DR WOJCIECH RAFAŁ WIEWIÓROWSKI – GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH – WYJAŚNIA

GIODO

PYTANIE:

Czy pracodawca może kontrolować pracowników w zakresie korzystania przez nich z Internetu, poczty elektronicznej czy telefonu, jak również stosowania wobec nich videomonitoringu?

ODPOWIEDŹ:

Tak, ale jednocześnie z poszanowaniem prawa do prywatności i ochrony danych osobowych każdego pracownika, przy czym pracodawca powinien poinformować pracowników o zakresie i celu prowadzonej kontroli przed jej rozpoczęciem.

UZASADNIENIE:

Pracodawca – co do zasady – ma prawo kontrolować pracowników, ale musi przy tym uwzględniać gwarantowane im przepisami Konstytucji RP i Kodeksu cywilnego prawo do prywatności i poszanowania dóbr osobistych. Zresztą zobowiązuje go do tego także art. 11^1 Kodeksu pracy.

Z kolei biorąc pod uwagę te przepisy Kodeksu pracy, które zobowiązują pracownika do sumiennego wykonywania swoich obowiązków oraz przestrzegania czasu pracy, to należy uznać, że w godzinach pracy nie powinien się on zajmować prywatnymi sprawami, np. prywatną korespondencją. Skoro zaś pracodawca wyposaża pracowników w odpowiednie narzędzia pracy, w tym komputer czy telefon komórkowy, to nie musi godzić się na wykorzystywanie ich do celów prywatnych. Ponadto ma prawo kontrolować, co pracownicy robią w godzinach pracy, w tym – do czego wykorzystują udostępnione im narzędzia.

Jednak w każdym przypadku, gdy pracodawca zdecyduje się na kontrolowanie pracowników (również w każdej z poniżej wymienionych przykładowych sytuacji), powinien poinformować pracownika o zakresie i celu prowadzonej kontroli. Informacja taka powinna zostać przekazana przed rozpoczęciem działań kontrolnych.

Dopuszczalne jest także, by pracodawca w celu ochrony tajemnicy przedsiębiorstwa zabronił pracownikom korzystania z Internetu, e-maila czy telefonu do celów innych niż służbowe i zastrzegł sobie prawo do kontrolowania również treści przesyłek czy rozmów. Jednak może tak postąpić tylko wtedy, gdy pracownik zostanie o tym uprzednio poinformowany, a nie dopiero wtedy, gdy pracodawca uzna, że nastąpiło przekroczenie zasad, które w przedsiębiorstwie obowiązują.

Obecnie większość firm domaga się, aby pracownicy korzystali ze służbowych skrzynek tylko do celów zawodowych. Dzięki temu pracodawca chroni swoje interesy, a jednocześnie nie ogranicza znacząco praw pracownika.

Jeśli generalnie pracodawca nie zezwala np. na używanie służbowych komputerów do celów prywatnych, ma prawo sprawdzić, czy ten zakaz jest respektowany. Jeżeli nie jest, może wyciągnąć wobec pracownika konsekwencje służbowe. Kontrolę tę może sprawować, sprawdzając np. sposób wykorzystywania Internetu (także przez zainstalowanie specjalnego oprogramowania) lub zawartość służbowej skrzynki e-mailowej pracownika. W przypadku przeglądania skrzynki e-mailowej pracodawca może uznać, że cała korespondencja wpływająca na służbową skrzynkę jest korespondencją służbową. I aby rzeczywiście to sprawdzić, jedynym rozwiązaniem jest czytanie całej poczty. U niektórych pracodawców konieczne może być nawet sprawdzanie, czy w listach sprawiających wrażenie prywatnych wiadomości pracownik nie ukrywa informacji, które mogą mieć charakter tajemnicy przedsiębiorstwa.

Trzeba jednak pamiętać, że taka ingerencja w pocztę pracownika jest rozwiązaniem skrajnym i może być dokonywana jedynie wówczas, gdy pracownik wie, że pracodawca zastrzegł sobie do tego prawo. Ponadto trzeba pamiętać, że okoliczności każdego przypadku sprawdzania poczty są różne. Podobnie jak przepisy regulaminów pracy w danych firmach. Zarzutów naruszenia tajemnicy korespondencji nie muszą obawiać się ci pracodawcy, którzy wprowadzą precyzyjne przepisy wewnątrzzakładowe i właściwie przedstawią je podwładnym.

Pracodawca ma również prawo wglądu do zapisanych w komputerze informacji służbowych. Jeśli pracownik zabezpieczył je hasłem, to na żądanie pracodawcy musi je udostępnić. Natomiast swoje prywatne materiały pracownik może zapisywać na komputerze tylko za zgodą przełożonego.

Jeżeli zaś pracodawca ustali, że pracownik na służbowym komputerze nie powinien instalować np. komunikatorów internetowych czy korzystać z serwisów społecznościowych w pracy, to podwładny musi się do tego dostosować, a pracodawca może sprawdzać, w jaki sposób podwładni korzystają ze sprzętu komputerowego lub Internetu, bo to narzędzia pracy dostarczone przez pracodawcę. Zawsze jednak pracodawca musi pamiętać o obowiązku poinformowania pracownika o swoim podejściu dotyczącym możliwości korzystania ze służbowego komputera do celów prywatnych i o ewentualnych kontrolach w tym zakresie. Może to zrobić, wprowadzając stosowne zapisy do regulaminu pracy lub innych dokumentów regulujących prawa i obowiązki stron stosunku pracy. Pracownicy zaś powinni się tym zaleceniom podporządkować.

Warto też wspomnieć, że pracodawca ma prawo zakazać wnoszenia i używania w pracy płyt CD, DVD i pamięci USB.

Jeżeli chodzi o instalowanie w zakładach pracy wideomonitoringu, to działanie takie powinno być uzasadnione konkretnym celem. Instalowanie kamer może być z jednej strony uznane za środek poprawiający bezpieczeństwo określonych miejsc (np. pomieszczeń, w których są przechowywane pieniądze lub wartościowe przedmioty), z drugiej jednak strony ich instalowanie w celu kontroli jakości pracy wykonywanej przez podwładnych wymaga analizy w kontekście ochrony prawa do prywatności oraz dóbr osobistych pracownika. W szczególności powinna zostać zachowana równowaga między bezpieczeństwem a prawem do godności i prywatności. Ważne jest, aby pracodawca podczas rejestrowania obrazu nie naruszał powyższych praw. Pracodawca przed zainstalowaniem kamer powinien zastanowić się, czy nie istnieją inne mniej ingerujące w prywatność środki umożliwiające osiągnięcie tego samego celu. Zwracała na to uwagę m.in. Grupa Robocza Art. 29 do spraw ochrony danych osobowych (będąca europejskim organem doradczym) w swojej opinii 4/2009. Jak uznała, urządzenia wideonadzoru mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony lub bezpieczeństwa, o charakterze fizycznym lub logicznym, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami.

W tym kontekście warto też wskazać na Rekomendację Nr R (89) 2 Komitetu Ministrów Rady Europy z 18 stycznia 1989 r. o ochronie danych osobowych wykorzystywanych na potrzeby zatrudnienia, nakazującą – poza poszanowaniem życia prywatnego i godności ludzkiej pracowników – informowanie ich lub konsultowanie się z nimi przed wprowadzeniem zautomatyzowanych systemów gromadzenia i wykorzystywania danych, ze szczególnym uwzględnieniem możliwości nawiązywania kontaktów towarzyskich i indywidualnych w miejscu pracy. Uregulowanie to jest istotne zwłaszcza dlatego, że polskie przepisy prawa pracy nie przewidują stosowania wideonadzoru w miejscu pracy.