Sygn. akt II PK 37/16

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 4 kwietnia 2017 r.

Sąd Najwyższy w składzie:

SSN Romualda Spyt (przewodniczący)
SSN Bohdan Bieniek
SSN Halina Kiryło (sprawozdawca)

w sprawie z powództwa E.D.
przeciwko Zakładowi Ubezpieczeń Społecznych Oddział w B.
o odszkodowanie,
po rozpoznaniu na posiedzeniu niejawnym w Izbie Pracy, Ubezpieczeń Społecznych i Spraw Publicznych w dniu 4 kwietnia 2017 r.,
skargi kasacyjnej strony pozwanej od wyroku Sądu Okręgowego w B.
z dnia 24 września 2015 r., sygn. akt VI Pa …/15,

uchyla zaskarżony wyrok i przekazuje sprawę Sądowi Okręgowemu w B. do ponownego rozpoznania i rozstrzygnięcia o kosztach postępowania kasacyjnego.

UZASADNIENIE

Powódka E.D. wniosła przeciwko Zakładowi Ubezpieczeń Społecznych Oddziałowi w B. pozew o zapłatę kwoty 20.091,60 zł z ustawowymi odsetkami od dnia doręczenia pozwu do dnia zapłaty, tytułem odszkodowania za rozwiązanie

umowy o pracę bez wypowiedzenia z naruszeniem przepisów o rozwiązaniu umów o pracę w tym trybie.

Wyrokiem z dnia 12 marca 2015 r. Sąd Rejonowy w B. oddalił powództwo.

Sąd pierwszej instancji ustalił, że E.D. zatrudniona była w Zakładzie Ubezpieczeń Społecznych Oddziale w B. na podstawie umowy o pracę od dnia 20 czerwca 1973 r., ostatnio (od dnia 1 lipca 2011 r.) na stanowisku kierownika Referatu Zasiłków. W zakresie swoich obowiązków służbowych powódka uzyskała dostęp do systemu informatycznego pozwanego, służącego do przetwarzania danych osobowych w Zakładzie. W dniu 30 października 2012 r. potwierdziła własnoręcznym podpisem znajomość art. 100 § 2 pkt 4 i 5 k.p., ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz przepisów wykonawczych do tej ustawy, Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych pozwanego oraz procedury prowadzenia postępowań w sytuacji naruszenia ochrony danych osobowych. Jednocześnie oświadczyła, iż jest świadoma odpowiedzialności karnej wynikającej między innymi z art. 266 § 1 k.k., art. 267 § 1 k.k. i art. 268 § 2 k.k. Zobowiązała się także do zachowania w poufności i nieujawniania osobom nieupoważnionym informacji dotyczących zbiorów zawierających dane osobowe lub innych wiadomości, które mogłyby ujawnić jakąkolwiek treść przetwarzanych danych osobowych lub umożliwiać dostęp do nich. Powódka zobowiązana była do dołożenia szczególnej staranności w celu ochrony interesu osób, których dane osobowe są przetwarzane, w szczególności ochrony tych danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz do przetwarzania danych osobowych w celach i w zakresie wynikającym z zajmowanego stanowiska i obowiązującego zakresu obowiązków. Powódka uzyskała upoważnienie do przetwarzania danych osobowych w zakresie danych dotyczących ubezpieczonych, członków rodzin ubezpieczonych i świadczeniobiorców oraz lekarzy, lekarzy dentystów, felczerów, starszych felczerów, których dane są przetwarzane w rejestrze prowadzonym przez Zakład, operacji na danych niezbędnych do wykonywania zadań wynikających ze szczegółowych obowiązków i odpowiedzialności, przetwarzania danych osobowych w systemach informatycznych zgodnie z nadanymi uprawnieniami. Wszystkie

oddziały pozwanego są monitorowane w zakresie bezpieczeństwa ochrony danych osobowych. Monitoring prowadzony jest w cyklach miesięcznych. Raporty przekazywane są za każdy miesiąc bezpośrednio do poszczególnych oddziałów w celu wyjaśnienia rozbieżności.

W dniu 13 października 2014 r. M. J., zatrudniony u pozwanego na stanowisku starszego specjalisty pełniącego obowiązki administratora bezpieczeństwa informacji, otrzymał z Departamentu Zarządzania Bezpieczeństwem Informacji Zakładu wiadomość, że doszło do pobrania danych przez powódkę. Pobranie to wykraczało poza zakres uprawnień powódki. W dniu 14 października 2014 r. M.J. rozpoczął audyt. Powódka została poproszona o wyjaśnienie całej sytuacji. W pisemnym wyjaśnieniu podała, że jest zatrudniona na podstawie umowy zlecenia w Firmie P.W. – J. i do zakresu jej obowiązków należy między innymi przygotowywanie i składanie dokumentów rozliczeniowych składek. W dniu 6 sierpnia 2014 r. dokonała sprawdzenia, czy formularz RZA za miesiąc maj 2014 r. został złożony i przetworzony przez KSI. W tym też dniu dokonała sprawdzenia pozostałej dokumentacji rozliczeniowej składek za miesiąc maj 2014 r. Uczyniła to w godzinach pracy u pozwanego, a celem jej działania było potwierdzenie prawidłowości dokumentacji złożonej przez nią w imieniu zleceniodawcy. Powódka sprawdzając te dane w KSI upewniła się o prawidłowości działań dokonanych na rzecz zleceniodawcy w ramach wiążącej ją umowy cywilnoprawnej. Pracodawca dowiedział się również, że powódka, jako Kierownik Referatu Zasiłków w ZUS Oddział w B., prowadziła poza godzinami pracy szkolenia dla firmy W. W efekcie pozwany uznał, że doszło ze strony powódki do zamierzonego działania spowodowanego świadomym przetwarzaniem danych osobowych z naruszeniem przepisów o ochronie danych osobowych, a sama powódka nie daje rękojmi bezpieczeństwa i poufności przetwarzanych danych i w dniu 16 października 2014 r. rozwiązał łączącą strony umowę o pracę bez wypowiedzenia. Jako przyczynę rozwiązania umowy o pracę wskazał ciężkie naruszenie przez powódkę podstawowych obowiązków pracowniczych, przez naruszenie ochrony danych osobowych zgromadzonych w Zakładzie, polegające na pobraniu informacji z konta płatnika P. W. J., w tym dokumentów ubezpieczonych, zatrudnionych przez tego płatnika oraz wykonywaniu w czasie

pracy czynności na rzecz płatnika, u którego powódka jest zatrudniona na podstawie umowy zlecenia, z nieuzasadnionym wykorzystaniem zasobów zgromadzonych w Zakładzie i przy wykorzystaniu sprzętu Zakładu.

Zdaniem Sądu pierwszej instancji, przyczyna ta była konkretna, rzeczywista i dlatego brak było podstaw do uwzględnienia roszczeń powódki. Wskazana w oświadczeniu pozwanego pracodawcy okoliczność zaistniała i może stanowić podstawę rozwiązania umowy o pracę bez wypowiedzenia, gdyż naruszenie zasady ochrony danych osobowych stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych, a czyn ten był zawiniony przez pracownika. Działanie powódki nosi podejrzenie popełnienia przestępstwa z art. 49 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (jednolity tekst: Dz.U. z 2014 r., poz. 1182). W niniejszej sprawie wystąpił drugi wariant przestępstwa, mianowicie przetwarzanie danych osobowych było wprawdzie dopuszczalne, ale powódka nie była do tego uprawniona, gdyż posiadała ona uprawnienia do korzystania z systemu informatycznego pozwanego jedynie w zakresie swoich obowiązków, jako Kierownika Referatu Zasiłków. Nie ulega wątpliwości, iż przestrzeganie ustawy o ochronie danych osobowych, prawidłowe korzystanie z zasobu danych pozwanego stanowi w przypadku wszystkich pracowników ZUS obowiązek podstawowy, a świadome naruszenie przepisów ustawy o ochronie danych osobowych jest ciężkim naruszeniem podstawowych obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 k.p.

Na skutek apelacji powódki, Sąd Okręgowy w B. wyrokiem z dnia 24 września 2015 r. zmienił zaskarżone orzeczenie w ten sposób, że zasądził od pozwanego na rzecz E.D. kwotę 20091,60 zł z ustawowymi odsetkami od dnia 27 listopada 2014 r. do dnia zapłaty oraz orzekł o kosztach procesu.

Sąd Okręgowy podzielił dokonane ustalenia faktyczne zawarte w uzasadnieniu zaskarżonego wyroku. Uzupełnił je przez stwierdzenie, że upoważnienie powódki, oprócz wskazanego przez Sąd Rejonowy upoważnienia w zakresie danych „dotyczących ubezpieczonych, członków ich rodzin i świadczeniobiorców oraz lekarzy, lekarzy dentystów, felczerów, starszych felczerów, których dane są przetwarzane w rejestrze prowadzonym przez Zakład zgodnie z art. 56 ustawy o świadczeniach pieniężnych z ubezpieczenia

społecznego w razie choroby i macierzyństwa, operacji na danych niezbędnych do wykonywania zadań wynikającego ze szczegółowych obowiązków odpowiedzialności, w systemach informatycznych", obejmowało nadto „przetwarzanie danych osobowych w celach ustalania uprawnień do świadczeń z ubezpieczenia społecznego objętych działaniem oddziału, łącznie z inspektoratami". Faktycznie więc powódka mogła bez żadnych przeszkód zalogować się do systemów informatycznych, uzyskując dostęp do danych przedsiębiorcy, dla którego świadczyła usługi jako księgowa, a także danych z innego oddziału w zakresie aplikacji PI. Powódka mogła bez zgody pozwanego świadczyć usługi na rzecz osoby trzeciej i świadczyła je wobec R. W. prowadzącego P.W. J. w O., na podstawie umowy z 1 kwietnia 2001 r. Umowa ta obejmowała sporządzenie dokumentacji rozliczeniowej składek ZUS. Przedsiębiorca R. W. nie zgłaszał wobec pozwanego pretensji związanych z naruszeniem jego danych osobowych. Dane, do których powódka uzyskała dostęp w dniu 6 sierpnia 2014 r., pochodziły z deklaracji złożonych przez samą powódkę w imieniu tego przedsiębiorcy, a więc i za jego zgodą.

W ocenie Sądu Okręgowego, wraz z ujawnieniem czynu, którego prawnokarna ocena miałaby znaczenie dla rozstrzygnięcia sprawy, Sąd Rejonowy uprawniony był do zawieszenia postępowania, a zgodnie z art. 304 § 2 k.p.k. - zobowiązany do zawiadomienia Prokuratora lub Policji o podejrzeniu popełnienia przestępstwa ściganego z urzędu. Pozwany, podkreślając znaczenie ochrony danych osobowych, nie zawiadomił organów ścigania o podejrzeniu popełnienia przestępstwa, a dyrektor oddziału, bez reakcji ze strony Sądu pierwszej instancji, odmówił odpowiedzi na pytanie, dlaczego do takiego zawiadomienia nie doszło. Uzasadnienie zaskarżonego wyroku nie zawiera jednak rozważań w tym zakresie, dokonaną zatem przez Sąd Rejonowy ocenę o charakterze prawnokarnym Sąd Okręgowy uznał za pozbawioną niezbędnego oparcia i niepopartą dostatecznie zebranym materiałem. Jest tak przede wszystkimi dlatego, że kwestia, czy samo odczytanie albo „wywołanie" danych z systemu informatycznego jest przetwarzaniem danych osobowych, o których mowa w ustawie, jest niejednoznaczna. Piśmiennictwo nie odpowiada kategorycznie na pytanie, czy

samo czytanie danych osobowych jest jego przetwarzaniem. Sprzeciwia się temu również gramatyczna wykładnia terminu „przetwarzanie”.

Sąd Okręgowy uznał za trafny zarzut związany z nierozważeniem przez Sąd pierwszej instancji znaczenia umowy zlecenia z 1 kwietnia 2001 r., która wskazywała na stosunki powódki z płatnikiem, zwłaszcza na wynikające z niej umocowanie do otrzymania informacji na temat dokumentów rozliczeniowych. Zdaniem Sądu odwoławczego, nie można abstrahować od okoliczności, że powódka działała na podstawie umocowania przedsiębiorcy prowadzącego P.W. J. do rozliczeń z pozwanym, w tym do składania deklaracji rozliczeniowych oraz że złożyła deklarację, z której dane pobrała następnie z systemu informatycznego. Tymczasem ustalenia w tym zakresie były istotne dla stwierdzenia naruszenia interesu płatnika lub pozwanego, jako kryterium kwalifikacyjnego ciężkiego naruszenia przez powódkę podstawowych obowiązków pracowniczych. W ocenie Sądu Okręgowego, skoro wniosek o podejrzeniu przestępstwa nie został wystarczająco uzasadniony, kluczowa dla rozstrzygnięcia sprawy była odpowiedź na pytanie o zagrożenie danych osobowych, które akcentował pozwany jako uzasadnienie dla swojego stanowiska oraz o znaczenie zachowania powódki, jako przyczyny zastosowania natychmiastowego trybu rozwiązania umowy o pracę. Zdaniem Sądu drugiej instancji, z zachowaniem powódki nie wiązało się ryzyko ujawnienia danych osobowych płatnika i jego pracowników.

W realiach niniejszej sprawy nie sposób było też przypisać powódce umyślności albo rażącego niedbalstwa, gdyż powódka nie obejmowała świadomością nawet możliwości narażania pracodawcy na szkodę, skoro działając w imieniu płatnika mogła swobodnie, formalnie uzyskać dostęp do informacji zawartych w tym samym systemie informatycznym. Pozwany przedwcześnie zakwalifikował działanie powódki, jako nielegalne przetwarzanie danych osobowych. Powódce można przypisywać wyłącznie jednorazowe, krótkotrwałe wykonywanie czynności na rzecz innej osoby z wykorzystaniem sprzętu pozwanego, co nie stanowiło ciężkiego naruszenia podstawowych obowiązków pracowniczych, tym bardziej, że powódka wykorzystała na to czas przerwy śniadaniowej, którą mogła wyznaczać we własnym zakresie.

Uznając rozwiązanie łączącej strony umowy o pracę za dokonane z naruszeniem obowiązujących przepisów, Sąd drugiej instancji uznał za uzasadnione roszczenia powódki o zasądzenie odszkodowania z art. 56 § 1 w związku z art. 58 k.p.

Pozwany zaskarżył powyższy wyrok skargą kasacyjną. Zaskarżonemu wyrokowi zarzucił naruszenie prawa materialnego, przez niewłaściwe zastosowanie i błędną interpretację art. 7, art. 37 i art. 49 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (jednolity tekst: Dz.U. z 2014 r., poz. 1182). Na tej podstawie wniósł o zmianę zaskarżonego wyroku przez oddalenie powództwa; ewentualnie wniósł o uchylenie zaskarżonego wyroku i przekazanie sprawy Sądowi drugiej instancji do ponownego rozpoznania oraz zasądzenie od powódki na rzecz pozwanego kosztów procesu według norm przepisanych.

Zdaniem pozwanego, w przedmiotowej sprawie doszło do naruszenia powołanych w petitum skargi przepisów, które pozwalały pracodawcy na dokonanie rozwiązania umowy o pracę w szczególnym trybie. Skarżący wskazał, że błędem zdaje się być twierdzenie Sądu drugiej instancji, jakoby sam fakt możliwości użycia do zalogowania do systemu informatycznego karty magnetycznej jest równoznaczny z możnością podglądu wszystkich kont, które dany czytnik otwiera. Po to pracodawca przedkłada do podpisania stosowne obostrzenia w korzystaniu z poszczególnych informacji, aby pracownik korzystał tylko z tych, do których ma formalne uprawnienia. Jak wykazało postępowanie sprawdzające Administratora Bezpieczeństwa Informacji ZUS, powódka nie miała formalnych uprawnień do pobierania danych z konta, które pobrała. Zatem sam fakt technicznej możliwości wejścia do danego systemu nie zwalnia z przestrzegania podpisanych przez pracownika, czyli przyjętych do wiadomości i stosowania, ograniczeń.

W odpowiedzi na skargę kasacyjną powódka wniosła o jej oddalenie oraz zasądzenie kosztów postępowania kasacyjnego.

Sąd Najwyższy zważył, co następuje:

Skarga kasacyjna zasługuje na uwzględnienie.

Analizę prawidłowości zaskarżonego wyroku wypada rozpocząć od przypomnienia, że oparte na art. 56 § 1 i art. 57 § 1 k.p. roszczenia pozwu wywodzone są z dokonanego przez pozwanego pracodawcę Zakład Ubezpieczeń Społecznych Oddział w B. rozwiązania umowy o pracę z powódkę E.D. bez wypowiedzenia z winy pracownika, które – zdaniem powódki - nastąpiło mimo niezaistnienia przyczyny z art. 52 § 1 pkt 1 k.p.

Co do merytorycznej zasadności rozwiązania przedmiotowego stosunku pracy należy zauważyć, że z mocy art. 30 § 4 k.p. na pracodawcy spoczywa obowiązek wskazania w pisemnym oświadczeniu woli przyczyny owego rozwiązania. Przyczyna ta powinna być prawdziwa i konkretna. Konieczne jest zatem należyte skonkretyzowanie czynu pracownika. Istotny pozostaje bowiem przede wszystkim fakt – działanie lub zaniechanie pracownika – z którego pracodawca wywodzi skutki prawne, natomiast nie jest ważne, dlaczego pracodawca kwalifikuje go jako ciężkie naruszenie podstawowych obowiązków pracowniczych. Jeżeli w oświadczeniu woli o rozwiązaniu niezwłocznym, poza ujęciem zarzucanego czynu i jego kwalifikacją jako ciężkiego naruszenia obowiązków pracowniczych, znajdują się jakieś inne elementy (twierdzenia) związane z tym czynem czy jego oceną, to nie mają one znaczenia z punktu widzenia „prawdziwości” podanej przyczyny, jeżeli tylko czyn pracownika miał miejsce. Wskazanie przyczyny lub przyczyn rozwiązania stosunku pracy przesądza o tym, że spór przed sądem pracy może się toczyć tylko w ich granicach. Okoliczności podane pracownikowi na uzasadnienie decyzji o rozwiązaniu stosunku pracy, a następnie ujawnione w postępowaniu sądowym, muszą być takie same, zaś pracodawca pozbawiony jest możliwości powoływania się przed organem rozstrzygającym spór na inne przyczyny mogące przemawiać za słusznością tejże decyzji. Wskazana przyczyna powinna być przy tym na tyle konkretna i zrozumiała, aby nie stwarzała wątpliwości interpretacyjnych, przy czym interpretacja ta nie polega na wykładni oświadczenia woli lecz na ustaleniu, jak pracownik powinien był i mógł ją zrozumieć w kontekście znanych mu okoliczności złożenia oświadczenia o zwolnieniu dyscyplinarnym.

W niniejszym przypadku jako przyczyny rozwiązania umowy o pracę bez wypowiedzenia z winy pracownika nie podano popełnienia przez powódkę

oczywistego lub stwierdzonego prawomocnym wyrokiem sądowym przestępstwa przeciwko ochronie danych osobowych, zatem dywagacje Sądów obu instancji na ten temat są bezprzedmiotowe. Granice kognicji Sądów rozpoznających sprawę zakreśla treść pisemnego oświadczenia woli pracodawcy o rozwiązaniu łączącego strony stosunku pracy i wskazana w nim kwalifikacja zachowania powódki jako ciężkiego naruszenia podstawowych obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 k.p.

Tak kwalifikowane zachowanie pracownika, uzasadniające rozwiązanie przez pracodawcę umowy o pracę bez wypowiedzenia, powinno być bezprawne, zawinione i zagrażające interesom pracodawcy.

Bezprawność zachowania pracownika przejawia się nieprzestrzeganiem przezeń porządku prawnego, a ściślej – naruszeniem podstawowego obowiązku pracowniczego. Obiektywnej cenie podlega fakt, czy pracownik naruszył swoje podstawowe obowiązki. Bezprawność zachowania stanowi element przedmiotowy kwalifikacji danego zachowania. Dla zastosowania przepisu art. 52 § 1 pkt 1 k.p. decydujące znaczenie ma ustalenie, czy dany obowiązek jest podstawowy, a jego naruszenie ma charakter ciężki. Co do samych podstawowych obowiązków pracowniczych trzeba przypomnieć, że zgodnie z art. 22 § 1 k.p., powinnością osoby zatrudnionej jest świadczenie pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem, w miejscu i czasie przez niego wyznaczonym. Świadczenie pracy podporządkowanej jest zatem obowiązkiem podstawowym, który wynika z istoty oraz charakteru stosunku pracy. Szereg przepisów Kodeku pracy precyzuje oraz uszczegóławia tę kwestię. W określeniu, czy dany obowiązek pracowniczy ma charakter podstawowy, bez wątpienia istotne znaczenie ma art. 100 k.p., aczkolwiek zawarty w nim katalog powinności pracowniczych nie jest wyczerpujący. Podstawowe obowiązki pracownicze mogą bowiem wynikać z innych przepisów prawa pracy, a nawet z treści samej umowy o pracę.

Bezprawność zachowania pracownika nie wystarcza jednak do przydania naruszeniu obowiązku pracowniczego charakteru ciężkiego. Określenie „ciężkie naruszenie” należy tłumaczyć z uwzględnieniem stopnia winy pracownika i

zagrożenia dla interesów pracodawcy powstałego wskutek jego działania (zaniechania).

Wina pracownika stanowi element podmiotowy kwalifikacji zarzucanego czynu, a ocenie podlega subiektywne nastawienie psychiczne sprawcy do swojego działania (zaniechania). Warunkiem zastosowania art. 52 § 1 pkt 1 k.p. jest zatem stosunek psychiczny pracownika do skutków swojego postępowania, określony wolą i możliwością przewidywania, czyli świadomością w zakresie naruszenia obowiązku (obowiązków) o podstawowym charakterze oraz negatywnych skutków, jakie zachowanie to może spowodować dla pracodawcy. Rozwiązanie umowy o pracę w trybie dyscyplinarnym jest uzasadnione w przypadku wystąpienia po stronie pracownika winy umyślnej lub rażącego niedbalstwa.

Wreszcie kwestia naruszenia lub zagrożenia interesów pracodawcy nierozerwalnie łączy się z uznaniem danego obowiązku pracowniczego za podstawowy, a jego naruszenia - za zawinione. Naruszenie lub zagrożenie interesów pracodawcy nie musi przy tym polegać na wyrządzeniu szkody majątkowej. Pojęcie to obejmuje bowiem także elementy niematerialne, jak np. dyscyplina pracy.

Wystąpienie wskazanych przesłanek kwalifikacyjnych ciężkiego naruszenia podstawowych obowiązków pracowniczych należy analizować łącznie w każdym konkretnym stanie faktycznym, z uwzględnieniem wszystkich okoliczności danego przypadku.

W przedmiotowej sprawie przyczyną rozwiązania przez pozwany Zakład Ubezpieczeń Społecznych Oddział w B. umowy o pracę z powódką E. D. bez wypowiedzenia z winy pracownika było sprawdzenie przez powódkę w Komputerowym Systemie Informatycznym pracodawcy prawidłowości dokumentacji rozliczeniowej składek na ubezpieczenia społeczne, przygotowanej i złożonej przez nią w imieniu płatnika P.W. J., dla której to firmy świadczyła usługi w ramach umowy zlecenia. Opisane zachowanie zostało uznane przez pracodawcę za ciężkie naruszenie podstawowych obowiązków w rozumieniu art. 52 § 1 pkt 1 k.p., przy czym kwalifikacja ta jest dwustopniowa. Zdaniem pozwanego, czyn powódki stanowi: 1/ naruszenie ochrony danych osobowych zgromadzonych w Zakładzie, polegające na pobraniu informacji z konta płatnika P. W. J., w tym dokumentów

ubezpieczonych zatrudnionych przez tego płatnika oraz 2/ wykonywanie w czasie pracy czynności na rzecz płatnika, u którego powódka jest zatrudniona na podstawie umowy zlecenia, z nieuzasadnionym wykorzystaniem zasobów zgromadzonych w Zakładzie i przy wykorzystaniu sprzętu Zakładu.

Wbrew stanowisku Sądu Okręgowego, druga z powyższych kwalifikacji zachowania powódki jako deliktu pracowniczego nie powinna budzić wątpliwości. Jak bowiem wskazano wyżej, zgodnie z art. 22 § 1 k.p. podstawowym obowiązkiem pracownika jest świadczenie pracy określonego rodzaju na rzecz pracodawcy i pod jego kierownictwem, w miejscu i czasie przez niego wyznaczonym. Doprecyzowaniem tego obowiązku w art. 100 § 1 i § 2 pkt 1 i 2 k.p. jest zaś wykonywanie pracy sumiennie i starannie oraz stosowanie się do poleceń przełożonych dotyczących pracy, a także przestrzeganie ustalonego w zakładzie czasu pracy oraz regulaminu pracy i ustalonego porządku. Niewątpliwie wykonywanie bez wiedzy i zgody przełożonych, w miejscu i czasie pracy oraz przy wykorzystaniu sprzętu i zgromadzonych przez pracodawcę zasobów danych osobowych, czynności na rzecz innego niż pracodawca podmiotu w ramach łączącego pracownika z tymże podmiotem odrębnego stosunku zatrudnienia, jest w świetle powołanych przepisów zachowaniem bezprawnym i zawinionym. Trudno bowiem zakładać, że powódka nie była świadoma niedopuszczalności realizowania treści zawartej z firmą P.W. J. umowy zlecenia w miejscu i czasie przeznaczonym na wykonywanie pracy u pozwanego. Usprawiedliwieniem dla takiego zachowania nie może być rzekome świadczenie wspomnianej usługi podczas tzw. przerwy śniadaniowej. Przerwa ta zgodnie z art. 134 k.p. podlega wliczeniu do czasu pracy i wynagrodzeniu, a jej celem jest odpoczynek i regeneracja sił przed dalszą pracą w ramach obowiązującego pracownika dobowego wymiaru czasu pracy trwającego więcej niż 6 godzin. Celem przerwy śniadaniowej nie jest zatem umożliwienie pracownikowi świadczenia usług na rzecz innego podmiotu i to w czasie traktowanym jako czas pracy (tj. w myśl art. 128 § 1 k.p., czas pozostawania do dyspozycji pracodawcy w zakładzie lub innym miejscu przeznaczonym na wykonywanie pracy) i objętym wynagrodzeniem wypłacanym przez pracodawcę.

Kwestia legalności wykorzystania przez powódkę zgromadzonych przez pozwanego danych osobowych płatnika składek i zatrudnionych przezeń

ubezpieczonych wymaga natomiast rozważenia w ramach pierwszego z zarzucanych przez pracodawcę naruszeń podstawowych obowiązków pracowniczych.

W tej materii warto przypomnieć, że gromadzone przez Zakład Ubezpieczeń Społecznych na podstawie przepisów ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (jednolity tekst: Dz.U. z 2016 r., poz. 963 ze zm.) i rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 21 grudnia 2009 r. w sprawie szczegółowego zakresu danych zawartych w centralnych rejestrach prowadzonych przez Zakład Ubezpieczeń Społecznych (jednolity tekst: Dz.U. z 2013 r., poz. 219) dane osobowe płatników składek i ubezpieczonych stanowią zbiór danych w rozumieniu art. 7 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (jednolity tekst: Dz.U. z 2016 r., poz. 922; dalej jako ustawa o o.d.o.), jakim jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany czy rozproszony, czy jest jednolity czy podzielony funkcjonalnie lub geograficznie, czy wreszcie jest zautomatyzowany czy niezautomatyzowany. Pojęcie to należy zaś do podstawowych terminów ustawy, wyznaczając zakres stosowania jej przepisów. Będąc zgodnie z art. 7 pkt 4 ustawy o o.d.o. administratorem danych osobowych, czyli mającą osobowość prawną państwową jednostką organizacyjną, o jakiej mowa w art. 3 ust. 1 ustawy, decydującą o celach i środkach przetwarzania danych osobowych (tj. faktycznie podejmującą we własnym imieniu decyzje w stosunku do danych podlegających przetworzeniu, za które to decyzje ponosi odpowiedzialność administracyjną), Zakład Ubezpieczeń Społecznych ma rozległe obowiązki informacyjne w stosunku do tych, których dotyczą zbierane i przetwarzane dane osobowe (art. 24, art. 25, art. 32, art. 33 i art. 54 ustawy o o.d.o.), a także obowiązek dbania o legalność i rzetelność przetwarzania danych osobowych (art. 26 i art. 49 ustawy o o.d.o), obowiązek dbania o zachowanie danych w poufności (art. 37 – 39, art. 51 ustawy o o.d.o.), obowiązek zabezpieczenia zbioru danych osobowych (art. 36 – 39, art. 52 ustawy o o.d.o.) i jego rejestracji (art. 40 – 46, art. 53 ustawy o o.d.o.). Administratorem danych nie jest każdy dysponent danych osobowych, a tylko ten, kto decyduje o celach i środkach ich przetwarzania. Wobec odesłania zawartego w

art. 7 pkt 4 ustawy o o.d.o., administratorem danych może być jedynie podmiot wymieniony w art. 3 ustawy o o.d.o. Jeśli jest nim w myśl ust. 1 tego artykułu organ państwowy lub organ samorządu terytorialnego albo państwowa lub komunalna jednostka organizacyjna, to administratorem danych nie jest osoba pełniąca funkcje kierownicze w tym organie lub jednostce organizacyjnej ani oznaczony pracownik, któremu powierzono wykonywanie obowiązków związanych z ochroną i operacjami na danych osobowych. Legitymowanie się upoważnieniem administratora danych do przetwarzania danych osobowych zgromadzonych w zbiorze nie czyni upoważnionego administratorem danych, nie wyposaża go w przypisaną tylko administratorowi kompetencję samodzielnego decydowania o celach i środkach przetwarzania danych osobowych. Osoba upoważniona dokonuje operacji na danych osobowych tylko w zakresie wyznaczonym przez administratora. Nie można na taką osobę scedować funkcji administratora danych, którym pozostaje podmiot wymieniony w art. 3 ust. 1 ustawy o o.d.o. Rację ma więc skarżący zauważając, że samo wyposażenie powódki w kartę magnetyczną do zalogowania się do systemu informatycznego Zakładu Ubezpieczeń Społecznych nie oznaczało uprawnienia do niczym nieograniczonego korzystania ze zgromadzonych w tym systemie danych osobowych klientów Zakładu.

Obowiązek zachowania informacji o klientach w tajemnicy jest obowiązkiem pracowniczym wynikającym z przepisów prawa powszechnie obowiązującego (art. 100 § 2 pkt 4 i 5 k.p.), a tym samym niezależnym od zastrzeżenia go w treści umowy o pracę lub upoważnienia do przetwarzania danych osobowych. Pracownik mający dostęp do danych osobowych klientów pracodawcy nie zyskuje statusu administratora danych, lecz pozostaje osobą dopuszczoną do przetwarzania danych osobowych na podstawie imiennego upoważnienia nadanego przez administratora – pracodawcę. Wymóg wydania upoważnienia do przetwarzania danych osobowych klientów pracodawcy pracownikom zatrudnionym przy przetwarzaniu danych osobowych wynika z art. 37 ustawy o o.d.o. Przepis ten ma na celu zapewnienie prawidłowości, a w szczególności poufności przetwarzania danych osobowych. Zakresem stosowania tego przepisu objęty jest każdy przypadek przetwarzania danych osobowych w zbiorze danych, bez względu na to, czy zbiór jest prowadzony w systemie informatycznym czy poza tym systemem.

Upoważnienie administratora danych jest konieczne do wykonywania jakiejkolwiek operacji na danych osobowych. Upoważnienie takie mają głównie pracownicy przetwarzający dane osobowe stale, w związku z zatrudnieniem na stanowisku, na którym rutynowo w efekcie wykonywania obowiązków ze stosunku pracy dane te są przetwarzane. Powinny się nim wykazać jednak nie tylko osoby, które na stałe zajmują się przetwarzaniem danych, pracownicy administratora, ale także osoby czasowo wykonujące czynności w tym zakresie, jak również osoby dokonujące przeglądów serwisowych sprzętu czy oprogramowania, osoby mające usunąć usterki czy awarie, z tego względu, że mają one dostęp do danych osobowych, a zatem można uznać, że przetwarzają dane (np. jeżeli mogą się zapoznać z treścią danych). Upoważnienie takie nie jest natomiast konieczne, gdy upoważnienie oraz obowiązek przetwarzania danych osobowych wynikają z przepisów ustawowych. W praktyce nadanie upoważnienia powinno być związane z podpisaniem przez osobę odbierającą upoważnienie oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz o przyjęciu do wiadomości obowiązku zachowania tajemnicy.

Przepis art. 37 ustawy o o.d.o. ustanawia zakaz dopuszczania osób innych niż mające upoważnienie nadane przez administratora danych, do przetwarzania danych osobowych. Oznacza to, że do przetwarzania danych nie jest wystarczające upoważnienie wynikające ze stosunku prawnego łączącego daną osobę z administratorem danych, np. w związku z zawarciem umowy o pracę czy umowy zlecenia albo innej umowy o świadczenie usług, do której stosuje się odpowiednio przepisy o zleceniu. Ustawa o o.d.o. nie określa wymagań kwalifikacyjnych, jakie muszą spełniać osoby upoważnione do przetwarzania danych osobowych. Nie oznacza to jednak, że administrator danych może nadawać upoważnienia do przetwarzania danych dowolnym osobom. Zgodnie z art. 26 ust. 1 ustawy, administrator danych jest bowiem obowiązany dołożyć szczególnej staranności w doborze osób upoważnionych do przetwarzania danych osobowych.

Ustawodawca nie określił formy i treści takiego upoważnienia, ale ze względów dowodowych należy przyjąć formę pisemną. Upoważnienie to powinno mieć charakter imienny – w jego treści należy wyraźnie wskazać osobę dysponującą tym upoważnieniem oraz zakres przetwarzania danych osobowych

realizowanych na jego podstawie. Brak precyzyjnego wyznaczenia zakresu upoważnienia należy kwalifikować jako niezgodny z prawem. Administrator danych jest bowiem obowiązany sprecyzować zakres upoważnienia, jaki jest konieczny do prawidłowego wykonywania obowiązków przez upoważnionego. Obowiązek taki nie został ustanowiony wyraźnie w ustawie o o.d.o., lecz mieści się w ramach ogólnego obowiązku zabezpieczenia danych osobowych (art. 36 ust. 1 ustawy), a także stanowi przejaw szczególnej staranności administratora danych w celu ochrony osób, których dane dotyczą (art. 26 ust. 1 ustawy). Zakresy upoważnień do przetwarzania danych osobowych powinny być ustalone tak, aby zapewnić realizację obowiązku wynikającego z art. 38 ustawy o o.d.o. Natomiast pracownicy (osoby upoważnione do przetwarzania danych osobowych) powinni mieć faktyczny dostęp do danych osobowych tylko w zakresie udzielonych upoważnień.

W literaturze zauważa się, że komentowany przepis stanowi obecnie swoisty odpowiednik postanowienia zawartego w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23 listopada 1995 r., s. 31), w myśl którego osoby, które są podporządkowane administratorowi lub wykonującemu przetwarzanie na zlecenie mające dostęp do danych osobowych, jak i sama osoba przetwarzająca dane na zlecenie administratora, mogą te dane przetwarzać tylko na polecenie administratora, chyba że istnieją w tej mierze zobowiązania ustawowe. Wynika to z całokształtu regulacji ustawowej, która odpowiedzialnym za przetwarzanie danych czyni administratora. Tego rodzaju podejście, jak podnoszą komentatorzy dyrektywy, statuuje nie tyle zobowiązanie do przestrzegania tajemnicy danych, ile raczej pewien rodzaj ogólnego (powszechnego) obowiązku posłuszeństwa względem administratora. Byłby on naruszony w każdym przypadku przetwarzania danych wykraczającym poza wskazówki (polecenia) administratora lub sprzeciwiającym się im, nawet przy zachowaniu poufności danych (por. J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych Komentarz, wydanie VI, LEX 2015, komentarz do art. 37).

W myśl art. 7 pkt 2 ustawy o o.d.o. przetwarzanie danych oznacza jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie,

utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Przetwarzanie danych osobowych należy do sfery czynności faktycznych, określanych jako czynności materialno – techniczne, z których to czynności wypływają konsekwencje prawne. W legalnej definicji przetwarzania danych ustawodawca wskazuje przykładowo operacje wykonywane na danych. Kolejność tych operacji wskazana w art. 7 pkt 2 ustawy nie jest przypadkowa i może być przydatna do ustalenia ram czasowych przetwarzania danych. O przetwarzaniu danych można mówić począwszy od zbierania danych, a skończywszy na ich usunięciu. Zarówno przed zbieraniem, jak i po usunięciu danych osobowych nie może być mowy o ich przetwarzaniu i tym samym o stosowaniu ustawy o o.d.o. Zdaniem J. Barta, przetwarzanie danych osobowych oznacza jakiekolwiek operacje wykonywane na danych osobowych od ich pozyskania do usunięcia (wymazania). Terminem tym objęte są takie działania, jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, łączenie zestawiane, wywoływanie, udostępnianie, rozpowszechnianie, przesyłanie, usuwanie, a zwłaszcza te, które wykonywane są w systemach komputerowych. Wystarczy zatem, że wykonywana jest którakolwiek z podanych operacji (np. samo zbieranie danych), a nawet operacja inna niż wymieniona w tym przepisie, mająca za przedmiot dane osobowe, aby należało uznać, iż dochodzi do przetwarzania danych, co otwiera drogę do stosowania regulacji zawartej w ustawie o o.d.o. Można nawet twierdzić, że samo czytanie danych osobowych przez administratora danych lub jego pracownika stanowi przetwarzanie danych w rozumieniu ustawy (por. J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych Komentarz, wydanie VI, LEX 2015, komentarz do art. 7).

Użyty w art. 7 pkt 2 ustawy o o.d.o. w odniesieniu do przetwarzania danych zwrot „a zwłaszcza te, które wykonuje się w systemach informatycznych”, nie oznacza, że ustawa wprowadza rozróżnienie między automatycznym i niezautomatyzowanym (ręcznym) przetwarzaniem danych osobowych. Oznacza on tyle, że nawet wtedy, gdy określonej operacji na danych osobowych nie można określić jako zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie (a może to mieć miejsce zwłaszcza w systemie

informatycznym), to i tak jest ona przetwarzaniem danych w rozumieniu ustawy o o.d.o. (por. A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, wydanie IV, LexisNexis 2008, komentarz do art. 7). Stwierdzenie ustawodawcy, że przetwarzaniem danych są zwłaszcza operacje wykonywane w systemach informatycznych, ma za zadanie podkreślenie rangi problematyki przetwarzania danych z wykorzystaniem nowoczesnej techniki informatycznej i przypomnienie o potrzebie poddania tej sfery ocenie prawnej z punktu widzenia ustawy o o.d.o. Przepis art. 7 pkt 2a ustawy o o.d.o. definiuje system informatyczny jako zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, natomiast przepis art. 7 pkt 2b ustawy wprowadza definicję zabezpieczenia danych w systemie informatycznym jako wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem, zaś przepisy rozdziału 5 ustawy o o.d.o. nakładają na administratora danych obowiązki związane z zabezpieczeniem danych osobowych, tak w zakresie zabezpieczenia danych przetwarzanych w systemie informatycznym, jak i zabezpieczenia danych przetwarzanych poza tym systemem.

Jak zauważył Naczelny Sąd Administracyjny w uzasadnieniu wyroku z dnia 19 grudnia 2001 r., II SA 2869/2000 (ONSA 2003 nr 1, poz. 29), posługiwanie się taką czy inna techniką utrwalania danych (kopiowanie lub przepisywanie) nie przesądza samo przez się o legalności albo nielegalności tego utrwalania (przetwarzania). Dla takich ocen istotne znaczenie mają przede wszystkim: podstawa prawna przetwarzania danych (art. 23 ustawy o o.d.o.), rodzaj przetwarzanych danych (art. 27 ustawy o o.d.o.) oraz granice przetwarzania (art. 26 ust. 1 pkt 3 ustawy o o.d.o.).

Jeżeli chodzi o tzw. dane drażliwe czy sensytywne, to przesłanki ich przetwarzania reguluje art. 27 ustawy o o.d.o. Natomiast art. 23 ustawy normuje przesłanki przetwarzania tzw. danych zwykłych. Owo przetwarzanie może mieć miejsce w sytuacji, gdy 1/ następuje za zgodą osoby zainteresowanej; 2/ oparte jest na uprawnieniu lub obowiązku wynikającym z przepisów prawa; 3/ jest niezbędne do realizacji umowy, której stroną jest osoba, której dane dotyczą; 4/ jest niezbędne

do podjęcia działań przed zawarciem umowy na zadanie osoby, której dane dotyczą; 5/ jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; 6/ jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, a nie jest możliwe uzyskanie zgody osoby zainteresowanej; 7/ jest niezbędne do wypełnienia prawnie usprawiedliwionych celów przez administratorów danych lub odbiorców danych. Przy tym dodatkowe wymogi są przewidziane wówczas, gdy przetwarzanie danych następuje w innym celu niż ten, dla którego były zebrane. Przepis art. 26 ust. 2 ustawy o o.d.o. nakazuje wówczas, aby przetwarzanie danych nie naruszało praw i wolności osób, których dotyczą oraz następowało w celach badań naukowych, dydaktycznych, historycznych lub statystycznych.

Nie ulega wątpliwości, że dokonując operacji polegającej na pobraniu ze zbioru danych osobowych Zakładu Ubezpieczeń Społecznych informacji z konta płatnika składek P.W. J., E.D. uczyniła to niezgodnie z celem, dla jakiego zbiór ten stworzono (bo nie w ramach realizacji ustawowych zadań Zakładu, lecz dla wykonania umowy zlecenia łączącej powódkę z płatnikiem składek) i z przekroczeniem zakresu udzielonego jej przez administratora danych upoważnienia do przetwarzania danych osobowych. Należy odróżnić sytuację, gdy płatnik składek P.W. J. jako administrator danych osobowych swoich pracowników – ubezpieczonych upoważnia powódkę do przetwarzania tych danych w ramach umowy zlecenia na usługę sporządzenia dokumentacji rozliczeniowej do Zakładu Ubezpieczeń Społecznych, od sytuacji, gdy E.D. będąc pracownikiem Zakładu Ubezpieczeń Społecznych dokonuje operacji na danych osobowych wspomnianego płatnika składek i jego pracowników zgromadzonych w zbiorze administrowanym przez Zakład i czyni to sprzecznie z ustawowym celem, dla jakiego zbiór ten utworzono oraz z naruszeniem zasad wynikających z powołanych art. 23 i art. 27 ustawy o o.d.o., a zarazem z przekroczeniem udzielonego przez administratora upoważnienia do przetwarzania danych osobowych, gdyż upoważnienie to nie dotyczyło wykonywania operacji na danych osobowych płatnika i ubezpieczonych w celu realizacji łączącej powódkę z owym płatnikiem umowy zlecenia, o której zawarciu przez strony Zakład nie został nawet poinformowany. Nie można zasadnie twierdzić, że spełniona została ta przesłanka dopuszczalności przetwarzania

danych osobowych z art. 23 ustawy o o.d.o., jaką jest niezbędność owego przetworzenia do realizacji umowy, której stroną jest osoba, której dane dotyczą. Administratora danych, tj. Zakładu Ubezpieczeń Społecznych i podmiotów, których dane osobowe przetworzono (czyli płatnika składek P.W. J. i jego pracowników) nie łączyła żadna umowa, dla wykonania której powódka dokonała przetworzenia owych danych. Nie sposób też zgodzić się z tezą o przeprowadzeniu przez powódkę opisanych operacji na danych osobowych płatnika i jego pracowników za zgodą podmiotu, którego dane dotyczą, o jakiej to zgodzie mowa w powołanym przepisie. Zgoda taka, będąca oświadczeniem woli, powinna być bowiem złożona administratorowi danych i jemu też należałoby udzielić zgody na udostępnienie tychże danych kolejnym podmiotom. Zachowanie powódki stanowi naruszenie podstawowych obowiązków pracowniczych wynikających z art. 100 § 2 pkt 4 i 5 k.p. oraz powołanych wyżej przepisów ustawy o o.d.o., do których przestrzegania powódka zobowiązała się w stosownym oświadczeniu woli. Trudno bronić tezy, by opisany delikt pracowniczy nie miał zawinionego charakteru. Powódka znała zakres udzielonego jej przez pracodawcę upoważnienia do przetwarzania danych osobowych zawartych w zbiorze Zakładu, a podpisując stosowne oświadczenie o znajomości przepisów dotyczących ochrony owych danych miała świadomość, jakie znaczenie przypisuje tejże ochronie zarówno ustawodawca, jak i pozwany. Nie sposób przyjąć, by nie zdawała sobie sprawy z tego, że dokonując bez upoważnienia operacji na danych osobowych płatnika i jego pracowników narusza ciążące na niej obowiązki pracownicze. Nie należy też – jak uczynił to Sąd drugiej instancji - bagatelizować skutków tego rodzaju bezprawnych zachowań osób legitymujących się upoważnieniem do przetwarzania danych osobowych, zwłaszcza gdy mieć na uwadze rozmiary zbioru danych osobowych, jakimi administruje Zakładu Ubezpieczeń Społecznych i konieczność zapewnienia przez administratora tymże danym właściwej ochrony oraz przedsiębrania w tym zakresie stosownych środków, miedzy innymi przez odpowiedni dobór osób mających dostęp do zbioru, właściwe określenie ich kompetencji w przedmiocie przetwarzania danych oraz kontrolę nad sposobem realizowania przez nie udzielonych im upoważnień. Jak bowiem zauważono wyżej, instytucja upoważnienia przez administratora danych do ich przetwarzania statuuje nie tyle

zobowiązanie do przestrzegania tajemnicy danych, ile raczej pewien rodzaj ogólnego (powszechnego) nakazu posłuszeństwa względem administratora, na którym spoczywają liczne obowiązki w zakresie ochrony danych osobowych i który ponosi z tego tytułu odpowiedzialność prawną. W niedopełnieniu przez pracownika upoważnionego do przetwarzania danych osobowych tegoż nakazu trzeba upatrywać naruszenia interesów pracodawcy.

Podzielając zatem kasacyjne zarzuty naruszenia prawa materialnego przy ferowaniu zaskarżonego wyroku, Sąd Najwyższy z mocy art. 398^{15} § 1 k.p.c. oraz art. 108 § 2 k.p.c. w związku z art. 398^{21} k.p.c. orzekł jak w sentencji.

kc