



12.7.2010

COMUNICAZIONE AI MEMBRI

Oggetto: Petizione 1198/2009, presentata da J.F.K., cittadino ungherese, sull'intrusione delle società multinazionali nella sfera privata dei lavoratori

1. Sintesi della petizione

Il firmatario protesta contro la prassi delle società multinazionali di controllare le borse dei dipendenti dopo il lavoro, contro i sistemi di videosorveglianza durante il lavoro e contro l'obbligo di presentare un CV quando ci si candida per un posto di lavoro. Ritiene che si tratti di una violazione dei diritti umani e chiede al Parlamento di prendere misure per porre rimedio alla situazione.

2. Ricevibilità

Dichiarata ricevibile il 1° dicembre 2009. La Commissione è stata invitata a fornire informazioni (articolo 202, paragrafo 6, del regolamento).

3. Risposta della Commissione, ricevuta il 12 luglio 2010.

La petizione

Il firmatario contesta tre tipi di pratiche compiute in Ungheria da società multinazionali come Jabil, Nokia e Sanmina: 1) controlli quotidiani dei dipendenti da parte di agenti di sorveglianza (spesso ricorrendo a perquisizioni personali) nei locali delle multinazionali, 2) l'obbligo di presentare un CV in anticipo nel candidarsi a un posto di lavoro e 3) un'inadente videosorveglianza sul posto di lavoro. Fa presente di non poter addurre prove a sostegno delle sue affermazioni, ma spiega che i dipendenti devono firmare un accordo separato in cui si conferma di non far uso di telefoni cellulari o macchine fotografiche sul posto di lavoro. Egli sostiene inoltre che esistono disposizioni secondo cui la videoregistrazione di suoni e immagini non può avvenire in modo inadente, molestando altre

persone o registrandole contro la loro volontà. In casi di estrema necessità e per giustificati motivi, tutti potrebbero procedere a registrazioni a fini di prova.

Il firmatario ritiene che tali controlli siano umilianti, che l'obbligo di presentare il proprio CV in anticipo rappresenti un'illecita raccolta di dati e che il divieto di utilizzare un cellulare con fotocamera sul posto di lavoro rappresenti una violazione dei diritti umani. Egli chiede che siano posti in atto strumenti giuridici per proteggere i lavoratori dalle pratiche summenzionate.

Osservazioni della Commissione in merito alla petizione

La direttiva sulla protezione dei dati (*direttiva 95/46/CE*¹) definisce il quadro giuridico per il trattamento dei dati personali in tutti gli Stati membri. Qualora gli Stati membri non abbiano adempiuto a questo obbligo di attuazione, i cittadini possono chiedere la diretta applicazione di alcune disposizioni della direttiva. In proposito, la Corte di giustizia europea ha stabilito nella causa C-465/00² che talune disposizioni, come l'articolo 6, paragrafo 1, lettera c) (principi relativi alla qualità dei dati: i dati devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati) e l'articolo 7, lettere c) e e) (principi relativi alla legittimazione del trattamento dei dati) hanno effetto diretto.

La direttiva si applica solo ai dati personali ai sensi della direttiva 95/46/CE. L'articolo 2 definisce come "dati personali" qualsiasi informazione concernente una persona fisica identificata o identificabile (persona interessata); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un numero di identificazione o a uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

La direttiva 95/46/CE stabilisce le condizioni alle quali i trattamenti di dati personali sono leciti. Stabilisce inoltre taluni diritti alle persone i cui dati personali vengono trattati, in modo da garantire il rispetto del loro diritto fondamentale alla protezione dei dati personali. I principi contenuti all'articolo 6 sono le basi per la protezione dei dati personali, poiché riguardano la qualità dei dati quando vengono trattati: la raccolta e il trattamento di dati personali deve avvenire per finalità determinate ed esplicite (principio della limitazione delle finalità), e i dati personali devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati (principio di proporzionalità) e, se necessario, aggiornati (articolo 6). Inoltre, i dati personali possono essere conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati.

Il trattamento dei dati viene legittimato (articolo 7) soltanto quando:

- a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile, oppure
- b) è necessario all'esecuzione del contratto concluso con la persona interessata, oppure

¹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24.10.1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pag. 31.

² Corte di giustizia UE C-465/00, C-138/01 e C-139/01, *Rechnungshof and Österreichischer Rundfunk*, 20.5.2003, punto 98 e seguenti.

- c) è necessario per adempiere a un obbligo legale, oppure
- d) è necessario per la salvaguardia dell'interesse della persona interessata, oppure
- e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, oppure
- f) è necessario per il perseguimento dell'interesse legittimo di una persona fisica o giuridica, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

La persona interessata ha diritto a ricevere informazioni, il diritto di accesso, il diritto di rettifica, cancellazione o congelamento dei suoi dati personali nonché il diritto a un effettivo risarcimento per il trattamento illecito dei suoi dati. Questi diritti sono soggetti a restrizione nel caso in cui tale restrizione costituisca una misura necessaria alla salvaguardia non solo della sicurezza e della difesa dello Stato ma anche a fini di accertamento e perseguimento di infrazioni penali.

Il trattamento dei dati è sottoposto alla sorveglianza e al controllo di autorità pubbliche di controllo indipendenti (articolo 28), comunemente chiamate "autorità per la protezione dei dati", che sono le autorità competenti incaricate di verificare la conformità di qualsiasi trattamento di dati personali a livello nazionale con la normativa nazionale che dà attuazione alla direttiva.

Due elementi devono sussistere affinché la direttiva sulla protezione dei dati 95/46/CE sia applicabile.

L'elemento più importante è quello concernente i dati trattati e se rientrano nella definizione di "dati personali" di cui all'articolo 2, lettera a). Per quanto attiene alla seconda e alla terza contestazione fatta dal firmatario, i dati contenuti in un CV e registrati dalla videosorveglianza sono dati personali secondo l'accezione della direttiva 95/46/CE. Per quanto riguarda la prima contestazione, la perquisizione personale non rientra nel campo di applicazione della direttiva sulla protezione dei dati.

Il secondo importante elemento è quello di stabilire chi tratta i dati personali. A seconda che sia un responsabile del trattamento o semplicemente un incaricato del trattamento dei dati, essi devono rispettare una serie di obblighi. Le multinazionali come Jabil, Nokia e Sanmina sono persone giuridiche che determinano la finalità e le modalità del trattamento dei dati personali che raccolgono, come i dati contenuti nei CV o i dati raccolti tramite videosorveglianza. Così facendo essi vengono considerati come responsabili del trattamento ai sensi della direttiva 95/46/CE, sebbene possano delegare/subappaltare il trattamento di dati personali a incaricati del trattamento che svolgono questo compito per conto loro.

1^a contestazione: Controlli dei dipendenti da parte degli agenti di sorveglianza (spesso ricorrendo a perquisizioni personali)

Ai sensi del trattato sull'Unione europea e del trattato sul funzionamento dell'Unione europea, la Commissione europea non ha competenze generali per intervenire in singoli casi di presunte violazioni dei diritti fondamentali. Può farlo solo se si tratta di una questione inerente al diritto dell'Unione europea.

Per quanto concerne l'accusa del firmatario inerente ai controlli dei dipendenti da parte di agenti di sorveglianza in impianti di assemblaggio, giova rilevare che non esiste una normativa specifica dell'Unione europea che disciplina la materia. Per questo motivo, la Commissione non può occuparsi di questa prima contestazione.

2^a contestazione: Raccolta illecita di dati nel richiedere il CV di un potenziale futuro dipendente

Attualmente le posizioni aziendali sono stilate dopo un processo di selezione dei candidati interessati e idonei, il che generalmente comprende una fase di preselezione, effettuata sulla base dei CV precedentemente presentati dai candidati interessati. Il trattamento dei dati contenuti nei CV rientra nell'ambito di applicazione della direttiva sulla protezione dei dati 95/46/CE ed è soggetta ai principi di legittimità, necessità e proporzionalità (articolo 6 della direttiva).

Nella maggior parte dei casi il trattamento dei dati forniti sotto forma di CV può essere ritenuto legittimo in quanto

- è effettuato con il consenso della persona interessata (articolo 7, lettera a) oppure
- è necessario per l'esecuzione di un contratto concluso fra un datore di lavoro e un dipendente (articolo 7, lettera b) oppure
- fa parte del legittimo interesse perseguito dal datore di lavoro di conoscere le qualifiche di potenziali futuri dipendenti in modo da coprire al meglio la posizione vacante con la persona più idonea (articolo 7, lettera f).

Il trattamento dei dati personali raccolti dai CV deve essere proporzionato ai legittimi obiettivi perseguiti e dovrebbe in particolare offrire i mezzi meno intrusivi di trattamento dei dati. A condizione che sussistano sufficienti garanzie, tale trattamento per i motivi indicati sarebbe conforme alla direttiva 95/46/CE. Tali garanzie potrebbero essere, ad esempio, quelle di

- informare i lavoratori circa l'identità del responsabile del trattamento e lo scopo della sorveglianza e fornire altre informazioni necessarie a garantire un corretto trattamento dei dati dell'interessato (articolo 11);
- informare l'interessato del diritto di rettifica dei dati che lo riguardano e – in particolare per i candidati poi esclusi – del diritto di cancellazione.

Per il semplice fatto che il potenziale datore di lavoro chieda anticipatamente una copia del CV di un potenziale dipendente, la raccolta dei dati non può essere considerata illecita, così come asserito dal firmatario.

3^a contestazione: videosorveglianza sul posto di lavoro

La videosorveglianza rientra nel campo di applicazione della direttiva sulla protezione dei dati 95/46/CE. I principi di protezione dei dati, segnatamente i principi di legittimità, necessità e proporzionalità (articolo 6 della direttiva) si applicano a qualsiasi trattamento di dati personali mediante apparecchiature di videosorveglianza.

Il gruppo di lavoro ex articolo 29¹ ha emesso due pareri in materia di videosorveglianza² nei luoghi di lavoro, che forniscono indicazioni su come applicare le disposizioni della direttiva sulla protezione dei dati alla videosorveglianza. In base a tali pareri, la liceità della videosorveglianza nei luoghi di lavoro dipende da vari fattori:

In primo luogo, la finalità del trattamento: i sistemi di videosorveglianza possono essere giustificati se sono impiegati, fatte salve le garanzie del caso, per soddisfare necessità di produzione o di sicurezza sul lavoro, o per motivi di sicurezza. I diversi interessi in gioco andrebbero presi in considerazione caso per caso e alla luce del contesto specifico.

L'installazione dei sistemi di videosorveglianza dalle aziende per finalità adottate per esigenze di sicurezza della produzione o per motivi di sicurezza (per scongiurare il furto di prodotti elettronici o di ricerca tecnologica) potrebbe essere legittima, nella misura in cui sia necessaria per il perseguimento dell'interesse legittimo di queste aziende ("responsabile del trattamento dei dati") per garantire la sicurezza dei locali e per impedire il furto di ricerche tecnologiche e segreti commerciali, condizione che su questo interesse non prevalgano gli interessi dei dipendenti (articolo 7, lettera f).

È anche possibile che l'utilizzo di sistemi di videosorveglianza sia giustificato per proteggere un interesse vitale della persona interessata, segnatamente per ragioni di sicurezza sul lavoro, come nel caso di incidenti in fase di produzione (articolo 7, lettera d).

In secondo luogo, la necessità e la proporzionalità del trattamento: l'impiego di apparecchiature di videosorveglianza deve essere proporzionato agli scopi legittimi perseguiti e dovrebbe in particolare utilizzare i mezzi meno intrusivi di trattamento dei dati. Gli interessi del datore di lavoro a installare impianti di videosorveglianza devono essere controbilanciati dagli interessi del lavoratore di ottenere la protezione dei propri dati personali. Questo può essere fatto solo se sussistono adeguate garanzie. Solo così la videosorveglianza è conforme alla direttiva 95/46/CE. Tali garanzie potrebbero comprendere, ad esempio, le seguenti misure:

- assenza di impianti di videosorveglianza in bagni, docce, armadietti e luoghi di ricreazione;
- informazioni per i dipendenti circa l'identità del responsabile del trattamento dei dati e l'obiettivo della sorveglianza, e altre informazioni necessarie a garantire un trattamento corretto dei dati nel rispetto della persona interessata;
- una limitazione della durata di conservazione dei video;
- il controllo indipendente effettuato da autorità nazionali di protezione dei dati preposte alla verifica dell'osservanza delle disposizioni nazionali sulla protezione dei dati che danno

¹ Il gruppo per la tutela delle persone riguardo al trattamento dei dati personali è stato istituito dall'articolo 29 della direttiva sulla protezione dei dati 95/46/CE. Il gruppo è composto da rappresentanti delle autorità nazionali preposte alla protezione dei dati. Opera in maniera indipendente e fornisce consulenza alla Commissione.

² *Parere 8/2001 (WP48) sul trattamento dei dati personali nel contesto occupazionale, documento di lavoro del 25 novembre 2002 (WP67) sul trattamento dei dati personali tramite videosorveglianza e Parere 4/2004 (WP89) sul trattamento dei dati personali tramite videosorveglianza.*

attuazione alla direttiva 95/46/CE e a fornire le garanzie e i requisiti idonei affinché il sistema sia legale.

Infine il responsabile del trattamento dei dati ha l'obbligo (articolo 11) di informare in maniera visibile, chiara ed esplicita, le persone che entrano in un luogo videosorvegliato del fatto che sono sottoposte a controllo video. Nel caso di impianti di videosorveglianza installati sui luoghi di lavoro, bisognerebbe informare anche i rappresentanti dei lavoratori.

Conclusioni

Per quanto concerne la prima contestazione concernente i controlli effettuati sui dipendenti e in particolare le perquisizioni personali, la questione non rientra nel campo di applicazione del diritto dell'Unione e pertanto non è di competenza della Commissione.

Per quanto concerne le altre contestazioni, il firmatario non ha fornito alcuna prova che dimostri che le filiali delle multinazionali Jabil, Nokia e Sanmina abbiano violato la direttiva 95/46/CE.

Si invita il firmatario a rivolgere qualsiasi accusa riguardante queste multinazionali e attinente alla violazione dei suoi diritti alla protezione dei dati all'autorità nazionale per la protezione dei dati in Ungheria:

Commissario ungherese per la protezione dei dati
Nádor str. 22.
1051 Budapest
Tel.: (+36 1) 475 7100, (+36 1) 475 7186
Fax: (+36 1) 269 3541
E-mail: adatved@obh.hu