2

Vidéosurveillance : le Conseil d'Etat dessine les contours de la protection des salariés

Par Christèle Morand, avocat associé, Eole Avocats

Pour être valable, un dispositif de surveillance des salariés doit être légitime et proportionné au but poursuivi, avoir été porté à la connaissance des salariés et les données collectées doivent être sécurisées.
Christèle Morand, avocat associé au sein du cabinet Eole Avocats, revient sur ces règles à la lumière d'une décision du Conseil d'Etat du 18 novembre 2015.

1 Comme d'autres technologies de contrôle déployées dans l'entreprise, la vidéosurveillance interfère nécessairement avec la **sphère de la vie privée** des salariés, et engendre à ce titre pour l'employeur des obligations et contraintes juridiques, dont force est de constater qu'elles sont loin encore d'être maîtrisées.
Or, s'il est admis de longue date que l'employeur peut mettre en place un système de vidéosurveillance au sein de son entreprise (Cass. soc. 20-11-1991 n° 88-43.120 : RJS 1/92 n° 1), le **contournement** (voire le détournement) des règles à observer peut être lourd de conséquences, comme on le verra par la suite (n° 22).

2 Ainsi, comme le juge régulièrement la **Cour de cassation**, si l'employeur peut surveiller l'activité de ses salariés et les sanctionner, il ne peut pas le faire par des procédés qui n'ont pas été portés préalablement à leur connaissance, ni procéder à une surveillance illicite. Et conformément à la **loi « informatique et libertés »**, en cas de traitement de données à caractère personnel recueillies au moyen d'un dispositif de contrôle, les données collectées doivent l'être « de façon adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi ».
La Commission nationale informatique et libertés (**Cnil**), garante de la bonne application de la loi « informatique et libertés », est l'acteur majeur de protection des droits fondamentaux des salariés dans le monde professionnel numérique : outre un rôle de conseil, elle opère des **contrôles** du respect de cette loi, qui aboutissent parfois à des sanctions pécuniaires.

3 C'est tout l'intérêt de la décision du Conseil d'Etat du 18 novembre 2015 (CE 18-11-2015 n° 371196 : FRS 25/15 4 p. 7) qui vient rappeler les règles principales à observer pour que la vidéosurveillance en entreprise évite la censure de la Cnil.
Profitant d'une espèce dans laquelle la Cnil avait sanctionné pécuniairement l'employeur d'une « amende » de 10 000 euros (situation de plus en plus fréquente si l'on en croit ses statistiques les plus récentes), le Conseil d'Etat invite les entreprises à édicter un **dispositif légitime et proportionné** au but poursuivi (1re exigence) ; rappelle que celui-ci doit avoir été porté à la **connaissance des salariés** et des représentants du personnel (2e exigence) ; et exige enfin que les **données récoltées soient sécurisées** (3e exigence).

Un dispositif légitime et proportionné au but poursuivi

4 Cela paraît relever de l'évidence, mais le dispositif de surveillance doit, en premier lieu, respecter les libertés individuelles et la vie privée des salariés. Le principe, bien connu, est posé à l'article L 1121-1 du Code du travail : « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».
En termes moins juridiques, il faut **concilier** la finalité pour l'entreprise du dispositif de surveillance et le respect de la vie privée des salariés sur leur lieu de travail (notamment leur droit à l'image). Dans sa décision, le Conseil d'Etat confirme les sanctions prononcées par la Cnil, notamment en raison de la **finalité** du dispositif invoquée par l'employeur et de la **disproportion** à celle-ci.

Christèle Morand est avocat associé au sein du cabinet Eole Avocats (Paris – Lyon – DOM). Avocat depuis 2003, elle a collaboré précédemment au sein du cabinet Yramis Avocats et Fromont Briens & Associés. Elle intervient dans les domaines du droit du travail et de la protection sociale, tant en conseil qu'en contentieux, et collabore régulièrement en tant qu'expert-formateur pour Francis Lefebvre Formation.

La vidéosurveillance sert à assurer la sécurité des biens et des personnes

5 Pour justifier le recours à la vidéosurveillance, la société prestataire de services informatiques avait invoqué la nécessité d'assurer la **sécurité de son personnel et de ses équipements**, ainsi que le **caractère confidentiel** de ses missions. Cet argumentaire n'a pas convaincu le Conseil d'Etat, qui relève, tout comme l'avait fait la Cnil, que la sécurité des locaux était ici déjà suffisante, l'entrée ne pouvant s'opérer qu'après autorisation et vérification d'identité. Les magistrats en concluent qu'en dehors de « la volonté de la direction de lutter contre des vols susceptibles d'être perpétrés par ses propres salariés, rien ne venait étayer les préoccupations de sécurité alléguées » par l'employeur.

6 Il faut rappeler ici qu'un dispositif de surveillance en entreprise peut poursuivre des **finalités** de divers ordres :
– assurer la sécurité des biens et des personnes, lorsqu'il existe un risque particulier de vols dans l'entreprise, à titre dissuasif ou pour identifier les auteurs de vols, d'agressions ou de dégradations ;
– surveiller un poste de travail particulièrement dangereux ;
– garantir une protection spéciale résultant d'une obligation de secret-défense.

Ces finalités doivent être non seulement légitimes mais surtout **respectées** ; à défaut, l'employeur risque une condamnation délictuelle. Le Code pénal prévoit qu'un tel détournement est réprimé par une peine pouvant aller jusqu'à **3 ans d'emprisonnement et 300 000 euros d'amende** (C. pén. art. 226-21).

Les salariés ne peuvent pas être sous surveillance permanente

7 Le second motif de sanction, confirmé par le Conseil d'Etat, tient au **positionnement des caméras**. S'il existe un motif légitime de recours à la surveillance, encore faut-il que le procédé mis en place n'empiète que de manière « relative » sur le droit à la vie privée des salariés contrôlés. En ce sens, la Cnil a considéré disproportionné un système mis en place dans un centre commercial déployant 240 caméras, filmant même l'accès aux toilettes, la salle de pause, les vestiaires et le cabinet médical, mettant ainsi les salariés sous une surveillance permanente à leur poste de travail (Délibération Cnil 2013-29 du 12-7-2013).

8 Le Conseil d'Etat relève ici que lors de ses contrôles, la Cnil avait constaté qu'une caméra « permettait de voir le poste de travail d'une salariée et qu'une autre était orientée en direction d'une salle où travaillaient 6 personnes », assimilable à un placement sous surveillance non proportionné aux finalités poursuivies par le dispositif.

« La caméra ne doit en aucun cas être figée sur un poste de travail ou sur une personne en particulier »

En effet, « si le déploiement de tels dispositifs sur un lieu de travail répond généralement à un objectif sécuritaire (contrôle d'accès aux locaux, surveillance de zones de travail à risque), il ne peut avoir pour seul objectif la mise sous **surveillance spécifique** d'un employé déterminé ou d'un groupe d'employés » (Guide Cnil 2010 pour les employeurs et les salariés, fiche 8 p. 26).

9 Par ailleurs, « dès lors qu'un dispositif de vidéosurveillance est susceptible de viser des membres du personnel, le nombre, l'emplacement, l'orientation, les périodes de fonctionnement des caméras ou la nature des tâches accomplies par les salariés sont autant d'éléments à prendre en compte lors de l'installation du système » (Délibération Cnil 2009-201 du 16-4-2009). Les caméras ne peuvent donc pas être disposées **aléatoirement** : leur positionnement est particulièrement encadré et contrôlé. Le plan des emplacements doit être réfléchi et correspondre strictement à la finalité du dispositif de surveillance. Il ne peut pas ainsi conduire à placer les salariés sous une surveillance **constante et permanente**. La caméra ne doit en aucun cas être figée sur un poste de travail ou sur une personne en particulier : au travail comme ailleurs, tout un chacun doit être garanti du respect du droit à l'image et à la vie privée.
Des **exceptions** à cette règle existent toutefois, notamment pour les postes dangereux ou pour les postes impliquant la manipulation d'argent (dans ce cas, c'est la caisse qui doit être filmée et non le salarié).

10 Dans les autres cas, la Cnil autorise que les caméras soient régulièrement placées au niveau des entrées et sorties du bâtiment, des voies de secours et des voies de circulation (couloirs). Les caméras ne doivent pas filmer les **zones de pause ou de repos** des salariés (ni leur accès), les **vestiaires** ou les **toilettes** évidemment (Délibération Cnil 2014-307 du 17-7-2014, notamment). Si des dégradations sont constatées sur un distributeur alimentaire, les caméras ne doivent filmer que les distributeurs et non toute la pièce.
Une **illustration récente** est donnée par la cour d'appel de Metz, laquelle a prononcé la résiliation judiciaire du contrat de travail d'une salariée aux torts de l'employeur : la vidéosurveillance mise en place dans la boulangerie n'était pas proportionnée, en raison du placement de certaines caméras dans le laboratoire où se trouvaient les fours et machines à pains, sans que puisse être justifiées la prévention des atteintes aux biens invoquée ni la nécessité d'assurer la sécurité du personnel (CA Metz 3-11-2015 n° 14-01404).

11 Enfin, une interdiction particulière est à souligner, concernant les caméras filmant les locaux des **représentants du personnel** et leur accès (lorsqu'ils mènent à ces seuls locaux) : au-delà du caractère non proportionné du procédé, celui-ci pourrait caractériser un délit d'entrave au libre fonctionnement des institutions représentatives du personnel.

Un dispositif transparent

12 La légalité du dispositif de vidéosurveillance installé dans l'entreprise suppose le respect d'une **transparence** garantie à 3 niveaux : vis-à-vis des salariés tout d'abord, des instances de représentation du personnel ensuite, et de la Cnil enfin.

Les salariés doivent être individuellement informés

13 En premier lieu, chaque salarié doit avoir été individuellement informé de la mise en place de la vidéosurveillance, en application de l'article L 1222-4 du Code du travail. La Cnil ajoute que les salariés doivent, comme cela résulte de la loi « informatique et libertés », être informés des **finalités** du dispositif, des **destinataires** des images et des modalités concrètes de l'exercice de leur **droit d'accès** à ces données (Délibération Cnil 2009-201 du 16-4-2009).
L'information est donc primordiale car elle constitue une condition de la légalité de la vidéosurveillance dans l'entreprise. Elle doit être réalisée de façon **expresse et individuelle** : l'envoi d'un courrier ou la remise d'une **notice informative** en main propre contre décharge est conseillée, pour rapporter la preuve de la réalité de cette information ; une **mention portée au contrat de travail** peut être également envisagée, lorsque cela est possible.

14 Il faut ajouter que cette information dépasse le cadre strict de l'entreprise employeur : elle est obligatoire également lorsque la vidéosurveillance est mise en place chez un **client de l'employeur** (Cass. soc. 10-1-2012 n° 10-23.482 : RJS 3/12 n° 212). Il s'agissait ici d'une société de **nettoyage** dont certains salariés intervenaient chez un client ayant installé au sein de ses locaux des caméras de surveillance. Si les salariés de l'entreprise de nettoyage avaient été informés de l'existence de ces caméras, il n'avait pas été porté à leur connaissance que leur employeur pouvait utiliser les images enregistrées pour contrôler leur activité, et notamment leurs horaires. La chambre sociale de la Cour de cassation a considéré que l'obligation d'information n'avait pas été respectée et que les images en question ne leur étaient donc pas opposables.

L'existence du dispositif doit être affichée dans l'entreprise

15 L'information passe également par un affichage dans l'entreprise rappelant l'existence du dispositif, le nom de son responsable, ainsi que la **procédure à suivre** pour demander l'accès aux enregistrements visuels et sonores. Ces indications conditionnent le respect de l'obligation d'information, comme le rappelle le Conseil d'Etat dans l'arrêt du 18 novembre 2015. En l'espèce, l'employeur avait bel et bien procédé à un affichage à l'entrée des locaux, mais celui-ci ne comportait pas les mentions précitées. L'information n'était donc opérée que de manière très **aléatoire**, selon la Cnil.

Dans une précédente délibération, la Cnil avait déjà précisé que la simple apposition d'un autocollant comportant le dessin d'une caméra et le mot « vidéo » est notoirement insuffisante (Délibération Cnil 2009-201 du 16-4-2009).

Les représentants du personnel doivent être consultés

16 L'employeur doit naturellement consulter son **comité d'entreprise** sur la mise en place de la vidéosurveillance au sein de l'entreprise, lorsque le dispositif a un but de management, c'est-à-dire de contrôle et d'évaluation. En effet, selon l'article L 2323-47 du Code du travail, le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. Ce **défaut** de consultation entraîne l'illicéité de l'utilisation des images comme mode de preuve (Cass. soc. 7-6-2006 n° 04-43.866 : RJS 11/06 n° 1143).

17 Il est préconisé de consulter en amont le **CHSCT**, même si aucun texte ne lui prévoit de façon expresse de prérogative particulière en la matière. L'article L 4612-8-1 du Code du travail prévoit en effet que le CHSCT est consulté dès lors qu'une décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail est prise par l'employeur. La mise en place de la vidéosurveillance, d'autant plus si elle sert à contrôler l'activité des salariés, peut être une source de **stress** impactant la santé et les conditions de travail, appelant donc potentiellement sa consultation.

Sauf exceptions, l'employeur doit déclarer le dispositif à la Cnil

18 L'employeur doit procéder à une déclaration auprès de la Cnil de son dispositif, pour chaque site ou établissement concerné. Deux exceptions à cette obligation sont toutefois prévues : la première, lorsque le dispositif de vidéosurveillance n'enregistre ni ne **conserve aucune image** (Avis CE 24-5-2011) ; la seconde, lorsque l'entreprise a désigné un **correspondant informatique des libertés** (CIL), à condition de lui donner les moyens de sa mission (Guide du CIL, éd. 2011).

Le **non-respect** de cette formalité déclarative prive l'employeur de la possibilité de se prévaloir, à l'appui d'une sanction disciplinaire, du refus du salarié de se conformer au dispositif installé (Cass. soc. 6-4-2004 n° 01-45.227 : RJS 6/04 n° 787). Il lui est également impossible d'utiliser les informations collectées, ce mode de preuve étant considéré comme illicite (Cass. soc. 8-10-2014 n° 13-14.921 : RJS 12/14 n° 826).

Sécurisation des données personnelles

19 Au-delà des questions de pertinence de la vidéosurveillance et de l'information des salariés, les données collectées doivent être sécurisées.

Les images enregistrées par la vidéosurveillance ne peuvent pas être consultées par n'importe qui. Seules les **personnes habilitées** doivent pouvoir y accéder et non tous les salariés. Ces personnes devront être particulièrement formées et sensibilisées aux règles de sa mise en œuvre. L'employeur ne pourra pas ainsi faire visionner les images à certains salariés afin de les divertir (CA Metz 3-11-2015 n° 14-01404). L'employeur doit veiller à protéger l'accès au dispositif contre des tiers non autorisés (Loi 78-18 du 6-1-1978, art. 34 ; voir aussi Délibération Cnil 2010-112 du 22-4-2010).

20 Dans l'arrêt du 18 novembre 2015, le Conseil d'Etat reproche à l'employeur de ne pas avoir satisfait à cette obligation de sécurisation, puisque le mot de passe permettant l'**accès aux enregistrements** était inchangé depuis 2011 et qu'il correspondait au prénom de l'agent, ce qui a été jugé insuffisant. La Cnil, lors d'un contrôle, avait relevé ce manquement, mais l'employeur n'avait pas pris les mesures nécessaires pour pallier ce manque de sécurité.

21 Selon l'article 6, 5° de la loi « informatique et libertés », l'employeur ne peut pas **conserver** indéfiniment les enregistrements d'images stockés. La Cnil admet que les enregistrements puissent être gardés jusqu'à un mois maximum, estimant qu'en cas de besoin cette **durée** de conservation sera largement suffisante pour effectuer les vérifications nécessaires.

Conséquences d'un dispositif illicite

22 Au plan individuel, les **salariés** peuvent demander à être **indemnisés du préjudice subi** du fait de la violation de l'obligation de loyauté par l'employeur (CA Aix-en-Provence 21-5-2015 n° 14-01795) : l'exécution de mauvaise foi du contrat de travail, par l'utilisation d'un procédé attentatoire à ses droits dont il ignorait l'existence, lui cause nécessairement un préjudice. D'autre part, contrairement au droit pénal (Cass. crim. 23-7-1992 n° 92-82.721), le droit civil, et tout particulièrement le droit du travail, repose sur un **système de preuve légal**. Les juges déclareront donc irrecevable toute preuve, dès lors qu'elle provient d'un système de surveillance dont la mise en place ou l'utilisation n'ont pas été réalisées dans les règles de l'art (CA Aix-en-Provence 22-12-2015 n° 14-03847). L'enjeu est de taille : les sanctions prononcées sur le fondement d'une preuve non valable sont injustifiées. S'il s'agit d'un **licenciement**, il sera nécessairement requalifié en licenciement sans cause réelle et sérieuse, avec les conséquences indemnitaires associées (Cass. soc. 23-5-2012 n° 10-23.521 : RJS 8-9/12 n° 673) et ce, quand bien même la réalité des griefs reprochés au salarié serait avérée (dans ce sens, CA Paris 4-3-2016 n° 12-10491 : RJS 5/16 n° 305). Enfin, comme cela a été souligné au fil du texte, la méconnaissance des dispositions de la loi « informatique et liberté » est passible de **sanctions pénales**.