12.7.2010

KOMUNIKAT DLA POSŁÓW

Przedmiot: **Petycja 1198/2009, którą złożył J.F.K. (Węgry) w sprawie ingerencji w prywatność pracowników przez koncerny międzynarodowe**

1. Streszczenie petycji

Składający petycję protestuje przeciwko stosowanym przez przedsiębiorstwa wielonarodowe praktykom polegającym na kontroli toreb i teczek pracowników wychodzących po pracy, nadzorze kamer podczas pracy i wymogu przedstawiania CV podczas ubiegania się o pracę. Uważa to za naruszenie praw człowieka i zwraca się do Parlamentu o podjęcie działań mających zaradzić tej sytuacji.

2. Dopuszczalność

Petycja uznana została za dopuszczalną dnia 1 grudnia 2009 r. Zwrócono się do Komisji o udzielenie informacji zgodnie z art. 202 ust. 6 Regulaminu.

3. **Odpowiedź Komisji**, otrzymana dnia 12 lipca 2010 r.

Petycja

Składający petycję zgłasza zastrzeżenia do trzech rodzajów praktyk stosowanych na Węgrzech w międzynarodowych koncernach, takich jak Jabil, Nokia i Sanmina: 1) codzienne kontrole rzeczy osobistych pracowników przez ochronę (często obejmujące rewizję osobistą) w budynkach międzynarodowych koncernów, 2) obowiązek uprzedniego przedłożenia życiorysu przy staraniu się o pracę oraz 3) uwłaczający nadzór kamer wideo w miejscu pracy. Składający petycję podkreśla, że choć nie ma materialnych dowodów na poparcie swych zarzutów, to uważa, że pracownicy muszą podpisywać oddzielną umowę, w której zobowiązują się nie używać telefonów komórkowych ani kamer w miejscu pracy. Twierdzi on także, że istnieją przepisy stanowiące, że obrazy i dźwięk z nagrań taśmowych i wideo nie

mogą być odtwarzane w sposób obraźliwy, w celu prześladowania osób lub nagrywania wbrew ich woli. W wyjątkowych okolicznościach i z uzasadnionych powodów każdy może przedstawić nagranie jako dowód.

Składający petycję uważa, że takie kontrole są upokarzające, że obowiązek uprzedniego przedłożenia życiorysu stanowi przykład bezprawnego gromadzenia danych oraz że zakaz używania telefonów z funkcją aparatu fotograficznego w miejscu pracy stanowi przykład łamania praw człowieka. Składający skargę zwraca się z prośbą, aby stworzono instrumenty prawne służące ochronie pracowników przed wyżej wymienionymi praktykami.

Uwagi Komisji do petycji

Dyrektywa w sprawie ochrony danych *(dyrektywa 95/46/WE*[1]*)* ustanawia ramy prawne obejmujące przetwarzanie danych osobowych we wszystkich państwach członkowskich. Jeżeli państwa członkowskie nie przestrzegają obowiązku jej wdrożenia, obywatele mogą domagać się bezpośredniego zastosowania postanowień dyrektywy. W tym zakresie ETS orzekł w sprawie C-465/00[2], że niektóre przepisy, takie jak art. 6 ust. 1 lit. c) (zasady dotyczące jakości danych: dane powinny być prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone oraz art. 7 lit. c) i e) (kryteria legalności i przetwarzania danych) mają bezpośredni skutek.

Dyrektywa ma zastosowanie tylko do danych osobowych w rozumieniu dyrektywy 95/46/WE. Artykuł 2 definiuje, że „dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"). Osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość.

Dyrektywa 95/46/WE określa zasady, którym musi podlegać przetwarzanie, aby spełnić wymóg legalności. Przyznaje także pewne prawa osobom, których dane osobowe są przetwarzane, aby zagwarantować przestrzeganie podstawowego prawa do ochrony danych osobowych. Zasady zapisane w art. 6 stanowią podstawę ochrony danych osobowych, ponieważ dotyczą jakości danych podczas ich przetwarzania: gromadzenie i przetwarzanie danych osobowych musi się odbywać w określonym i jednoznacznym celu (zasada ograniczenia celu) oraz dane muszą być prawidłowe, stosowne i nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone (zasada proporcjonalności), a także, w razie konieczności, aktualizowane (art. 6). Dane osobowe muszą być także przetwarzane przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane.

Przetwarzanie danych (art. 7) jest legalne, jeżeli:

[1] Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z dnia 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.
[2] ETS C-465/00, C-138/01, *Rechnungshof and Österreichischer Rundfunk*, 20.5.2003, pkt 98 i następne.

a) osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę; lub
b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub
c) jest konieczne dla wykonania zobowiązania prawnego, lub
d) jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą; lub
e) jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej, lub
f) odbywa się dla potrzeb wynikających z uzasadnionych interesów osoby fizycznej lub prawnej, pod warunkiem, że są one podporządkowane interesom lub prawom i wolnościom osoby, której dane dotyczą.

Osoba, której dane dotyczą ma prawo do uzyskania informacji dotyczących dostępu do danych, sprostowania, usunięcia lub zablokowania swych danych, a także prawo do wyrównania szkód poniesionych wskutek niezgodnego z prawem przetwarzania jej danych. Prawa te podlegają ograniczeniu o ile konieczna jest ochrona, na przykład, nie tylko bezpieczeństwa narodowego i obronności, ale także w celu dochodzenia i prowadzenia spraw karnych.

Przetwarzanie jest nadzorowane i kontrolowane przez niezależny publiczny organ nadzorczy (art. 28), zwany zwykle „organem ochrony danych", który jest właściwym organem posiadającym uprawnienia do kontrolowania przestrzegania przepisów krajowych wdrażających dyrektywę w zakresie przetwarzania danych osobowych na szczeblu krajowym.

Aby zastosować dyrektywę w sprawie ochrony danych nr 95/46/WE należy stwierdzić dwa fakty.

Najważniejsza kwestia dotyczy przetwarzanych danych oraz czy podlegają one definicji „danych osobowych" zawartej w art. 2 lit. a). Jeśli chodzi o drugi i trzeci zarzut składającego petycję, dane zawarte w życiorysie i zarejestrowane za pomocą kamer wideo są danymi osobowymi w rozumieniu dyrektywy 95/46/WE. Jeśli chodzi o pierwszy zarzut, rewizja osobista nie podlega zakresowi dyrektywy w sprawie ochrony danych.

Drugą ważną kwestią, jest stwierdzenie, kto przetwarza dane osobowe. W zależności od tego, czy jest to administrator danych czy też tylko przetwarzający dane, muszą oni spełniać pewne wymagania. Międzynarodowe korporacje, takie jak Jabil, Nokia i Sanmina, są osobami prawnymi, które samodzielnie określają cele i metody przetwarzania danych osobowych, które gromadzą, takie jak dane zawarte w życiorysach lub dane zebrane za pomocą nadzoru wideo. W tym sensie są one administratorami danych w rozumieniu dyrektywy 95/46/WE, choć mogą delegować/zlecić przetwarzanie danych osobowych przetwarzającym, którzy w ich imieniu wykonują to zadanie.

Pierwszy zarzut: Kontrola pracowników przez ochronę (często obejmująca rewizję osobistą)

Na podstawie Traktatu o Unii Europejskiej oraz Traktatu o funkcjonowaniu Unii Europejskiej Komisja Europejska nie posiada uprawnień ogólnych do podejmowania działań w indywidualnych przypadkach domniemanego naruszania praw podstawowych. Może ona tak postąpić jedynie w sytuacji, gdy sprawa dotyczy kwestii wchodzącej w zakres prawa Unii Europejskiej.

Jeśli chodzi o skargę składającego petycję dotyczącą kontroli pracowników przez ochronę w montowniach, należy podkreślić, że nie istnieje prawodawstwo UE regulujące tę kwestię. Dlatego też Komisja nie ma możliwości podjęcia działań w związku z pierwszym zarzutem.

Drugi zarzut: niezgodne z prawem gromadzenie danych w związku z żądaniem życiorysu przyszłego potencjalnego pracownika

Aktualnie stanowiska w przedsiębiorstwach są obsadzane po przeprowadzeniu selekcji wśród zainteresowanych i kwalifikujących się kandydatów. Selekcja obejmuje zazwyczaj etap preselekcji, którą przeprowadza się na podstawie życiorysów przedkładanych wcześniej przez zainteresowanych kandydatów. Przetwarzanie danych zawartych w życiorysie podlega zakresowi dyrektywy w sprawie ochrony danych nr 95/46/WE oraz zasadom legalności, celowości i proporcjonalności (art. 6 dyrektywy).

W większości przypadków przetwarzanie danych przedłożonych w formie życiorysu może być uzasadnione jako legalne, ponieważ:

– odbywa się za zgodą osoby, której dane dotyczą (art. 7 lit. a) lub
– jest konieczne do zawarcia umowy o zatrudnienie między pracodawcą i pracownikiem (art. 7 lit. b) lub
– wynika z uzasadnionych interesów pracodawcy, który chce wiedzieć, jakie kwalifikacje zdobyli potencjalni przyszli pracownicy, aby najlepiej dopasować wolne stanowisko do najbardziej odpowiedniej osoby (art. 7 lit. f)).

Przetwarzanie danych osobowych zgromadzonych z życiorysów musi być proporcjonalne do uzasadnionych realizowanych celów i powinno zwłaszcza stosować jak najmniej natarczywe metody przetwarzania danych. Jeśli zastosowano wystarczające zabezpieczenia, takie przetwarzanie do określonych celów spełnia wymogi dyrektywy 95/46/WE. Zabezpieczenia te mogą przykładowo obejmować:

– poinformowanie pracowników o tożsamości administratora oraz podanie celu, jakiemu służy nadzór oraz wszelkich innych informacji, mających na celu zagwarantowanie rzetelnego przetwarzania w stosunku do osoby, której dane dotyczą (art. 11);

– poinformowanie osoby, której dane dotyczą, o prawie do sprostowania swoich danych oraz – zwłaszcza w przypadku odrzuconych kandydatów – prawie do ich usunięcia.

Sam fakt, że potencjalny pracodawca pragnie wcześniej otrzymać kopię życiorysu potencjalnego pracownika nie może zostać uznany za niezgodne z prawem gromadzenie danych, co zaskarżył składający petycję.

Trzeci zarzut: nadzór kamer wideo w miejscu pracy

Nadzór kamer wideo wchodzi w zakres stosowania dyrektywy w sprawie ochrony danych 95/46/WE. Zasady ochrony danych, zwłaszcza zasady legalności, celowości i proporcjonalności (art. 6 dyrektywy) mają zastosowanie do wszelkiego przetwarzania danych przez sprzęt do nadzoru wideo.

Grupa robocza powołana zgodnie z art. 29 (GR29)[1] wydała dwie opinie dotyczące nadzoru kamer wideo w miejscu pracy[2], które zawierają wytyczne na temat tego jak stosować postanowienia dyrektywy w sprawie ochrony danych w przypadku nadzoru kamer wideo. Zgodnie z tymi opiniami legalność nadzoru kamer wideo w miejscu pracy zależy od kilku czynników:

Po pierwsze, cel przetwarzania danych: systemy nadzoru wideo mają uzasadnienie, jeśli są rozmieszczane – pod warunkiem zachowania odpowiednich gwarancji – aby spełnić wymogi związane z bezpieczeństwem produkcji lub pracowników lub z powodów związanych z ogólnie pojętym bezpieczeństwem. Należy wziąć pod uwagę różne interesy analizując poszczególne przypadki oraz uwzględniając konkretny kontekst.

Instalacja systemów nadzoru wideo przez przedsiębiorstwa z powodów dotyczących wymogów bezpieczeństwa produkcji lub ogólnie pojętego bezpieczeństwa (aby zapobiec kradzieży sprzętu elektronicznego lub badań technologicznych) może być legalne w zakresie w jakim jest to konieczne do celów wynikających z uzasadnionych interesów tych przedsiębiorstw („administrator danych"), aby zagwarantować bezpieczeństwo budynków i zapobiec kradzieży tajemnic badań technologicznych i biznesowych, oraz jeśli te względy są podporządkowane interesom pracowników (art. 7 lit. f)).

Możliwe jest również, że stosowanie systemów nadzoru wideo jest uzasadnione w celu ochrony żywotnych interesów osoby, której dane dotyczą, takich jak bezpieczeństwo pracy, tj.: ochrona przed wypadkami podczas produkcji (art. 7 lit. d)).

Po drugie, celowość i proporcjonalność przetwarzania: umieszczenie sprzętu do nadzoru wideo musi być proporcjonalne do legalnie realizowanych celów, a w szczególności powinno stosować jak najmniej natarczywe metody przetwarzania danych. Interesy pracodawcy stosującego sprzęt do nadzoru wideo muszą brać pod uwagę interesy pracownika, który pragnie chronić swe dane osobowe. Może się to stać tylko jeśli zastosowane zostaną odpowiednie gwarancje. Tylko w takim przypadku nadzór kamer wideo spełnia wymogi dyrektywy 95/46/WE. Gwarancje te mogą przykładowo obejmować:

– brak kamer do nadzoru wideo w toaletach, prysznicach, schowkach i miejscach przeznaczonych do wypoczynku;

– poinformowanie pracowników o tożsamości administratora oraz podanie celu, jakiemu służy nadzór oraz wszelkich innych informacji, mających na celu zagwarantowanie rzetelnego przetwarzania w stosunku do osoby, której dane dotyczą;

[1] *Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych* (GR29) została powołana art. 29 dyrektywy w sprawie ochrony danych nr 95/46/WE. Grupa składa się z przedstawicieli krajowych organów ochrony danych. Działa ona w sposób niezależny i udziela rad Komisji.

[2] Opinia 8/2001 (GR48) w sprawie przetwarzania danych osobowych w miejscu zatrudnienia, dokument roboczy z 25 listopada 2002 r. (GR67) w sprawie przetwarzania danych osobowych przez nadzór kamer wideo i opinia 4/2004 (GR89) w sprawie przetwarzania danych osobowych przez nadzór kamer wideo.

– ograniczony czas przechowywania taśm;

– niezależny nadzór krajowych organów ochrony danych uprawnionych do monitorowania stosowania krajowej ustawy o ochronie danych wdrażającej dyrektywę 95/46/WE i zapewnienie odpowiednich zabezpieczeń i warunków, gwarantujących legalność systemu.

Administrator danych ma obowiązek (art. 11) poinformowania osób wchodzących do pomieszczenia znajdującego się pod nadzorem kamer wideo w widoczny, klarowny i jednoznaczny, że są monitorowane. W przypadku nadzoru kamer wideo w miejscu pracy należy także poinformować przedstawicieli pracowników.

Wnioski

Jeśli chodzi o pierwszy zarzut dotyczący kontroli pracowników, a zwłaszcza rewizji osobistych, to znajduje się on poza zasięgiem prawodawstwa Unii i Komisja nie może w związku z tym się nim zająć.

Jeśli chodzi o pozostałe zarzuty, składający petycję nie przedłożył żadnych dowodów świadczących o łamaniu przez filie międzynarodowych koncernów Jabil, Nokia i Sanmina dyrektywy 95/46/WE.

Składający petycję może kierować wszelkie zarzuty przeciw tym koncernom dotyczące łamania jego prawa do ochrony danych osobowych do krajowego węgierskiego organu ochrony danych.

Węgierski Inspektor Ochrony Danych
Nádor str. 22.
1051 Budapest
Tel: (+36 1) 475 7100, (+36 1) 475 7186
Fax: (+36 1) 269 3541
E-mail: **adatved@obh.hu**