[pouvoir disciplinaire de l'employeur]

Quelles sont les limites de la vidéosurveillance ?

La mise en place d'un système de vidéosurveillance, qui permet d'enregistrer les faits et gestes des salariés, est soumise à des exigences strictes. Jusqu'à présent, l'accent était placé sur l'information préalable des salariés et de leurs représentants. Mais la Cnil a rappelé qu'un dispositif de vidéosurveillance doit également être justifié par la nature de la tâche à accomplir et proportionné au but recherché, et que l'information des salariés doit être suffisamment précise.

Faits : à la suite d'une plainte, la Commission nationale de l'informatique et des libertés (Cnil) procède à un contrôle au sein d'une société de prêt-à-porter (sur les modalités d'un tel contrôle, voir p. 12). Après deux heures d'investigations, la délégation de la Cnil se voit contrainte d'interrompre sa mission, le directeur général de la société lui ordonnant de quitter les lieux – ce qui vaudra à ce dernier une condamnation par le tribunal correctionnel pour entrave à l'action de la commission. Munie cette fois d'une autorisation du président du tribunal de grande instance, la commission effectue un second contrôle deux mois plus tard. Elle constate alors que, pour lutter contre le vol, un système de vidéosurveillance composé de 23 caméras est implanté au sein des trois magasins et du siège social de l'entreprise, les images filmées étant enregistrées en continu sur un support numérique. La Cnil relève plusieurs manquements à la loi informatique et libertés [L. n° 78-17, 6 janv. 1978, JO 7 janv., modifié par L. n° 2004-801, 6 août 2004, JO 7 août] : le système ne lui a pas été préalablement déclaré ; des caméras sont placées dans des lieux réservés au personnel où aucune marchandise n'est entreposée ; seules les personnes embauchées postérieurement à l'installation des caméras ont été informées, par le biais d'une clause de leur contrat, de l'existence de ce dispositif ;

l'accès aux images enregistrées peut être effectué à partir de postes informatiques non protégés par un mot de passe. La Cnil met alors la société en demeure de se conformer aux dispositions de la loi informatique et libertés. L'employeur se soumet partiellement à ces injonctions : il procède à la déclaration du système de vidéosurveillance auprès de l'institution et renforce la sécurité du système informatique, mais il refuse de retirer les caméras installées dans des lieux réservés au personnel où aucune marchandise n'est stockée et se borne à informer les salariés de l'existence d'un système de vidéosurveillance, sans plus de précision.

➡**Solution :** considérant que l'entreprise n'a que partiellement répondu à la mise en demeure qui lui était adressée, la formation contentieuse de la Cnil se penche sur la légalité de son système de vidéosurveillance. Elle estime que le fonctionnement de ce dispositif constitue une collecte illicite de données personnelles, aux motifs qu'il est disproportionné au regard de la finalité de lutte contre le vol et que l'information remise aux salariés est insuffisante. Elle décide, en conséquence, d'infliger à la société une sanction pécuniaire de 10 000 € [Délib. Cnil n° 2009-201, 16 avr. 2009].

Cette décision comporte des précisions importantes sur les règles à suivre pour mettre en place un système de vidéosurveillance. Le point sur ces obligations.

Déclarer préalablement le système à la Cnil

➡**Le principe : une déclaration préalable à la Cnil.** L'employeur doit déclarer à la Cnil la mise en place d'un dispositif de vidéosurveillance dans l'entreprise, dès lors que ce dispositif s'accompagne d'un système d'enregistrement ou de conservation des images dans des traitements informatisés ou des fichiers nominatifs. Cette déclaration doit être préalable à la mise en place du dispositif. À défaut, l'employeur peut être condamné à réparer le préjudice subi par les salariés, même s'il a ultérieurement régularisé la situation [Cass. soc., 7 juin 1995, n° 91-44.919]. Un système qui n'aurait pas été préalablement déclaré à la Cnil ne peut, en outre, être opposé aux salariés [Cass. soc., 6 avr. 2004, n° 01-45.227] : dans cette affaire, la Cour de cassation a ainsi jugé sans cause réelle et sérieuse le licenciement d'un salarié qui avait refusé d'utiliser son badge, au motif que l'employeur n'avait pas déclaré le système mis en place.

➡**Une autorisation préfectorale lorsque les lieux filmés sont partiellement ouverts au public ?** Lorsque les lieux où sont installées les caméras sont pour partie privés (atelier, usine) et pour partie ouverts au public (magasin ouvert aux clients), une déclaration préalable à la Cnil n'est semble-t-il pas suffisante. La difficulté provient de l'existence de deux régimes distincts : celui de la loi informatique et libertés et celui de la loi de programmation pour la sécurité, qui exige une autorisation préfectorale préalable en cas de mise en place d'un dispositif de vidéosurveillance dans des lieux publics ou ouverts au public [L. n° 95-73, 21 janv. 1995, art. 10, JO 24 janv.].

Dans deux situations, les choses sont claires :
– lorsque le dispositif de vidéosurveillance est installé uniquement dans un lieu ouvert au public et qu'aucune image n'est enregistrée ni conservée dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques. Dans ce cas, seule une autorisation préfectorale est nécessaire ;
– lorsque le dispositif de vidéosurveillance est installé uniquement dans un lieu privé et que les images sont enregistrées ou

conservées dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques. Seule une déclaration auprès de la Cnil est alors requise.

Mais le régime n'est pas évident, de l'aveu même de la Cnil, lorsque le dispositif de vidéosurveillance est installé dans un lieu mixte (lieu ouvert au public qui comporte également des zones privées). Dans ce cas, si les images sont enregistrées ou conservées dans un fichier nominatif, une déclaration à la commission est nécessaire. L'employeur doit-il également solliciter une autorisation préfectorale ? Il convient, pour plus de prudence, de considérer que les deux formalités se cumulent.

Ne pas instaurer de surveillance généralisée et continue

➡ Dans la mesure où il porte atteinte aux droits fondamentaux et libertés individuelles des salariés – en particulier le droit au respect de l'intimité de la vie privée –, un système de contrôle par vidéosurveillance doit être **justifié par la nature de la tâche à accomplir et proportionné au but recherché** [C. trav., art. L. 1121-1].

Le plus souvent, la mise en place d'un dispositif de vidéosurveillance obéit à un objectif de sécurité (contrôler l'accès des locaux, surveiller les zones de travail à risques, etc.). Si un tel objectif est légitime, serait en revanche illicite le dispositif destiné à surveiller uniquement un salarié ou un groupe particulier de salariés. De même, est illégal le système destiné à enregistrer de manière spécifique les entrées et sorties des locaux syndicaux.

Quant aux modalités de la vidéosurveillance, elles doivent être adéquates et proportionnées à l'objectif poursuivi. La Cnil explique ainsi que, pour apprécier si un système de vidéosurveillance susceptible de viser des membres du personnel est strictement nécessaire à l'objectif poursuivi, il convient de tenir compte du nombre, de l'emplacement, de l'orientation, des périodes de fonctionnement des caméras et de la nature des tâches accomplies par les personnes filmées. Ainsi, est illégal le système de vidéosurveillance installé dans les vestiaires, les douches ou les toilettes. Par ailleurs, si l'enregistrement des images peut être nécessaire pour assurer la sécurité des locaux ou des biens, il n'en va pas de même de l'enregistrement du son qui y est associé ; peut donc être considéré comme disproportionné le dispositif reposant sur l'enregistrement des images et du son associé.

➡ Dans l'affaire dont la Cnil était saisie, l'installation des caméras de vidéosurveillance dans l'entreprise était justifiée, selon l'employeur, par la volonté de lutter contre le vol de marchandises. Si cet objectif a bien été jugé légitime par la Cnil, les moyens mis en œuvre pour l'atteindre lui sont, en revanche, apparus disproportionnés.
En effet, l'objectif de lutte contre le vol de marchandises ne justifie nullement l'installation de caméras dans des locaux où il n'existe aucun risque de vol puisque aucune marchandise n'y est stockée, tels les couloirs, les ateliers de création ou les bureaux administratifs dans l'affaire dont il est ici question. En outre, cet objectif ne peut conduire, comme c'était le cas ici, à filmer les salariés en continu et, ainsi, à les placer sous la surveillance constante de l'employeur. En résumé, le déploiement d'un dispositif de surveillance, même justifié par un impératif de sécurité, **ne doit pas conduire à une mise sous surveillance généralisée et permanente du personnel.**

Informer précisément les salariés

Information exigée par le Code du travail

Simple information préalable du salarié. Le Code du travail exige de l'employeur qu'il informe le salarié de la mise en place de tout dispositif permettant de collecter des informations qui le concernent personnellement [C. trav., art. L. 1222-4]. En application de cette règle, l'employeur est tenu de « porter préalablement à la connaissance » du salarié tout système de vidéosurveillance qui permet de capter son image.
Cette information constitue une formalité substantielle selon la Cour de cassation : tout élément recueilli à l'aide d'un dispositif de contrôle, comme une caméra de surveillance, qui a été mis en place à l'insu du salarié, constitue un **mode de preuve illicite.** Ainsi, a été jugé irrecevable l'enregistrement du comportement et des paroles d'une salariée, effectué par une caméra dissimulée à proximité de son poste de travail, dont la présence n'avait pas été préalablement portée à sa connaissance [Cass. soc., 20 nov. 1991, n° 88-43.120].

Il existe cependant une exception à cette règle : la Cour de cassation considère que l'employeur n'a pas à informer les salariés d'un système de vidéosurveillance installé dans des entrepôts ou autres locaux de rangement dans lesquels ces derniers **ne travaillent pas** [Cass. soc., 31 janv. 2001, n° 98-44.290]. Il n'est pas non plus tenu de divulguer l'existence des procédés installés par les clients de l'entreprise, dans des locaux auxquels les salariés n'ont pas accès [Cass. soc., 19 avr. 2005, n° 02-46.295]. Par conséquent, est recevable la preuve issue d'un dispositif de vidéosurveillance installé par un client de l'entreprise, qui avait pour objet, non pas de contrôler l'activité des salariés, mais de surveiller la porte d'accès d'un local dans lequel ceux-ci ne devaient avoir aucune activité.

Information et consultation du comité d'entreprise. La mise en place d'un système de vidéosurveillance doit également faire l'objet d'une information et d'une consultation préalables du comité d'entreprise [C. trav., art. L. 2323-32, al. 3]. Cette information-consultation constitue elle aussi une formalité substantielle : tout élément de preuve issu d'un dispositif de vidéosurveillance dont l'installation n'a pas fait l'objet d'une information et d'une consultation du comité d'entreprise est illicite et donc irrecevable en justice. La consultation du CHSCT ne peut pas se substituer à celle du comité d'entreprise [Cass. soc., 7 juin 2006, n° 04-43.866].

À NOTER
Même si, à notre connaissance, la Cour de cassation ne s'est jamais prononcée sur cette question, il semble plus prudent d'informer et de consulter le CHSCT préalablement à la mise en place d'un système de vidéosurveillance. En effet, l'installation d'un dispositif de contrôle de l'activité des salariés pourrait être considérée comme une modification importante de leurs conditions de travail [C. trav., art. L. 4612-8].

Exigences de la loi informatique et libertés

Le Code du travail et la Cour de cassation se satisfaisaient jusqu'à présent d'une simple information préalable du salarié, sans poser d'exigence particulière quant aux modalités et au contenu de cette information. La remise d'une note interne ou d'une circulaire informant les salariés de la présence de caméras dans les locaux de l'entreprise semblait donc suffisante.
Cependant, la loi informatique et libertés est bien plus exigeante, comme le rappelle la Cnil. Selon l'article 32 de cette loi, le responsable d'un traitement automatisé de données personnelles est tenu d'informer les per-

sonnes concernées par le traitement de sa finalité, du caractère obligatoire ou facultatif des réponses, des destinataires des informations, ainsi que de leurs droits d'accès, de rectification et, le cas échéant, d'opposition. S'agissant d'un dispositif de vidéosurveillance susceptible de viser les membres du personnel, la commission estime que les salariés doivent être informés :
– des finalités poursuivies par le dispositif ;
– des destinataires des images ;
– des modalités concrètes de l'exercice du droit d'accès dont ils disposent.

Dans l'affaire ayant donné lieu à la délibération de la Cnil examinée ici, l'information délivrée aux salariés a été jugée nettement insuffisante. La clause insérée dans les contrats de travail des salariés embauchés après l'installation des caméras et la circulaire adressée à tous les salariés de l'entreprise, postérieurement à la mise en demeure de la Cnil, les informaient seulement de l'existence d'un système de vidéosurveillance dans tous les sites de l'entreprise, mais ni de la finalité de ce dispositif, ni des destinataires des images enregistrées, ni de leur droit d'accès aux données personnelles les concernant. Les panneaux d'information à destination de la clientèle, apposés derrière le guichet d'accueil des magasins, et les affichettes disposées à divers endroits ne permettaient pas davantage de satisfaire ces exigences.

Sécuriser le système d'information

Selon l'article 34 de la loi informatique et libertés, le responsable d'un traitement automatisé de données à caractère personnel est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès (voir encadré p. 26).

L'entreprise qui met en place un système de vidéosurveillance doit donc prendre toute mesure nécessaire pour **garantir la sécurité et la confidentialité des données enregistrées.** Le système d'information qui permet de stocker et de consulter ces données doit donc, lui-même, être sécurisé, afin que seules les personnes habilitées de par leurs fonctions puissent y avoir accès. Dans l'affaire qui nous intéresse ici, la Cnil avait relevé, lors de son contrôle sur place, que l'accès au logiciel de « supervision » et celui aux serveurs informatiques n'étaient pas sécurisés : les images filmées étaient accessibles à partir de deux postes de supervision situés à l'accueil et dans le bureau du PDG, sans mot de passe sur la station de supervision de l'accueil ; deux serveurs étaient également libres d'accès.

Néanmoins, après la mise en demeure, l'entreprise avait procédé à la sécurisation de son système d'information, en isolant le serveur d'enregistrement dans un local muni d'un système de verrouillage dont l'accès était réservé aux responsables habilités et en limitant l'accès au visionnage des images au seul représentant légal de la société, au moyen d'un mot de passe. La commission a considéré que ces démarches permettaient de garantir la sécurité des données enregistrées et étaient, par conséquent, satisfaisantes.

À NOTER
Selon la Cnil, les images enregistrées ne doivent pas être conservées plus de quelques jours, en tout état de cause au-delà d'un mois. Il convient, par conséquent, lorsque c'est techniquement possible, de paramétrer dans le système d'information une durée maximale de conservation des images.

Les dix conseils de la Cnil pour sécuriser un système d'information

La Cnil a publié, sur son site Internet, dix conseils pour sécuriser les données contenues dans un système d'information. En voici un bref résumé.

➔**Adopter une politique de mot de passe rigoureuse.** Le mot de passe pour l'accès à un poste de travail ou à un fichier doit être individuel, comporter au minimum huit caractères, et être renouvelé fréquemment.

➔**Concevoir une procédure de création et de suppression des comptes utilisateurs.** Il est préférable de créer des comptes utilisateurs (et des comptes des administrateurs réseaux) nominatifs, et non génériques, afin de pouvoir tracer les interventions faites sur un fichier et de responsabiliser les intervenants.

➔**Sécuriser les postes de travail.** Il est recommandé de paramétrer les postes de travail afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité, d'inciter les utilisateurs à verrouiller leur poste de travail dès qu'ils s'absentent et de limiter l'usage des ports USB sur les postes sensibles.

➔**Identifier précisément qui peut avoir accès aux fichiers.** L'accès aux données personnelles contenues dans un fichier doit être réservé aux personnes qui peuvent légitimement y avoir recours pour l'exécution de leurs missions. Pour ce faire, il convient de vérifier les profils des applications et les droits d'accès périodiquement et lors de chaque nouvelle affectation d'un salarié.

➔**Veiller à la confidentialité des données vis-à-vis des prestataires.** Pour garantir la sécurité et la confidentialité des données, les interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre. Les données « sensibles », comme les données de santé ou les données relatives à des moyens de paiement, doivent être chiffrées.

➔**Sécuriser le réseau local.** Le système d'information doit être sécurisé vis-à-vis des attaques extérieures. La messagerie électronique, les réseaux sans fil et les accès distants au système d'information par les postes nomades doivent faire l'objet d'une vigilance particulière.

➔**Sécuriser l'accès physique aux locaux.** Il est préconisé de limiter l'accès aux locaux qui hébergent les serveurs informatiques et les éléments du réseau aux personnes habilitées, en usant d'une sécurisation particulière : badge, gardiennage, portes fermées à clef…

➔**Anticiper le risque de perte ou de divulgation des données.** Il convient de stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs. Il convient également de s'assurer que les matériels recyclés, réaffectés ou donnés soient préalablement vidés des données qui y sont stockées.

➔**Anticiper et formaliser une politique de sécurité du système d'information.** L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des salariés et régulièrement mis à jour.

➔**Sensibiliser les utilisateurs aux « risques informatiques » et à la loi informatique et libertés.** Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service ou de fiches pratiques. Il est également suggéré d'élaborer une « charte informatique » qui précise les règles à respecter en matière de sécurité informatique, d'utilisation de la téléphonie, de la messagerie électronique ou d'Internet. Les utilisateurs doivent enfin être incités à nettoyer régulièrement leurs vieux documents et messages électroniques sur leurs postes.