Surveillance salariés : lois, règles & sanctions employeur

L’employeur peut au sein de son entreprise choisir de surveiller ses salariés qu’ils soient présents physiquement ou en télétravail. Pour cela, il dispose de différents moyens à sa disposition. Cependant la surveillance des salariés à des limites.

- Quels sont les outils de surveillance de l’employeur ?
- Qui contacter en cas d’abus ?
- Quelles peuvent être les sanctions ?

Toutes les explications dans cet article.

sommaire

Le cadre légal de la surveillance des salariés

La surveillance des salariés ne peut s’effectuer que dans un cadre fixé par la loi.

Un premier principe que l'employeur doit respecter est celui de l’obligation de loyauté et de transparence envers les salariés. Comme indiqué dans l’article L.1222-4 du Code du travail, il doit donc les informer de l’existence de dispositifs de contrôle mis en place.

L’article L.1121-1 du Code du travail précise également que la surveillance de l’employeur doit être non seulement en adéquation avec le but recherché, mais aussi proportionné par rapport à celui-ci.

De plus, le cybercontrôle du salarié doit observer les règles applicables à la protection des données. L'employeur doit ainsi respecter le règlement sur la protection des données personnelles (RGPD), les préconisations de la CNIL et porter une attention particulière sur la protection des données personnelles du salarié (surtout en cas de télétravail) et de celles qu'il utilise à des fins professionnelles.

Surveillance des salariés et CSE

Droits du CSE

L'article L.2312-38 du Code du travail indique que le CSE doit être informé et consulté, préalablement à leur mise en œuvre dans l'entreprise, des moyens ou techniques permettant un contrôle de l'activité des salariés.

Comment le CSE peut-il s'opposer à une surveillance illicite ?

En cas de surveillance illicite, il est possible de saisir :

- L'inspection du travail.
- Le service des plaintes de la CNIL.
- Les services de police ou de gendarmerie.

Comment le CSE peut-il se plaindre auprès de la CNIL ?

Si le CSE constate le non-respect du RGPD, il peut s'adresser à la CNIL. Afin d'effectuer cette démarche, plusieurs étapes sont à respecter.

Préparer de façon complète votre plainte

En effet, votre plainte doit :

- Être rédigée en français.
- Contenir les informations sur l'organisme visé par celle-ci (nom, numéro SIREN, coordonnées).
- Indiquer votre identité et vos coordonnées. Sauf en cas de nécessité, ces informations ne seront pas révélées à l'organisme visé par votre plainte.
- Comporter un mandat écrit si vous intervenez pour quelqu'un d'autre (collègue, salarié…).
- Présenter toutes les informations utiles sur la situation que vous rencontrez avec une copie des pièces permettant une meilleure compréhension de votre plainte. Par exemple, les échanges de courriers, votre qualité (employé, élus CSE, etc. de l'organisme).

N'envoyez surtout pas vos documents originaux. Vous devez les conserver pour un possible usage ultérieur.

Envoyer votre plainte

Il existe 2 possibilités pour faire parvenir votre plainte à la CNIL.

Par courrier à l'adresse suivante

Commission nationale de l'informatique et des libertés

Service des plaintes

3 Place de Fontenoy

TSA80715

75334 PARIS CEDEX 07

Par internet

Le service de plainte en ligne vous permet, après avoir créé votre compte, d'accéder à des formulaires propres à chaque situation (travail, téléphonie, internet…).

Par la suite, votre compte vous permettra de suivre l'évolution du traitement de votre demande et de communiquer plus facilement avec la personne en charge de votre dossier, de manière sécurisée.

À noter : Dans le cas où vous ne souhaitez pas créer de compte, vous pouvez tout de même consulter les questions-réponses dans la rubrique "Besoin d'aide" du site : https://www.cnil.fr/. Si toutefois, vous ne trouvez pas la question se rapprochant de votre situation, n'hésitez pas à contacter la CNIL.

Une fois la plainte envoyée

Lorsque la CNIL reçoit votre dossier, elle vérifie en premier lieu qu'elle est recevable et complète.

Si la réponse est positive, alors la CNIL pourra :

- Dans le cas d'une plainte concernant l'exercice de vos droits, écrire à l'organisme mis en cause afin que des mesures soient prises pour répondre à votre demande.
- Dans le cas d'un autre motif, intervenir de différentes manières en fonction de votre plainte, des manquements dénoncés et de la nature de l'organisme.

Si la réponse est négative, un courrier vous sera envoyé afin de vous en informer.

À noter : La CNIL s'engage à vous informer de l'état d'avancement de votre dossier au moins sous un délai de 3 mois suivant son dépôt et de l'issue de votre plainte.

Les voies de recours en cas de désaccord

Si vous êtes en désaccord avec l'issue de votre plainte, vous pouvez adresser un recours gracieux par courrier à l'attention de Madame la Présidente de la CNIL, sous deux mois après la date de clôture de votre dossier.

Si ce recours n'aboutit pas, vous pouvez dès lors saisir le Conseil d'État en application des règles de contentieux administratif et sous réserve de votre intérêt à agir.

Une plainte à la CNIL n'a pas valeur de dépôt de plainte. Si les faits dont vous êtes victime sont susceptibles de relever d'une infraction pénale alors vous pouvez déposer à n'importe quel moment une plainte.

La surveillance des salariés sur son lieu de travail

Une fois le CSE informé des outils de contrôle qu'il souhaite mettre en place, l'employeur dispose de plusieurs moyens différents.

Les moyens de contrôle des salariés sur leur lieu de travail

La vidéosurveillance

L'utilisation de vidéosurveillance sur les lieux de travail est légale si elle est justifiée par l'intérêt de l'entreprise et proportionnée au but recherché. Elle peut être effective après consultation du CSE. Elle peut également nécessiter l'accord du préfet si le lieu de travail est ouvert au public.

Elle répond cependant à certaines règles, ainsi, les caméras ne peuvent pas filmer :

- Les locaux syndicaux ou du CSE, ni leur accès s'il ne mène qu'à eux.
- Les zones de pause, de repos et les toilettes.
- Les employés sur leur poste de travail (sauf exception : employé manipulant de l'argent, entrepôt stockant des biens de valeur).

La consultation du CSE n’est pas obligatoire dans le cas où les locaux ne sont pas affectés au travail.

La géolocalisation

Le recours à la géolocalisation ne se justifie que dans certaines situations :

- La lutte contre le vol d’un véhicule.
- La vérification des règles d'utilisation d’un véhicule.
- Le suivi du temps de travail d’un salarié à condition qu’il ne puisse être réalisé d’une autre façon.
- La justification d’une prestation auprès d’un donneur d’ordre ou d’un client.
- Une optimisation des moyens lorsque les prestations fournies sont accomplies dans des lieux différents (chauffeurs de taxi, etc.).
- La sécurité du salarié, du véhicule ou des marchandises.
- Le suivi et la facturation de prestations de personnes, de marchandises ou de services liées à l’utilisation directe du véhicule (livraison, ramassage scolaire, etc.).

Afin de pouvoir utiliser ce dispositif dans les véhicules mis à disposition des salariés, l’employeur doit effectuer une déclaration en ligne à la CNIL et en informer au préalable les salariés en leur spécifiant ses finalités. Dès lors, toute autre utilisation est interdite (Cass. soc. 3-11-2011 n° 10-18.03).

La CNIL interdit également la collecte et le traitement de données de localisation en dehors du temps de travail, y compris pendant le trajet domicile-travail ou pendant le temps de pause. Il doit donc être possible pour le salarié de désactiver le système de géolocalisation sur ces périodes.

De par ses conditions, ce dispositif ne peut se justifier pour les professions disposant de liberté dans l'organisation de leurs déplacements (VRP, visiteurs médicaux, etc.) ou pour ceux effectuant des déplacements dans le cadre de mandat syndical ou électif.

À noter : Les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés ont fait l’objet d’une délibération CNIL (Délibération Cnil 2015-165 du 4-6-2015 art. 3 et 5 : JO 17).

Le traçage informatique

L’employeur peut contrôler les traces informatiques (consultation de comptes bancaires, historique des sites consultés, favoris du navigateur, etc.) sans autorisation et même en l’absence du salarié.

Ces traces ne constituant pas un dispositif de surveillance, elles ne nécessitent donc pas d’information préalable.

Un disque dur ne peut être utilisé comme élément de preuve en justice, car il peut être manipulé, sauf dans le cas où il a été mis sous scellés entre la date des faits et celle de l’audience.

Dans le cas contraire, un licenciement ayant cette preuve comme motif sera considéré comme sans cause réelle et sérieuse.

Cependant, s’il utilise un outil de traçabilité de l’activité informatique des salariés, il est obligé d’en informer au préalable la CNIL, les salariés et le CSE.

La lecture des courriers et emails adressés aux salariés

Un employeur ne peut pas ouvrir un courrier destiné à un salarié s’il est indiqué que celui-ci est personnel. Pour cela, il doit comporter la mention « personnel » ou « confidentiel ».

Cependant, en l’absence de cette indication, l’ouverture est légale, mais l'employeur ne peut se baser sur son contenu pour prononcer une sanction disciplinaire.

Il est possible pour l'employeur d'inscrire une clause dans le règlement intérieur interdisant aux salariés de se faire adresser du courrier personnel sur le lieu de travail.

Il lui est également possible de limiter l'usage privé des réseaux et matériels informatiques. Il peut ainsi, par exemple, décompter les courriers d'un salarié présentés comme personnels et le sanctionner si leur nombre est trop important.

Les règles applicables aux e-mails sont identiques avec cependant quelques aménagements :

- Si un e-mail personnel d'un salarié est envoyé à l'employeur par le destinataire de celui-ci, il peut en prendre connaissance et si son contenu se révèle fautif (injures, menaces, etc.) sanctionner le salarié sur la base de l'e-mail.
- Pour être considéré comme personnel, l'e-mail doit comporter la mention « personnel et confidentiel » ou être rangé dans un répertoire intitulé « personnel ».
- Si l'employeur soupçonne une concurrence déloyale, il peut obtenir en justice, la nomination d'un commissaire de justice qui pourra ouvrir les messages personnels du salarié en présence de celui-ci.

Les écoutes téléphoniques

L'employeur a le droit de contrôler l'usage du téléphone ou la qualité des réponses données par ce moyen dans le cadre de son travail. Pour cela, il doit répondre à certaines conditions, dont l'information du salarié.

Il peut utiliser un commutateur pour quantifier l'importance des appels téléphoniques privés. En effet, cet usage est toléré dès lors qu'il n'est pas abusif.

L'employeur peut par l'intermédiaire de relevés de communication fournis par l'opérateur vérifier la durée, le coût et les numéros de téléphone passés à partir de chaque poste de travail, édités par l'autocommutateur téléphonique de l'entreprise. Cette vérification est légale même si elle n'a pas été portée à la connaissance du salarié.

L'écoute et l'enregistrement des communications peuvent être justifiés dans plusieurs cas dont la gestion des réclamations clients, le contrôle qualité…

Ces moyens peuvent constituer des preuves licites s'ils respectent plusieurs conditions : la consultation du CSE, l'information des salariés, la déclaration à la CNIL.

La ligne téléphonique des membres du CSE ou des délégués syndicaux ne peut pas faire l'objet d'écoutes téléphoniques.

Les connexions internet du salarié

En cas d'usage abusif du réseau internet, le salarié peut être licencié pour faute.

Les réseaux sociaux du salarié

Lorsque les informations diffusées sur les réseaux sociaux sont à destination d'un nombre restreint de personnes autorisées, alors l'employeur ne peut y accéder sans porter atteinte à la vie privée du salarié. De fait, il ne pourra utiliser ces éléments dans le cadre d'un licenciement par exemple.

Cependant, il existe des subtilités que nous avons détaillées dans notre article dédié : Réseaux sociaux en entreprise : règles & loi à respecter.

Les fichiers enregistrés sur l'ordinateur du salarié

Les fichiers professionnels appartenant à l'entreprise, l'employeur peut les consulter à tout moment même si le salarié n'est pas présent. D'autant plus, s'ils sont nécessaires au bon fonctionnement de l'entreprise.

À noter : Si les fichiers sont identifiés comme personnels. Ils ne pourront être ouverts qu'à 2 conditions :

- Le contrôle est justifié et proportionné au but recherché (exemples : sécurité du réseau informatique, détournement d'informations confidentielles) (Cass. soc., 17 mai 2005, n° 03-40.017).
- Le salarié est présent lors de l'ouverture du fichier sauf en cas de risque ou d'évènement particulier, par exemple un virus informatique.

La fouille des sacs, casiers et armoires individuels

En cas d'absence de circonstance particulière, le salarié peut s'opposer à toute fouille.

Les conditions préalables à la fouille sont :

- Le motif légitime (sécurité ou hygiène par exemple).
- L'information préalable du salarié de l'ouverture de son casier ou de son armoire.
- La présence du salarié sauf par exception si le salarié a été prévenu en avance.

L'ouverture des sacs peut être exigée dans certains cas. En dehors de circonstances exceptionnelles (alerte à la bombe…), le salarié doit donner son accord et avoir été averti auparavant de son droit de s'y opposer et d'exiger la présence d'un témoin.

Dans certaines entreprises, l'ouverture des sacs ou les fouilles corporelles peuvent être systématiques en cas de circonstances particulières (risques de vol, disparition de matériels ou de produits…). Dans ce cas, le consentement du salarié doit être recueilli de préférence devant témoin (représentant du personnel ou autre salarié). En cas de refus, l'employeur peut faire appel à un officier de police.

Les tests d'alcoolémie

Dans le cas où le règlement intérieur le prévoit, l'employeur peut faire subir un alcootest à ses salariés (Cass, soc, 31 mars 2015, n°13-25436, société Autoroute Paris Rhin Rhône).

Cependant, sa contestation est possible et il doit être réservé aux salariés dont la nature du travail (manipulation de produits dangereux, conducteurs…) peut exposer les personnes ou les biens à un danger.

L’admission de preuves illicites au nom du droit à la preuve de l’employeur et du salarié

La Cour de cassation a considéré que le droit à la preuve de l’employeur peut justifier de produire en justice des éléments de preuves illicites (obtenues en absence d’information préalable des salariés sur la finalité du dispositif). Si et seulement si ces éléments sont indispensables à l’exercice de ce droit et que l’atteinte à la vie privée du salarié soit proportionnée au but poursuivi.

Dans ce cas, le juge doit apprécier si l’utilisation de cette preuve illicite porte atteinte au caractère équitable de la procédure (Cass. Soc. 10 novembre 2021, n°20-12.263 ; voir également Cass. Soc. 25 novembre 2020, n°17-19.523).

La surveillance du salarié en télétravail

Le télétravail est un mode d’organisation du contrat de travail, de fait, l’employeur possède toujours sur le salarié son pouvoir de direction, de contrôle et de sanction.

Les outils de surveillance des salariés en télétravail

Il existe plusieurs moyens pour l’employeur pour suivre le temps de travail et l’activité d’un employé en télétravail :

- La mise en place de compte rendu régulier, quotidiens ou hebdomadaires, par téléphone ou par mail.
- Le suivi par un logiciel auto déclaratif de suivi du temps rempli par le salarié ou d’un logiciel de badge-age.

À côté de ces moyens, se sont développés des systèmes de contrôle plus intrusifs. Ils permettent non seulement d’identifier le salarié et son temps de travail, mais également d’analyser la qualité et la productivité du travail fourni.

Il peut s’agir de dispositifs de :

- Suivi de la boîte mail.
- Écoutes téléphoniques.
- Vidéosurveillance.
- Traçage informatique.
- Logiciels espions appelés aussi keylogger et permettant d’enregistrer la totalité des actions du salarié.

Les droits en matière de protection de la vie privée spécifiques au télétravail

Les droits en matière de protection de la vie privée spécifiques au télétravail sont définis par différentes institutions.

L’Accord National Interprofessionnel

L’Accord National Interprofessionnel (ANI) du 26 novembre 2020 définit dans son article 3 que « Les dispositions légales et conventionnelles applicables aux relations de travail s’appliquent aux salariés en télétravail. Ces derniers ont les mêmes droits légaux et conventionnels que le salarié qui exécute son travail dans les locaux de l’entreprise. »

Il précise également que l’employeur doit s’assurer du respect du droit à la déconnexion du salarié. Ce droit doit lui aussi faire l’objet d’un accord ou d’une charte définissant ses modalités de mise en œuvre.

Le Comité européen de la protection des données (CEPD) - CNIL

De plus, la CNIL exclut les procédés de surveillance invasifs et imposant une surveillance permanente et disproportionnée des activités du salarié.

Elle indique de fait que ne doivent pas être utilisés :

- L'utilisation de keylogger.
- Le partage d'écran permanent.
- La surveillance constante du salarié au travers de dispositifs audio et/ou vidéo.
- L'obligation pour le salarié d'effectuer des actions régulières pour prouver sa présence derrière l'écran.

En revanche, elle préconise la mise en place de :

- Contrôle de la réalisation par objectifs pour une période donnée.
- Compte rendu régulier du salarié.
- Floutage de l'arrière-plan lors des visioconférences depuis le domicile du salarié afin de ne pas l'obliger à révéler plus d'informations personnelles que lors d'une réunion sur le lieu de travail.

L'employeur ne peut pas imposer systématiquement l'activation de la caméra lorsqu'il n'est pas possible de recourir au floutage. Cependant, la CNIL indique que l'activation de la caméra peut être exigée dans certains cas (rendez-vous client, entretien RH, etc.) à condition que le salarié en soit informé en amont afin qu'il puisse s'organiser préalablement.

Le Code du travail

L'article L.1222-9 du Code du travail précise également que le fait que le salarié soit en télétravail n'autorise pas l'employeur à le contacter à n'importe quelle heure. Ainsi, l'accord ou la charte d'entreprise doit fixer les plages horaires durant lesquelles le télétravailleur peut être contacté (surtout pour ceux relevant d'un forfait annuel en jours).

Cette détermination doit se faire en concertation entre l'employeur et le salarié en cohérence avec les horaires en vigueur dans l'entreprise et en respectant le droit du travail.

Que risque l'employeur en cas de surveillance abusive ?

En cas de violation du RGPD et notamment en cas de surveillance abusive, la CNIL peut prononcer des sanctions à l'encontre de l'employeur. Celles-ci peuvent aller du simple rappel à l'ordre jusqu'à des amendes administratives d'un montant maximal de 10 M€ ou 2 % du chiffre d'affaires annuel mondial de l'entreprise lors de l'exercice précédent.

Tout comme l'employeur, le CSE est concerné par la protection des données personnelles et peut de fait être sanctionné.

Pour en savoir plus, consultez notre article dédié : Protection des Données Personnelles du CSE (RGPD) Guide.

Des poursuites pénales sont également possibles en cas de contrôle excessif du salarié en télétravail. Ainsi l'article 226-1 du Code pénal indique que l'employeur peut encourir une peine d'un an d'emprisonnement et 45 000 euros d'amende en cas d'utilisation d'un procédé permettant de capter, d'enregistrer ou de transmettre, sans consentement de leur auteur, des paroles prononcées à titre privé ou confidentielles, des images d'une personne se trouvant dans un lieu privé ou encore sa localisation présente ou passée.

De plus, l'article 226-16 du Code pénal ajoute que la mise en place d'un système automatique de traitement des données personnelles ne respectant pas le RGPD peut être punie de 5 ans d'emprisonnement et de 300 000 € d'amende.

En cas de licenciement dont la cause découle d’un contrôle abusif, le salarié pourra le faire requalifier et obtenir des dommages et intérêts (Cass. soc., 1er juin 2017, n° 15-23522 – Cass. soc., 8 oct. 2014, n° 13-14991).

Les outils a disposition de l'employeur en matière de surveillance de ses employés sont donc extrêmement variés. Il est de fait nécessaire de bien en connaître les usages et les limites afin de pouvoir pour vous, élus, protéger au mieux les intérêts du salarié.