemie informatycznym, ma w praktyce zasadnicze znaczenie dla prawidłowości ich ochrony przed zagrożeniami zewnętrznymi.

Przepis art. 39 ust. 2 ustawy o.d.o. w swoim obecnym brzmieniu nie odnosi się w żaden sposób do kwestii granic czasowych trwania obowiązku zachowania tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. W swojej poprzedniej wersji określał on natomiast dość ogólnie, iż obowiązek ten miał istnieć „również po ustaniu zatrudnienia". Nie wyznaczano przy tym żadnej górnej granicy czasowej trwania tego obowiązku. Przyjętą ówcześnie konstrukcję można było, zdaniem autora, oceniać krytycznie – w świetle brzmienia

[37] G. Sibiga, *Dostęp do informacji publicznej a prawo do prywatności jednostki i ochrony jej danych osobowych*, Samorząd Terytorialny nr 11/2003, s. 9.

[38] Por. charakterystyka powinności z art. 100 § 2 pkt 5 k.p.; L. Florek, T. Zieliński, *Prawo pracy*, Warszawa 2000, s. 152. Dane osobowe przetwarzane w danym zakładzie pracy mogą również się mieścić w szerszej kategorii tajemnic pracodawcy, czyli informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę; patrz np. T. Kuczyński, [w:] Z. Kubot, T. Kuczyński, Z. Masternak, H. Szurgacz, *Prawo pracy. Zarys wkładu*, Warszawa 2005, s. 152–153.

powołanego przepisu należało bowiem przyjąć istnienie dożywotniego obowiązku tajemnicy, a więc tego obowiązku formuły, która nie stanowi reguły w szeroko rozumianym prawie ochrony informacji. Warto zwrócić uwagę, że nawet w przypadku bardziej rygorystycznych unormowań chroniących tak newralgiczną kategorię danych, jak informacje niejawne, ustawodawca jasno wskazuje zróżnicowane, w zależności od tzw. klauzul tajności, okresy trwania stanu tajemnicy informacji danej kategorii. W aktualnym stanie prawnym ustawa o ochronie danych osobowych pomija kwestię okresu obowiązywania stanu tajemnicy danych osobowych. W literaturze wyrażono w związku z tym pogląd, ze zmiana dokonana w 2004 r. w przepisie art. 39 ust. 2 miała charakter jedynie redakcyjny; związany z tym obowiązek zachowania tajemnicy danych osobowych i sposobów ich zabezpieczania ma ciążyć nie tylko na osobach zatrudnionych, lecz także na wszystkich upoważnionych do przetwarzania tej kategorii informacji. Podnosi się przy tym, że pomimo iż analizowany przepis nie wskazuje wyraźnie obowiązku zachowania tajemnicy po ustaniu upoważnienia, to należy przyjąć, że omawiany obowiązek trwa także po jego ustaniu, gdyż ustawa nie przewiduje ograniczenia czasowego tego obowiązku[39]. Zwraca jednak – moim zdaniem – uwagę to, że ustawa o.d.o. wiąże istnienie tego obowiązku z posiadaniem przez zobowiązanego do zachowania tajemnicy statusu osoby upoważnionej do przetwarzania danych osobowych („Osoby, które zostały upoważnione do przetwarzania danych…" art. 39 ust. 2 ustawy o.d.o., podkreślenie – J.B.). Były pracownik, którego zatrudnienie ustało, nie ma już zatem statusu osoby upoważnionej do przetwarzania danych osobowych, z jakimi miał do czynienia u byłego pracodawcy. O ile więc w dalszym ciągu dysponuje nimi (i przetwarza je w zbiorze – choć nie jest do tego uprawniony – por. art. 49 ust. 1 ustawy o.d.o.[40]), to można mu zasadnie postawić zarzut nieuprawnionego dysponowania tymi danymi oraz bezprawnego ich przetwarzania. Nie wydaje się natomiast, aby w świetle przepisów ustawy o.d.o zasadne było stwierdzenie, że narusza on powinności zachowania ich w tajemnicy[41]. Powinność zachowania informacji w tajemnicy może naruszyć jedynie osoba zobowiązana do dochowania tej tajemnicy. W związku z podniesionymi wątpliwościami należałoby raczej postulować doprecyzowanie unormowania zawartego w art. 39 ust. 2 ustawy o.d.o. mogące polegać chociażby na wyraźnym stwierdzeniu, iż obowiązek

[39] A. Drozd, *Ustawa o ochronie*..., s. 260–261.

[40] „Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

[41] Chyba że uzna się istnienie ustawowego obowiązku zachowania tajemnicy danych osobowych o charakterze powszechnym, niezwiązanego ze statusem pracowniczym, czy też szerzej – z istnieniem aktualnego upoważnienia do przetwarzania danych osobowych. Taka powinność jednak ciążyłaby z mocy ustawy na każdym, kto nie będąc uprawniony, w jakichkolwiek okolicznościach zapoznałby się z danymi osobowymi, co jednak, jak się wydaje, nie odpowiada literalnemu brzmieniu zapisu ustawowego.

zachowania tajemnicy danych osobowych ciąży na osobie upoważnionej także po ustaniu tego upoważnienia[42].

Wychodząc poza ściśle językową analizę tego przepisu, można zastanowić się nad celowością nieograniczonego w czasie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Odwołać się można do pewnych ogólnych obserwacji związanych także w dużej mierze z ochroną informacji, a mianowicie dotyczących sfery własności intelektualnej (a więc także przypadku unormowań wyznaczających pewne granice czasowe ochrony, w tym przypadku np. w odniesieniu do majątkowych uprawnień twórców). Wskazać można np. na zjawisko dyfuzji nowych rozwiązań, a więc na proces, w którym nawet rozwiązania / utwory chronione z upływem czasu wchodzą do obrotu (upowszechniają się), niekiedy wbrew woli dysponentów praw, a więc nawet w drodze nielegalnej. Podchodząc do sprawy zdroworozsądkowo, należy uznać, że procesu tego nie da się w całości powstrzymać. Stąd też, jak można przypuszczać, ograniczony czasowo monopol twórcy / wynalazcy na eksploatację swego wytworu intelektualnego. W odniesieniu do informacji zachodzić mogą podobne procesy, a więc jej naturalna dyfuzja, ale też jej „starzenie" się, dezaktualizacja – zjawiska podważające, zdaniem autora, celowość jej niczym nieograniczonej w czasie ochrony. Sposoby zabezpieczenia danych osobowych mogą również, wraz z postępem technicznym i rozwojem informatyki, ulegać zmianom (swoistej „dezaktualizacji", starzeniu się, wypieraniu przez rozwiązania nowe).

Także sygnalizowane już analogie z unormowaniami chroniącymi informacje niejawne, które można by rozszerzyć o pewne odniesienia co do czasu trwania klauzuli poufności w przypadku ochrony tajemnicy przedsiębiorstwa[43] czy też powinności sprecyzowania okresu trwania mowy o zakazie konkurencji po ustaniu stosunku pracy[44], pozwalałyby na sformułowanie postulatu wyznaczenia

[42] Warto zwrócić uwagę, że art. 294 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa, zobowiązujący w § 1 do przestrzegania tajemnicy skarbowej m.in. pracowników urzędów skarbowych oraz izb skarbowych; pracowników urzędów celnych oraz izb celnych; czy też pewne kategorie harcowników samorządowych (odpowiednio są to wójt, burmistrz (prezydent miasta), starosta, marszałek województwa oraz pracownicy samorządowych służb finansowych) formułuje wprost w swoim § 3 regułę zobowiązującą wskazane podmioty do zachowania tajemnicy skarbowej również po ustaniu zatrudnienia lub zakończeniu praktyki zawodowej. Tak więc możliwe jest, że ustawodawca w sposób bezpośredni wskazuje w przepisach na taki właśnie otwarty zakres czasowy obowiązywania tajemnicy informacji określonej kategorii.

[43] Art. 11 ust. 1 i 2 Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jedn. Dz.U. 03.153.1503 z późn. zm.), zgodnie z którym czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy. Przepis ust. 1 stosuje się również do osoby, która świadczyła pracę na podstawie stosunku pracy lub innego stosunku prawnego przez okres trzech lat od jego ustania, chyba że umowa stanowi inaczej albo ustał stan tajemnicy.

[44] Zawieranej z pracownikiem mającym dostęp do szczególnie ważnych informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, por. art. 101^2 § 1 k.p.

w przepisach ustawy o.d.o. jasnych granic czasowych obowiązku zachowania tajemnicy danych osobowych i sposobów ich zabezpieczania.

4.3. Obowiązek współdziałania z organem ochrony danych osobowych

Obowiązek współdziałania z organem ochrony danych osobowych będzie wynikać z całokształtu unormowań określających uprawnienia Generalnego Inspektora Danych Osobowych i reprezentujących go w ramach przeprowadzanych działań kontrolnych inspektorów danych osobowych. Należy przyjąć, że korelatem uprawnień do wstępu do pomieszczeń, w których przetwarzane są dane osobowe, żądania wyjaśnień, wzywania i przesłuchiwania osób w zakresie niezbędnym do ustalenia stanu faktycznego, uzyskiwania wglądu do dokumentów i danych czy też przeprowadzenia oględzin, badań i innych czynności (art. 14 pkt 1–4 ustawy o.d.o.) będą powinności pracowników przetwarzających dane osobowe sumujące się w zespole zróżnicowanych zachowań umożliwiających realizację ustawowych uprawnień przypisanych inspektorowi ochrony danych osobowych (opisowy obowiązek współdziałania z organem ochrony danych osobowych). Należy podkreślić, że podmiotem odpowiedzialnym za realizację tych powinności przez poszczególnych pracowników przetwarzających dane osobowe jest, na mocy art. 15 ust. 1 ustawy o.d.o., kierownik kontrolowanej jednostki organizacyjnej. Przepis ten nakłada na niego szczególny obowiązek zachowania się w taki sposób, aby kontrolujący inspektorzy mogli wykonywać działania kontrolne określone w art. 14 pkt 1–4 ustawy o.d.o., co może znaleźć swój wyraz w wydawaniu pracownikom przetwarzającym dane osobowe odpowiednich poleceń służących zapewnieniu właściwego współdziałania tych pracowników z inspektorem[45].

5. Pracownicza odpowiedzialność przetwarzającego dane osobowe w ramach wykonywania obowiązków ze stosunku pracy

Rozważając stosowanie w sytuacji naruszenia przez pracownika zasad ochrony danych osobowych reguł odpowiedzialności przewidzianych w prawie pracy, należy na wstępie zaznaczyć, że w literaturze problem ten rozpatruje się w kontekście szerokiego rozumienia pojęcia odpowiedzialności pracowniczej. Zgodnie z nim przez odpowiedzialność pracowniczą należy rozumieć przewidziane w przepisach prawa negatywne skutki (dolegliwości) o charakterze

[45] A. Drozd, *Ustawa o ochronie*..., s. 99.

prawnym, które mogą być zastosowane wobec pracownika za jego naganne zachowanie się[46]. Jak jednocześnie podkreśla się w literaturze, szeroko rozumiana odpowiedzialność według przepisów prawa pracy, którą objąć można osoby uchybiające obowiązkom związanym z ochroną danych osobowych przetwarzanych w związku z wykonywaniem pracy umówionej, pełni funkcję subsydiarną względem odpowiedzialności cywilnej, a zwłaszcza przewidzianej przez ustawę o.d.o. odpowiedzialności karnej (rozdz. 8 tej ustawy)[47].

Zastosowanie tego ujęcia odpowiedzialności pracowniczej pozwala przyjąć, iż pracodawca może zastosować wobec pracownika zatrudnionego przy przetwarzaniu danych osobowych nie tylko odpowiedzialność porządkową (art. 108 i n. k.p.) i materialną (art. 114 i n. k.p.), lecz także inne środki stosowane w sytuacjach nagannych zachowań pracowników, jak np. rozwiązanie umowy o pracę (w szczególności w trybie natychmiastowym – art. 52 k.p.)[48] czy też pozbawienie lub obniżenie składnika wynagradzania powiązanego z wynikami pracy (premia). Pracodawca występuje więc w pozycji podmiotu uprawnionego do zastosowania wobec pracownika naruszającego zasady ochrony przetwarzanych danych osobowych jednego ze wskazanych środków.

Wybór środka służącego realizacji odpowiedzialności danego pracownika pozostawiony zostaje co do zasady pracodawcy oceniającemu wagę naruszenia zasad przetwarzania danych osobowych w kontekście rodzaju wykonywanej pracy oraz rodzaju i konsekwencji naruszenia zasad i stopnia winy „sprawcy". Swoboda wyboru przez pracodawcę tych środków doznaje pewnego ograniczenia w sytuacji wskazanej w art. 17 ust. 2 ustawy o.d.o. Na podstawie tego przepisu inspektor ochrony danych osobowych, opierając się na wynikach przeprowadzonej kontroli, może wystąpić do pracodawcy – administratora danych osobowych z żądaniem wszczęcia „postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania" przeciwko osobie winnej dopuszczenia do uchybień. Przy braku ustawowych definicji przez odpowiedzialność dyscyplinarną należy rozumieć postać odpowiedzialności szczególnej, której podlegają mianowani pra-

[46] Szerokie ujęcie odpowiedzialności pracowniczej przeciwstawia się w doktrynie wąskiemu jej definiowaniu. Zgodnie z nim odpowiedzialność pracowniczą łączyć można tylko z reżimem odpowiedzialności majątkowej i osobistej, a jej przejawem może być tylko dolegliwość formalnie objęta reżimami odpowiedzialności w prawie pracy, czyli np. odpowiedzialność porządkową lub materialną. O różnych ujęciach odpowiedzialności pracowniczej: np. T. Kuczyński, [w:] Z. Kubot, T. Kuczyński, Z. Masternak, H. Szurgacz, *Prawo pracy*..., s. 155–156. Tenże autor opowiada się za szerokim ujęciem odpowiedzialności pracowniczej w przypadku naruszenia zasad ochrony danych osobowych przez osoby zatrudnione, T. Kuczyński, *Ochrona danych osobowych w stosunkach zatrudnienia*, Przegląd Sądowy nr 11–12/1999, s. 128.

[47] T. Kuczyński, *Ochrona danych*... Autor ten również wskazuje na możliwość zastosowania reguł odpowiedzialności cywilnej w sytuacjach powstających na gruncie art. 31 ustawy o.d.o. Zagadnienie odpowiedzialności cywilnej na gruncie tego przepisu rozważa również A. Szewc, *Z problematyki ochrony danych osobowych*, cz. III, Radca Prawny 5/1999, s. 15 i n.

[48] T. Kuczyński, *Ochrona danych*..., s. 129–130.

cownicy służby publicznej z powodu naruszenia obowiązków pracowniczych[49]. Przez pojęcie „innego przewidzianego prawem postępowania" w przypadku naruszenia zasad ochrony pracowniczych danych osobowych w umownych stosunkach pracy należy rozumieć zastosowanie reguł odpowiedzialności porządkowej według art. 108 i n. k.p.[50] Trzeba bowiem uznać, że ponieważ inspektor może zażądać wszczęcia „postępowania" (dyscyplinarnego lub innego przewidzianego prawem), żądanie to odnosić się więc może wyłącznie do uruchomienia uregulowanej prawnie procedury, w której ramach wskazane zostały przesłanki odpowiedzialności, rodzaje kar, podmioty orzekające, tryb postępowania i środki odwoławcze przysługujące ukaranemu pracownikowi. Zwraca uwagę, iż ustawodawca nie wyposażył inspektora w ogólnie sformułowane prawo żądania od administratora danych osobowych, np. wyciągnięcia konsekwencji czy też podjęcia odpowiednich działań wobec osoby winnej uchybień w przetwarzaniu danych osobowych. Należałoby zatem wykluczyć możliwość żądania przez inspektora wprost zwolnienia pracownika czy też zażądanie, aby pracodawca wystąpił wobec niego na drogę sadową z roszczeniem o odszkodowanie.

Pracodawca ma zatem obowiązek wszcząć na żądanie inspektora przewidziane prawem postępowanie w celu ustalenia odpowiedzialności danego pracownika za stwierdzone w trakcie kontroli naruszenia zasad ochrony danych osobowych. Pracodawca bada zatem, czy istnieją przewidziane w odpowiednich przepisach przesłanki wszczęcia postępowania dyscyplinarnego lub porządkowego i w razie odpowiedzi pozytywnej wszczyna je. Dopiero po zakończeniu tego postępowania jest możliwe np. stwierdzenie przez pracodawcę istnienia lub braku przesłanek do ukarania pracownika zgodnie z odpowiednim reżimem odpowiedzialność i w konsekwencji ukaranie lub rezygnacja z zastosowania kary porządkowej czy dyscyplinarnej wobec pracownika wskazanego jako winnego uchybień przez inspektora. Możliwe jest też przyjęcie kwalifikacji zachowania pracownika jako stanowiącego ciężkie naruszenie obowiązków pracowniczych. W takiej sytuacji zapoznanie się przez pracodawcę z protokołem pokontrolnym przekazanym przez inspektora powinno być traktowane jako powzięcie wiadomości o okolicznościach uzasadniających rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika, data zaś zapoznania się z tym protokołem będzie stanowić punkt wyjścia do liczenia terminu na podjęcie decyzji o zwolnienie pracownika w tym trybie, wskazanego w art. 52 § 2 k.p.[51]

[49] *Ibidem*.

[50] Tak więc, w świetle przepisów ustawy o ochronie danych osobowych, w zależności od podstawy nawiązania stosunku pracy naruszenie obowiązków pracowniczych związanych z ochroną tych danych może być przedmiotem odpowiedzialności dyscyplinarnej lub porządkowej (w przypadku pracowników mianowanych) lub tylko porządkowej (np. w przypadku pracowników zatrudnionych na podstawie umów o pracę); J. Borowicz, *Obowiązek prowadzenia*..., s. 8.

[51] Zgodnie z jego brzmieniem „rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika nie może nastąpić po upływie 1 miesiąca od uzyskania wiadomości o okoliczności uzasadniającej rozwiązanie umowy".