La surveillance des salariés de l'agence

Il peut être tentant de contrôler l'activité des salariés de l'agence au moyen des outils informatiques ou de la vidéo surveillance. Une telle surveillance est possible mais elle est strictement encadrée par le Règlement Général de Protection des Données (RGPD).

La CNIL a prononcé le 19 décembre 2024 une sanction de 40 000 euros à l'encontre d'une entreprise du secteur immobilier pour une surveillance excessive des salariés. C'est l'occasion de rappeler les règles en matière de contrôle de l'activité des collaborateurs de l'agence.

Puis-je mettre en place un système de vidéo-surveillance des salariés ?

Les caméras de surveillance sont aujourd'hui largement utilisées sur les lieux de travail. Si ces outils sont légitimes pour assurer la sécurité des biens et des personnes, ils ne peuvent pas conduire à placer les employés sous surveillance constante et permanente.
La CNIL rappelait dans une recommandation du 23 juillet 2018 qu'un employeur ne peut pas installer des caméras dans ses locaux **sans définir un objectif, qui doit être légal et légitime**. Par exemple, des caméras peuvent être installées sur un lieu de travail à des fins de sécurité des biens et des personnes, à titre dissuasif ou pour identifier les auteurs de vols, de dégradations ou d'agressions.
Sauf cas exceptionnels, ces caméras ne peuvent pas filmer les employés sur leur poste de travail, dans des zones de repos ou aux toilettes ou dans des locaux syndicaux.
Les images ne doivent être accessibles qu'à un nombre limité de personnes habilitées disposant d'un mot de passe d'accès et conservées pour une durée limitée qui ne devrait pas excéder un mois.

Puis-je contrôler l'utilisation d'internet et de la messagerie électronique ?

Comme le prévoit une recommandation de la CNIL du 20 novembre 2015, **l'employeur peut contrôler et limiter l'utilisation d'internet** (dispositifs de filtrage de sites, détection de virus...) **et de la messagerie** (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « *anti-spam* »...) afin d'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie...) ou de limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux...). Une utilisation personnelle de ces outils est tolérée si elle reste raisonnable et n'affecte pas la sécurité des réseaux ou la productivité. C'est à l'employeur de fixer les contours de cette tolérance et d'en informer ses employés.
Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé.
Toutefois, l'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés ou enregistrer à distance toutes les actions accomplies sur un ordinateur. Il ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles. Il ne pourra notamment pas accéder à un dossier identifié comme « *personnel* » sur l'ordinateur du salarié.
Les informations de connexion ne peuvent pas être conservées plus de 6 mois.

Puis-je surveiller l'activité de mes salariés ?

L'employeur peut mettre en œuvre un logiciel de suivi de l'activité de ses salariés, par exemple à des fins de mesure de leur temps de travail ou de mesure de leur productivité. Toutefois, il devra dans ce cas **justifier de la raison pour laquelle il exerce de contrôle** et que ces mesures ne conduisent pas à une atteinte disproportionnée à la vie privée,

aux intérêts et aux droits fondamentaux des salariés.
Dans tous les cas, il faudra toujours respecter les principes du RGPD et notamment justifier que le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement (article 6) et que celui-ci restreigne sa collecte aux données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées *(article 5)*.

Quelle information faut-il donner aux salariés ?

S'agissant de la **vidéo surveillance, les personnes concernées**, employés et visiteurs, **doivent être informées** de son existence au moyen de panneaux affichés en permanence, de façon visible, dans les lieux concernés.
Comme le prévoit l'article 13 du RGPD, lorsqu'il collecte des données à caractère personnel, le responsable du traitement doit fournir à la personne concernée, au moment où les données en question sont obtenues, des informations relatives notamment à l'identité du responsable du traitement et le cas échéant, du délégué à la protection des données, aux finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement. Le respect de cette obligation peut notamment résulter de l'information écrite des salariés, de documents d'information internes à la société, ou d'une clause insérée dans les contrats de travail des salariés.

Quand faut-il réaliser une analyse d'impact ?

L'article 35 du RGPD impose au responsable de traitement de réaliser une d'analyse d'impact relative à la protection des données (AIPD) lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Il faut tenir compte de la nature, de la portée, du contexte et des finalités du traitement. Il s'agit, avant toute collecte de données, de réaliser une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Si les données collectées par une agence immobilière sur ses clients nécessiteront rarement de réaliser une AIPD, la mise en place d'une surveillance des salariés justifiera souvent une telle analyse d'impact.

Exemple de surveillance disproportionnée

Dans l'affaire décidée le 19 décembre 2024, outre le décompte des horaires de travail, la société avait paramétré le logiciel de manière à pouvoir mesurer nominativement les temps qu'elle considérait comme des temps « *d'inactivité* » des salariés. Le logiciel détectait automatiquement, tout au long de la journée, si le salarié n'effectuait aucune frappe sur le clavier ou mouvement de souris sur une durée paramétrée de 3 à 15 minutes. Ces temps « *d'inactivité* » comptabilisés, à défaut d'être justifiés par les salariés ou rattrapés, pouvaient faire l'objet d'une retenue sur salaire par la société. Or, les périodes pendant lesquelles le salarié n'utilise pas son ordinateur pouvaient également correspondre à du temps de travail effectif dans le cadre de ses missions (réunions ou appels téléphoniques par exemple).
Le logiciel permettait, sur la base d'une liste de sites web et de programmes préalablement identifiés et paramétrés par la société comme « *productifs* » ou non, de déterminer le temps passé sur des sites web jugés non productifs durant leur temps de travail. En outre, le logiciel était paramétré par la société pour effectuer des captures régulières des écrans des ordinateurs des salariés, selon une récurrence déterminée individuellement par la société entre 3 et 15 minutes. Ce dispositif, tel que paramétré, constituait une surveillance particulièrement intrusive, d'autant qu'il pouvait conduire à la captation d'éléments d'ordre privé (courriels personnels, conversations de messageries instantanées ou mots de passe confidentiels par exemple).

Délibération de la formation restreinte de la CNIL n°-SAN-2024-021 du 19 décembre 2024 concernant la société [...]

Faut-il nommer un délégué à la protection des données ?

L'article 37 du RGPD impose au responsable de traitement de nommer un délégué à la protection des données s'il réalise des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées.
La mise en place d'un système de vidéo surveillance ou de l'activité des salariés exigera souvent, en raison de la nature et de la quantité des informations collectées et des risques potentiels d'atteintes à la vie privée des salariés, la nomination d'un délégué à la protection des données.

Fiche pratique rédigée par Olivier BEDDELEEM,
Docteur en droit, Chargé d'enseignement à l'EDHEC Business School