12.7.2010

COMMUNICATION AUX MEMBRES

Objet: Pétition 1198/2009, présentée par J.F.K., de nationalité hongroise, sur l'invasion de la sphère privée des travailleurs par les sociétés multinationales

1. Résumé de la pétition

Le pétitionnaire proteste contre les pratiques de certaines sociétés multinationales, notamment le contrôle des sacs de leurs employés après le travail, la surveillance par caméra durant le travail et l'obligation de fournir un CV en cas de candidature à une fonction. Il considère qu'il s'agit de violations des droits de l'homme et prie le Parlement européen de bien vouloir prendre des mesures afin de remédier à cette situation.

2. Recevabilité

Déclarée recevable le 1er décembre 2009. La Commission a été invitée à fournir des informations (article 202, paragraphe 6, du règlement).

3. **Réponse de la Commission**, reçue le 12 juillet 2010.

Pétition

Le pétitionnaire proteste contre trois types de pratiques auxquelles ont recours des sociétés multinationales telles que Jabil, Nokia et Sanmina en Hongrie: 1) les fouilles quotidiennes des employés (comprenant souvent des fouilles au corps) par des vigiles dans les locaux des multinationales, 2) l'obligation de fournir un CV à l'avance en cas de candidature à un poste et 3) une vidéosurveillance offensante sur le lieu de travail. Il indique qu'il ne dispose d'aucune preuve pour appuyer ses affirmations, mais explique que les employés doivent signer un document séparé par lequel ils s'engagent à ne pas utiliser de téléphone portable ou d'appareil photo sur leur lieu de travail. Il affirme également qu'il existe des réglementations disposant que les images et les contenus audio pour des enregistrements audio ou vidéo ne doivent pas

être reproduits de façon offensante, en harcelant des personnes ou en les enregistrant contre leur gré. En cas d'extrême nécessité, et pour des raisons justifiées, tout un chacun peut produire un enregistrement dans le but de disposer de preuves.

Le pétitionnaire estime que ces fouilles sont humiliantes, que l'obligation de fournir un CV à l'avance constitue une collecte illégale de données et que l'interdiction d'utiliser un téléphone doté d'un appareil photo sur son lieu de travail représente une violation des droits de l'homme. Il demande que des instruments juridiques soient mis en place pour protéger les employés des pratiques susmentionnées.

Commentaires de la Commission sur la pétition

La directive relative à la protection des données (directive 95/46/CE[1]) fournit le cadre juridique pour le traitement des données à caractère personnel dans tous les États membres. Au cas où les États membres n'auraient pas honoré leur obligation de mise en œuvre, les citoyens peuvent demander l'application directe de certaines dispositions de cette directive. La Cour de justice de l'Union européenne a arrêté à cet égard dans l'affaire C-465/00[2] que certaines dispositions, telles que celles de l'article 6, paragraphe 1, point c) (principes relatifs à la qualité des données: les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement) et de l'article 7, points c) et e) (principes relatifs à la légitimation des traitements de données) sont directement d'application.

Ladite directive ne s'applique qu'aux données à caractère personnel au sens de la directive 95/46/CE. L'article 2 définit les "données à caractère personnel" comme toute information concernant une personne physique identifiée ou identifiable (personne concernée). Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

La directive 95/46/CE établit les principes que les activités de traitement doivent respecter pour être légales. Elle instaure également certains droits pour les personnes dont les données à caractère personnel sont traitées, de façon à garantir le respect de leur droit fondamental à la protection de leurs données personnelles. Les principes exposés à l'article 6 constituent le socle de la protection des données personnelles, puisqu'ils concernent la qualité des données lors de leur traitement: la collecte et le traitement des données à caractère personnel doivent être effectués pour des finalités déterminées et explicites (principe de limitation de la finalité), et les données personnelles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement (principe de proportionnalité) et, si nécessaire, mises à jour (article 6). Les données à caractère personnel doivent également être traitées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[2] Cour de justice de l'Union européenne, C-465/00, C-138/01 et C-139/01, *Rechnungshof contre Österreichischer Rundfunk,* 20.5.2003, point 98 et suivants.

lesquelles elles sont traitées ultérieurement.

Le traitement des données (article 7) n'est considéré comme légitime que si:

a) la personne concernée a indubitablement donné son consentement, ou
b) le traitement est nécessaire à la conclusion d'un contrat liant la personne concernée, ou
c) celui-ci constitue une exigence juridique, ou
d) le traitement vise la sauvegarde des intérêts vitaux de la personne concernée, ou
e) le traitement est nécessaire pour l'exécution d'une tâche dans l'intérêt public ou dans l'exercice d'une autorité officielle, ou
f) celui-ci est dans l'intérêt légitime d'une personne physique ou morale, à condition qu'il ne soit pas passé outre les intérêts ou les droits et les libertés de la personne concernée.

La personne concernée a le droit de recevoir des informations concernant l'accès à ses données personnelles ainsi que leur rectification, leur suppression ou leur blocage, de même qu'elle a le droit à un recours effectif en cas de traitement illicite de ses données. Ces droits peuvent être restreints si cela est nécessaire pour préserver la sécurité et la défense nationales, par exemple, mais aussi aux fins d'enquêtes criminelles et de poursuites pénales.

Les activités de traitement sont supervisées et contrôlées par des autorités de contrôle publiques et indépendantes (article 28) appelées généralement "autorités de protection des données", qui sont les autorités compétentes pour vérifier la conformité de tout traitement de données à caractère personnel au niveau national avec la législation nationale mettant en œuvre la directive.

Deux points doivent être confirmés pour que la directive 95/46/CE sur la protection des données soit applicable.

Le point le plus important est celui qui concerne les données traitées, et le fait de savoir si elles relèvent de la définition des "données à caractère personnel" établie par l'article 2, point a). En ce qui concerne les deuxième et troisième allégations du pétitionnaire, les données contenues dans un CV et celles enregistrées au moyen de la vidéosurveillance constituent des données à caractère personnel au sens de la directive 95/46/CE. En ce qui concerne la première allégation, la fouille au corps ne relève pas du champ d'application de la directive sur la protection des données.

Le deuxième point pertinent consiste à déterminer qui traite les données à caractère personnel. Selon qu'il s'agisse de responsables du traitement des données ou simplement de sous-traitants, ils doivent se plier à un certain nombre d'obligations. Des sociétés multinationales comme Jabil, Nokia et Sanmina sont des personnes morales qui déterminent elles-mêmes la finalité et les moyens du traitement des données à caractère personnel qu'elles collectent, telles que les données contenues dans des CVs ou celles recueillies au moyen de la vidéosurveillance. Ce faisant, elles sont considérées comme des responsables du traitement des données au sens de la directive 95/46/CE, bien qu'elles pourraient déléguer/sous-traiter le traitement des données à caractère personnel à des sous-traitants qui exécuteraient cette tâche en leur nom.

Première allégation: fouilles des employés par des vigiles (comprenant souvent des fouilles

au corps)

Selon le traité sur l'Union européenne et le traité sur le fonctionnement de l'Union européenne, la Commission n'a pas de compétences générales pour intervenir dans les cas individuels d'allégation de violations des droits fondamentaux. Elle ne peut le faire que lorsqu'une question de droit communautaire se pose.

Au sujet de la plainte du pétitionnaire relative aux fouilles effectuées par des vigiles et dont les employés font l'objet dans les ateliers de montage, il convient de souligner qu'il n'existe pas de législation européenne spécifique régissant cette question. Il n'est par conséquent pas possible pour la Commission de donner suite à cette première allégation.

Deuxième allégation: recueil illicite de données en demandant un CV à un futur employé potentiel

Aujourd'hui, les postes dans les sociétés sont pourvus une fois que les candidats intéressés et éligibles ont passé une procédure de sélection. Cela comprend généralement une étape de présélection qui est effectuée sur la base des CV envoyés à l'avance par les candidats intéressés. Le traitement des données contenues dans les CV relève du champ d'application de la directive 95/46/CE relative à la protection des données et est soumis au principe de légitimité, de nécessité et de proportionnalité (article 6 de la directive).

Dans la plupart des cas, le traitement des données transmises sous forme de CV peut être justifié et considéré comme légitime car:

- il est effectué avec le consentement de la personne concernée (article 7, point a)) ou
- il est nécessaire à l'exécution d'un contrat d'emploi entre un employeur et un employé (article 7, point b)) ou
- il fait partie de l'intérêt légitime poursuivi par l'employeur pour savoir quelles qualifications de futurs employés potentiels ont obtenues de manière à pourvoir le poste de la meilleure manière possible avec la personne la plus adéquate (article 7, point f)).

Le traitement des données à caractère personnel recueillies depuis les CV doit être proportionné aux objectifs légitimes visés et doit en particulier employer les moyens les moins intrusifs de traitement de données. À condition que des garanties suffisantes soient en place, un tel traitement pour les motifs évoqués serait conforme à la directive 95/46/CE. Ces garanties pourraient par exemple être les suivantes:

- informer les employés de l'identité du responsable du traitement des données et de la finalité de la surveillance, ainsi que d'autres informations nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données (article 11);

- informer la personne concernée de son droit à rectifier les données la concernant et – en particulier pour les candidats n'ayant pas été retenus – du droit de supprimer ces données.

Le simple fait qu'un employeur potentiel demande de recevoir à l'avance une copie du CV d'un employé potentiel ne peut être considéré comme un recueil illicite de données, contrairement à ce qu'avance le pétitionnaire.

Troisième allégation: vidéosurveillance sur le lieu de travail

La vidéosurveillance relève du champ d'application de la directive 95/46/CE sur la protection des données. Les principes de protection des données, en particulier les principes de légitimité, de nécessité et de proportionnalité (article 6 de la directive), s'appliquent à tout traitement de données à caractère personnel au moyen d'équipements de vidéosurveillance.

Le groupe de travail "article 29"[1] a élaboré deux avis relatifs à la vidéosurveillance sur le lieu de travail[2] qui fournissent des lignes directrices sur la matière d'appliquer à la vidéosurveillance les dispositions de la directive sur la protection des données. Selon ces avis, la légalité de la vidéosurveillance sur le lieu de travail dépend de plusieurs facteurs:

Premièrement, la finalité du traitement: les systèmes de vidéosurveillance peuvent se justifier s'ils sont mis en place, sous réserve de garanties appropriées, afin de répondre à des exigences de sécurité de production ou de sécurité au travail, ou pour des raisons de sûreté. Les différents intérêts en jeu doivent être pris en compte au cas par cas ainsi que dans leur contexte spécifique.

L'installation, par des sociétés, de systèmes de vidéosurveillance pour des raisons de sécurité de production ou pour des raisons de sûreté (pour prévenir le vol de produits électroniques ou de recherches technologiques) peut être légitime dans la mesure où elle est nécessaire aux fins de l'intérêt légitime desdites sociétés ("responsables du traitement des données") pour assurer la sécurité des locaux et pour prévenir le vol de recherches technologiques et de secrets d'affaires, et que les intérêts des employés ne prévalent pas sur cet intérêt (article 7, point f)).

Il est également possible que l'utilisation de systèmes de vidéosurveillance soit justifiée pour protéger l'intérêt vital de la personne concernée, par exemple pour des raisons de sécurité au travail, notamment vis-à-vis d'accidents qui surviendraient pendant la production (article 7, point d)).

Deuxièmement, la nécessité et la proportionnalité du traitement: la mise en place d'équipements de vidéosurveillance se doit d'être proportionnée aux objectifs légitimes visés et doit notamment utiliser les moyens les moins intrusifs de traitement de données. L'intérêt qu'a l'employeur à installer des équipements de vidéosurveillance doit être mis en balance avec l'intérêt qu'a l'employé à obtenir la protection de ses données à caractère personnel. Ceci ne peut être fait que si des garanties appropriées sont en place. Ce n'est qu'alors que la vidéosurveillance serait conforme à la directive 95/46/CE. Ces garanties pourraient par

[1] Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel a été établi par l'article 29 de la directive 95/46/CE relative à la protection des données. Il est composé de représentants des autorités nationales de protection des données. Il agit en toute indépendance et joue un rôle consultatif auprès de la Commission.

[2] *Avis 8/2001 (WP 48) sur le traitement des données à caractère personnel dans le contexte professionnel, document de travail du 25 novembre 2002 (WP 67) sur le traitement des données à caractère personnel au moyen de la vidéosurveillance* et *avis 4/2004 (WP 89) sur le traitement des données à caractère personnel au moyen de la vidéosurveillance.*

exemple être les suivantes:

- ne pas installer d'équipements de vidéosurveillance dans les sanitaires, les salles de douche, les vestiaires et les espaces de repos;

- informer les employés de l'identité du responsable du traitement des données et de la finalité de la surveillance, ainsi que d'autres informations nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données;

- limiter la durée de rétention des vidéos;

- mettre en place une supervision indépendante par les autorités nationales de protection des données qui sont compétentes pour vérifier la conformité avec les actes législatifs nationaux de protection des données mettant en œuvre la directive 95/46/CE et qui fournissent les garanties et les exigences adaptées pour que l'installation du système soit légale.

Enfin, le responsable du traitement des données a l'obligation (au titre de l'article 11) d'informer les personnes pénétrant dans une zone placée sous vidéosurveillance de l'existence d'une telle surveillance de manière visible, claire et explicite. Dans le cas des équipements de vidéosurveillance installés sur le lieu de travail, les représentants des travailleurs doivent également être informés.

Conclusions

En ce qui concerne la première allégation relative aux fouilles dont les employés font l'objet, en particulier les fouilles au corps, cette question ne relève pas du droit de l'Union et la Commission ne peut par conséquent pas y donner suite.

En ce qui concerne les autres allégations, le pétitionnaire n'a fourni aucune preuve établissant que les filiales des multinationales Jabil, Nokia et Sanmina ont violé la directive 95/46/CE.

Le pétitionnaire est invité à adresser toute accusation qu'il souhaiterait porter à l'encontre de ces multinationales, et qui sont liées à une violation de ses droits à la protection des données, à l'autorité nationale de protection des données de Hongrie:

Commissaire hongrois pour la protection des données
Nádor u. 22.
1051 Budapest
Tél: (+36 1) 475 7100, (+36 1) 475 7186
Fax: (+36 1) 269 3541
Courriel: adatved@obh.hu