Monitoring pracownika. Uwaga - nie wszystkim, wszystko wolno!

Kategoria: Felietony
Opublikowano: wtorek, 01, styczeń 2013 23:00
Bernadeta Skóbel

Pracownicy powinni mieć świadomość, iż sa poddawani monitoringowi przez pracodawcę. Taki monitoring, jak podkreśla się w piśmiennictwie, musi spełniać wymogi zgodności z prawem, usprawiedliwionego celu, proporcjonalności, transparentności oraz uwzględnienia przepisów o ochronie danych osobowych. Wymóg transparentności oznacza zaś, że pracownicy powinni mieć świadomość, iż są poddawani monitoringowi. Pracodawca winien zatem szczegółowo określić zasady monitoringu i zapoznać z nimi pracowników, którzy fakt zapoznania się powinni potwierdzić stosownym podpisanym oświadczeniem o ich akceptacji.

Prezentujemy ciekawe orzeczenie Wojewódzkiego Sądu Admninistarcyjnego z dnia 6 czerwca 2012 r. sygn. II SA/Wa 453/12 (źródło: Centralna Baza Orzeczeń Sądów Administarcyjnych). W uzasadnieniu wskazno m.in. że oprogramowanie zbierające informacje o połączeniach pomiędzy siecią wewnętrzną a siecią publiczną, zastosowane w ramach monitoringu (kontroli) działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych, w istocie stanowi też monitoring pracownika w miejscu pracy, jeżeli pozwala na sprawdzenie wykazów odwiedzanych stron internetowych, czasu zainicjowanych połączeń, adresów stron lub plików, z którymi nastąpiło połączenie.

Kwestie monitoringu w miejscu pracy były wielokrotnie przedmiotem orzecznictwa Europejskiego Trybunału Praw Człowieka. W wyroku z dnia 3 kwietnia 2007 r. w sprawie Copland przeciwko Zjednoczonemu Królestwu (sygn. 62617/00, Lex nr 527588), dotyczącym monitorowania przez przełożonego w miejscu pracy telefonu, poczty elektronicznej i połączeń internetowych Lynette Copland, przy czym monitorowanie użytkowania Internetu przybrało postać analizy odwiedzanych stron, daty i czasu odwiedzin oraz długości ich trwania, Trybunał uznał, że rozmowy telefoniczne z pracy, e-maile i użytkowanie internetu są objęte terminami "życie prywatne" i "tajemnica korespondencji". Podniósł też, że powódka nie została nigdy ostrzeżona, że jej rozmowy, e-maile oraz korzystanie z internetu mogą być monitorowane, a więc miała uzasadnione oczekiwanie zachowania ich prywatności.

Trybunał stwierdził, że w sprawie doszło do ingerencji w prawa zagwarantowane przez art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, zgodnie z którym każdy ma prawo do poszanowania życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji (ust. 1).

Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

Trybunał zwrócił ponadto uwagę, że pracownik musi mieć świadomość możliwości monitorowania jego czynności, a to wymaga stworzenia odpowiedniej procedury oraz zaznajomienia pracownika z trybem postępowania.

Powyższe rozważania prowadzą do wniosku, że nawet przy przyjęciu, że monitoring systemu informatycznego jest niezbędny dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych, przepis art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych nie mógł być przesłanką legalnego przetwarzania danych osobowych skarżącego, gdyż przetwarzanie to naruszało prawo do prywatności w sytuacji, kiedy skarżący nie miał świadomości monitoringu użytkowania komputera.

Ponadto zasadnie skarżący powołał się w niniejszej sprawie na przepisy Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. L. 281, 23/11/1995 P. 0031-0050), która już w pkt 33 Preambuły stanowi, że dane mogące ze względu na ich charakter powodować naruszenie podstawowych wolności lub prywatności, nie powinny być przetwarzane, o ile osoba, której dotyczą, nie udzieli wyraźnej zgody, należy jednak przewidzieć odstępstwa od tego zakazu dla szczególnych potrzeb, zwłaszcza w przypadkach, gdy przetwarzanie danych odbywa się w określonych celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi zachowania tajemnicy zawodowej, lub też w trakcie legalnych działań niektórych stowarzyszeń lub fundacji, których celem jest umożliwienie realizacji podstawowych wolności.

Z kolei w art. 7f dyrektywy stanowi się, że przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, których dane są zbywalne, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1. Obowiązek interpretacji przepisów krajowych w zgodzie z postanowieniami przedmiotowej dyrektywy, wynika z przepisu art. 91 Konstytucji RP.

Komentarz redakcji:

Cytowany wyrok wydaje się dosyć kontrowersyjny. Warto podkreślić, że w powołanej wyżej sprawie administrator danych osobowych uzasadniając przetwarzanie danych powołał się na punkt XII załącznika do rozporządzenia w sprawie dokumentacji rzetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Zgodnie z tym przepisem system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. W przypadku zastosowania logicznych zabezpieczeń obejmują one:
a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Zatem to przepis prawa powszechnie obowiazujęcego pozwala administratorowi danych osobowych kontrolować przepływ informacji pomiędzy systemie informatycznym wewnętrznym a siecią publiczną. Takie również stanowisko prezentował Generalny Inspektor Ochrony Danych Osobowych. Przyjęcie za prawidłową interpretację sądu i wymaganie by administartor uzyskał akceptację wszystkich użytkowników sieci wewnętrznej na wdrożenie opisanego rozwiązania wskazywałoby na niekonsekwencje prawodawcy, który z jednej strony wymaga wdrożenia instrumentów służących zabezpieczaniu danych przetwarzanych w systemie informatycznym a z drugiej strony wprowadza w tym zakresie obostrzenia, w praktyce uniemożliwiające wdrożenie określonych narzędzi ochrony danych osobowych.

Prezentowany wyrok nie jest jeszcze prawomocny. Sprawą zajmie się jeszcze Naczelny Sąd Administarcyjny.

Bernadeta Skóbel