

**31<sup>st</sup>**

Madrid, 4th, 5th and 6th, november 2009  
**international conference  
of data protection  
and privacy commissioners**

**Madrid, les 4, 5 et 6 novembre 2009**

**31<sup>e</sup> conférence internationale des commissaires à la protection des données et de  
la vie privée**

**Avez-vous une vie privée au travail?**

**La vie privée au travail dans les institutions et organes  
communautaires**

**Giovanni Buttarelli**

Dans le cadre de ses activités de supervision, le contrôleur européen de la protection des données (CEPD) a publié des orientations sur plusieurs questions, qui illustrent le juste milieu délicat devant être trouvé pour veiller au respect de la vie privée au travail. Je souhaite aborder brièvement quelques-uns des exemples les plus significatifs, concernant notamment le contrôle de l'usage de l'internet et de la téléphonie, la productivité et la qualité du travail des personnels, l'horaire flexible et la vidéosurveillance.

La principale législation en matière de protection des données applicable aux institutions et organes communautaires est le règlement (CE) n° 45/2001, qui régit le traitement des données à caractère personnel et la libre circulation de ces données. Des dispositions spécifiques relatives à la protection des données dans le secteur des communications électroniques sont également exposées dans la directive «vie privée et communications électroniques» (2002/58/CE).

Le règlement (CE) n° 45/2001 précise que l'autorité de contrôle indépendante requise en vertu de l'article 286 du Traité instituant la Communauté européenne est le CEPD. Les **missions de supervision** du CEPD sont exécutées par le biais d'activités diverses, dont le **contrôle préalable** des opérations de traitement présentant des risques spécifiques, la prise en charge des **réclamations** des membres du personnel et autres personnes concernées, et les **consultations** reçues des délégués à la protection des données (DPD) des institutions et organes communautaires. Elles couvrent l'ensemble de ces institutions et organes (par opposition aux institutions et organes de l'«Union»), à l'exception de la Cour de justice dans sa capacité judiciaire.

### **Contrôle des communications électroniques**

La question du contrôle des communications électroniques est probablement la plus illustrative et la plus compliquée dans ce domaine, qu'il s'agisse des communications par courrier électronique, de l'usage de l'internet ou de celui de la téléphonie fixe ou mobile.

Les considérants du règlement (CE) n° 45/2001 prévoient qu'il peut être nécessaire de contrôler les réseaux d'ordinateurs fonctionnant sous la responsabilité des institutions et organes communautaires en vue de prévenir un usage non autorisé, et que le contrôleur européen de la protection des données détermine si et sous quelles conditions cela est possible.

On **reconnait** donc qu'un certain degré de contrôle est permis, mais que ce contrôle doit respecter les règles établies par le règlement, notamment celles de **nécessité et de proportionnalité**. Le CEPD a indiqué sa préférence pour une démarche préventive, plutôt que répressive, en matière d'usage abusif des réseaux de communication, ainsi que pour un contrôle sélectif, dans des cas bien définis uniquement, par opposition à un contrôle généralisé. S'il y a violation de la politique d'usage, le CEPD recommande une approche graduelle de toute enquête éventuelle, l'identité des individus en violation des règles n'étant révélée à la direction qu'en cas d'absolue nécessité.

En ce qui concerne le contrôle de l'**usage de l'internet**, le CEPD a considéré, dans un avis sur le contrôle préalable, qu'en l'absence de soupçons adéquats, le contrôle de toutes les URL consultées par tous les utilisateurs était inutile et exagéré. Le CEPD a conseillé aux institutions de se fier à des indicateurs (par exemple au volume de données téléchargées) au lieu de contrôler toutes les URL. Seules certaines circonstances particulières peuvent faire juger nécessaire que l'institution contrôle toutes les URL consultées par des individus spécifiques. Tel est le cas, par exemple, lorsqu'il y a motif de soupçonner un certain utilisateur d'actes criminels (ex. téléchargement de contenu pédophile).

Le principe de proportionnalité a également guidé l'approche du contrôle des **communications téléphoniques** professionnelles adoptée par le CEPD, qui estime que le contrôle ciblé des données relatives au trafic est justifié uniquement lorsque le coût des communications est largement supérieur au coût moyen mensuel.

En ce qui concerne l'**enregistrement des communications** au travail, l'article 36 du règlement (CE) n° 45/2001 prévoit que les institutions et organes communautaires doivent garantir la confidentialité des communications dans le respect des principes généraux du droit communautaire. Ces principes généraux font référence à la notion des droits fondamentaux, tels que définis par la Convention européenne des droits de l'homme. Par conséquent, le CEPD préconise qu'une violation de la confidentialité des communications ne peut avoir lieu que dans des circonstances exceptionnelles, **en l'absence de méthodes moins intrusives ou invasives** et à condition de remplir plusieurs conditions très rigoureuses. Bien entendu, les enquêtes criminelles restent du ressort des États membres.

Par ailleurs, le CEPD a autorisé l'enregistrement de certaines communications professionnelles par la Banque centrale européenne dans le contexte de transactions commerciales types, à des fins de justification de la transaction et avec le consentement des intervenants de la communication.

Le CEPD a également estimé que l'enregistrement des appels au service d'assistance d'une institution pouvait être utilisé en vue de résoudre un problème informatique avec le consentement des individus impliqués. Il a toutefois jugé que tout autre usage des enregistrements à des fins de contrôle de la qualité et de formation professionnelle dépassait les limites de nécessité acceptables. Par conséquent, le CEPD a invité l'institution concernée à rendre les données anonymes ou à obtenir le consentement des parties impliquées.

L'enregistrement des communications à un service de secours d'urgence a également été considéré légitime par le CEPD, sur la base des obligations de l'institution en vertu de règles internes ou de dispositions sécuritaires nationales (dans le cas d'une agence ou institution sur un site nucléaire, par exemple).

### **Suivi de la disponibilité, de la productivité et de la qualité du travail des personnels**

Les institutions et les organes communautaires tendent de plus en plus à utiliser des bases de données informatiques pour contrôler la disponibilité et l'usage de leurs

ressources humaines et, plus particulièrement, pour surveiller la productivité et la qualité du travail, tant au niveau individuel qu'au niveau organisationnel. À ces fins précises, certaines agences sont allées jusqu'à créer des systèmes informatiques chargés de les alimenter en quantités importantes de données. Par exemple, une agence a mis au point un système selon lequel certains responsables (cadres supérieurs et certains chefs d'unités) examinaient au hasard certains documents (décisions, lettres, etc.) produits par les employés. Les résultats de ces examens (contenant, par exemple, les types d'erreurs commises par un individu) étaient ensuite introduits dans une base de données électronique. Une autre agence demandait à son personnel de tenir des feuilles de présence détaillées, divisées en plus de 50 catégories et sous-catégories spécifiques, à l'instar d'un cabinet d'avocats international à des fins de facturation. Ici aussi, ces informations étaient introduites dans une base de données. Nous avons également remarqué quelques efforts de mise au point de bases de données de compétences multicouche au sein d'une organisation, afin de permettre à la direction d'obtenir un tableau exact des compétences de son personnel et d'optimiser ainsi l'utilisation de ses ressources humaines. Toutes ces initiatives ont pour objectif commun de mesurer l'utilisation des ressources humaines des organisations et de contribuer à l'amélioration de la productivité et de la qualité générale du travail. Cependant, un autre objectif, parfois insuffisamment explicite, se profile souvent: celui de contrôler la productivité ou la qualité du travail d'un individu, à des fins d'évaluation de la performance. Ce contrôle sert ensuite de fondement à des décisions pouvant affecter les employés concernés, au niveau, par exemple, de la distribution des tâches, des renouvellements de contrats temporaires ou des promotions.

Dans la pratique, le contrôle à ces fins a sa place dans une culture administrative moderne. Il est toutefois important qu'il ait lieu dans le respect de la vie privée et des lois sur la protection des données. Les organisations doivent être parfaitement claires quant à ce qu'elles souhaitent accomplir et pourquoi. Les institutions doivent être conscientes du rapport évident qui existe entre, d'une part, le nombre de cibles, critères et contrôles en place pour surveiller l'utilisation du temps, la productivité et la qualité du travail et, d'autre part, la quantité de stress vécue par le personnel. En plus de saper la confiance entre une organisation et ses employés, de telles mesures pourraient être contre-productives et aboutir à une hausse des taux d'absentéisme et de roulement des personnels. Aussi le CEPD a-t-il mis l'accent sur le besoin de toujours s'interroger pour établir si tel ou tel suivi proposé est réellement nécessaire, s'il est exagéré et si les mêmes objectifs pourraient être accomplis par d'autres méthodes. Nous avons également souligné la nécessité de veiller à ce que les politiques de suivi soient explicites, de les détailler dans des décisions formelles ou des manuels rédigés en langage convivial, et d'en discuter avec les représentants du personnel préalablement à l'adoption d'un système quelconque. Par ailleurs, le CEPD a souligné que de telles procédures doivent veiller à un niveau élevé d'exactitude, de fiabilité et de cohérence des données. Même avec de telles garanties, le CEPD conseille que la direction reconnaisse clairement et explicitement les limitations de l'influence des données sur les décisions, plus particulièrement celles qui affectent des membres individuels du personnel.

Dans un cas, le CEPD a estimé légitime que la direction d'une unité de traduction contrôle la productivité individuelle de son personnel. Il convient toutefois de ne pas utiliser ce contrôle comme seul outil d'évaluation et des garanties suffisantes

doivent être apportées aux membres du personnel à l'égard de la rectification des données inexactes ou de la justification de certains chiffres.

### **Horaire flexible**

Le contrôle des heures de travail du personnel est un autre aspect à considérer dans le contexte du respect de la vie privée au travail. De nombreuses institutions et agences ont mis en place des politiques permettant au personnel d'adopter un horaire de travail flexible. Le CEPD a rappelé aux institutions que les données enregistrées par tout système d'horaire flexible ne devraient pas être utilisées dans le cadre d'un contrôle général de la présence au travail. Cette approche a été soulignée par l'objection du CEPD à l'envoi de courriers électroniques aux chefs d'unités lorsqu'un membre du personnel enregistrait ses heures de travail sur un système d'horaire flexible. Le CEPD a également fait opposition à l'utilisation des données de contrôle d'accès pour une vérification systématique du bon usage d'un système d'horaire flexible. Il a ordonné que les données de contrôle d'accès soient utilisées uniquement dans le cadre d'une procédure administrative prédéterminée enquêtant sur un soupçon spécifique et fondé d'abus du système d'horaire flexible.

### **Enquêtes de sécurité**

Un autre sujet de préoccupation concernant le respect de la vie privée au travail réside dans les enquêtes de sécurité menées dans certaines institutions et agences. Les services de sécurité de quelques institutions et de organes sont autorisés à prendre certaines mesures contre les actes criminels ou illégitimes visant des bâtiments occupés par l'institution/l'organe ou les personnes travaillant dans ces bâtiments (ou y ayant accès), ainsi que contre tous autres actes pouvant nuire à l'institution. Dans ce contexte également, le CEPD a souligné l'importance du principe de proportionnalité dans les enquêtes menées, notamment la «nécessité» du traitement des données, qui doit être évaluée au cas par cas. De ce point de vue, le CEPD a souligné que le traitement de données à caractère personnel requis dans le contexte des enquêtes doit être **proportionnel** non seulement au but **général** de l'opération de traitement (enquête sur des délits criminels, protection des personnes et des biens, etc.) mais aussi au but **particulier** de l'opération de traitement dans le contexte de l'affaire (en tenant compte, par exemple, de la gravité de l'incident objet de l'enquête, du type de données nécessaires pour éclairer les faits, etc.)

Dans ce contexte particulier, le CEPD a également rappelé aux institutions que chaque fois que l'accès aux données à caractère personnel paraît nécessaire aux fins de l'enquête, cet accès doit respecter les garanties appropriées, en tenant compte de tout risque potentiel d'**inadmissibilité des preuves** dans un dossier pénal futur éventuel, pouvant se présenter si les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel ne sont pas respectés au moment du rassemblement des preuves. Une attention particulière doit être accordée au respect de ces principes lorsque l'accès à des fichiers qui sont manifestement de nature privée paraît nécessaire aux fins de l'enquête.

Ces mêmes principes s'appliquent également aux opérations de traitement faisant intervenir **l'analyse criminalistique des ordinateurs**. Le CEPD estime que des précautions spécifiques devraient être prises concernant l'accès au contenu d'un ordinateur appartenant à une institution communautaire, étant donné qu'il peut également contenir des fichiers utilisés par l'employé(e) à des fins privées (par exemple dans le dossier «Mes documents» ou des courriers électroniques marqués «privé») ou des fichiers qui sont sans rapport avec l'enquête ou dont l'examen serait exagéré dans le cadre de celle-ci. L'analyse criminalistique des ordinateurs doit être soumise à des mécanismes d'autorisation particuliers. À cet égard, le CEPD recommande l'adoption de procédures formelles pour la conduite des analyses criminalistiques d'ordinateurs, qui permettront également de veiller au respect du principe de qualité des données.

## **Vidéosurveillance**

La vidéosurveillance est un autre domaine dont l'impact sur le respect de la vie privée au travail est significatif. Nous savons tous que la vidéosurveillance est devenue un outil très utilisé pour résoudre les problèmes de sécurité. Elle a également une présence accrue à l'intérieur des institutions et organes communautaires qui l'utilisent pour assurer la sécurité de leurs bâtiments, de leurs employés et de leurs visiteurs, ainsi que pour protéger les biens et les informations présents dans leurs locaux.

En dépit de sa popularité et de ses avantages potentiels, certains droits fondamentaux sont en jeu, dont le droit au respect de la vie privée au travail, le droit d'être libre de toute discrimination, la liberté d'expression et la liberté de réunion; autant de droits auxquels nous tenons profondément et qui ne sont que trop souvent tenus pour acquis en Europe. Par conséquent, les décisions sur l'installation ou non de caméras et sur leur utilisation ne devraient pas reposer uniquement sur les besoins sécuritaires. Il convient plutôt de peser les besoins sécuritaires par rapport au respect des droits fondamentaux de l'individu.

Dans ce contexte et dans un climat de préoccupation grandissante vis-à-vis de la surveillance, le CEPD travaille actuellement à des lignes directrices en matière de vidéosurveillance pour les institutions et organes communautaires. Ces lignes directrices sont conçues pour donner des conseils pratiques aidant à décider s'il convient ou non d'installer du matériel de vidéosurveillance, ainsi que sur les meilleurs moyens d'aborder les questions de protection des données dans les situations où ce matériel est employé. Une version de consultation de l'avant-projet a été publiée en juillet; je vous invite à la consulter sur notre site internet à l'adresse suivante:

<http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines>

Nous prévoyons la publication officielle des lignes directrices avant la fin de cette année. Elles concernent principalement la vidéosurveillance à des fins sécuritaires mais abordent également la question du contrôle des employés.

Le cadre de conformité proposé dans les lignes directrices est axé sur la nécessité de s'éloigner d'une culture qui considère la protection des données comme

un fardeau administratif et de se rapprocher d'une démarche reposant sur la prise en compte du respect de la vie privée dès la conception, sur la transparence dans le processus décisionnel local faisant intervenir tous les intéressés, sur des rôles actifs pour les délégués à la protection des données, et sur la responsabilisation des institutions.

En ce qui concerne le contrôle des employés, nous croyons fermement que des mesures exagérément intrusives peuvent causer un stress inutile aux employés et saper la confiance au sein d'une organisation. Il convient par conséquent d'éviter l'utilisation de la vidéosurveillance pour contrôler la manière dont les employés effectuent leur travail, sauf dans des circonstances exceptionnelles.

Pour déterminer si la vidéosurveillance à des fins autres que sécuritaires (par exemple, le contrôle des employés) est acceptable et si une telle utilisation nécessite des garanties supplémentaires qui ne sont pas prévues dans ces lignes directrices, une approche cas par cas est nécessaire. Ainsi toute vidéosurveillance proposée devrait-elle faire l'objet d'une évaluation de l'impact sur la vie privée et la protection des données par l'institution. À cet égard, nous soulignons l'importance de la responsabilisation et de la prise de décision locale. Cependant, en raison de sa nature intrusive, le CEPD tient également à suivre de près ce type de contrôle des employés. Par conséquent, l'institution doit également soumettre ses projets au CEPD pour contrôle préalable. Lorsque l'institution propose d'utiliser la vidéosurveillance pour contrôler le travail des employés, le CEPD accordera une attention particulièrement aux opinions et préoccupations exprimées par les représentants du personnel de l'institution et établira si ces opinions ont été prises en compte.

Des objectifs tels que la gestion de la productivité sur le lieu de travail, le contrôle de la qualité, l'application des politiques des institutions ou l'apport de preuves dans le cadre de la résolution d'un litige, ne justifient généralement pas à eux seuls le contrôle des employés par vidéosurveillance dans le contexte du travail des institutions. Voici quelques exemples simples: les institutions ne devraient pas utiliser leurs systèmes de vidéosurveillance existants pour contrôler l'efficacité du personnel de nettoyage au travail tôt le matin, même si un préavis adéquat lui est donné à cet égard, et si plusieurs réclamations ont été reçues au sujet de la qualité du travail. Elles ne devraient pas non plus utiliser les images de vidéosurveillance pour vérifier si les employés arrivent au travail à l'heure ou si leurs feuilles d'horaire flexible correspondent à leurs heures d'arrivée et de départ enregistrées sur les caméras. Quant au contrôle déclenché par des préoccupations de sécurité ou de santé, ou autres intérêts impérieux de même type dans des circonstances exceptionnelles, le CEPD évaluera l'utilisation de la vidéosurveillance au cas par cas.

Des problèmes complexes se posent également lorsqu'il s'agit de savoir si et, le cas échéant, dans quelles circonstances et sous réserve de quelles garanties, les images de vidéosurveillance devraient être utilisées pour des enquêtes internes, par exemple les enquêtes sur les fraudes aux prestations sociales, l'incompétence professionnelle, le harcèlement d'employés ou la fraude aux marchés publics.

Notre recommandation générale aux institutions est de déclarer clairement que la vidéosurveillance n'est pas utilisée pour contrôler la performance des employés et qu'elle ne sera pas non plus utilisée comme outil d'enquête ou comme preuve dans les

enquêtes internes ou les procédures disciplinaires, sauf en cas d'incident de sécurité ou de comportement criminel. Cela dit, les lignes directrices sont souples et des exceptions peuvent être accordées, moyennant une justification adéquate par les institutions de la nécessité et de la proportionnalité de la mesure proposée au moyen d'une évaluation de l'impact sur le respect de la vie privée et la protection des données et d'une procédure de contrôle préalable par le CEPD.

Il convient en outre d'éviter les pratiques mettant un(e) employé(e) sous surveillance constante (continuellement dans le champ de vision des caméras de vidéosurveillance). Par exemple, les institutions ne devraient pas utiliser des caméras de vidéosurveillance pour surveiller continuellement le caissier/la caissière et la caisse de la cantine aux heures d'ouverture, même si un préavis adéquat lui a été donné à cet égard.

Je tiens enfin à mentionner, toujours au sujet de la vidéosurveillance au travail, le problème de la «surveillance dissimulée». L'utilisation de la surveillance dissimulée est hautement intrusive en raison de sa nature secrète. De plus, elle n'a que peu ou aucun effet préventif et est souvent simplement proposée comme une forme de piège pour obtenir des preuves. Il convient donc d'en éviter l'utilisation. Les exceptions proposées, une fois de plus, doivent être accompagnées d'une justification solide, d'une évaluation de l'impact sur le respect de la vie privée et la protection des données, et être soumises à un contrôle préalable par le CEPD. Selon les besoins, ce dernier peut imposer des garanties spécifiques de protection des données. En principe, il est peu probable que le CEPD émette un avis positif à l'issue d'un contrôle préalable dans ce type de situation, à moins que ne soient remplies plusieurs conditions très strictes.