Travail &
Données personnelles

Le recrutement et la gestion du personnel

Dans le cadre de la gestion du recrutement, de la paie ou des carrières, employeurs et recruteurs ont fréquemment recours aux moyens informatiques. Ces outils contiennent de nombreuses informations concernant les candidats ou les employés. Quelles informations peuvent être utilisées ? Dans quel cadre les utiliser ? Combien de temps les conserver ? Quel type de traitement est interdit ?

Quelles informations ? Pour quoi faire ?

Dans le cadre d'un recrutement, les données collectées ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé (qualification, expérience, etc.). **Il est interdit de demander à un candidat à un emploi son numéro de sécurité sociale. Il est également interdit de collecter des informations sur ses parents, sa fratrie, ses opinions politiques ou son appartenance syndicale.**

À l'embauche du candidat, l'employeur pourra collecter des informations complémentaires. Outre celles nécessaires au respect d'une obligation légale (exemple : déclarations sociales obligatoires), l'employeur peut collecter des informations utiles :

- **à la gestion administrative du personnel** (par exemple, type de permis de conduire détenu ou coordonnées de personnes à prévenir en cas d'urgence),
- **à l'organisation du travail** (par exemple, photographie facultative de l'employé pour les annuaires internes et organigrammes),
- **à l'action sociale** prise en charge par l'employeur (par exemple, les informations concernant les ayants-droit de l'employé).

> Les « zones commentaires » qui enregistrent des appréciations d'un employeur sur ses employés ne doivent comporter que des éléments pertinents et non excessifs. Les employés ont le droit d'y accéder.

Qui peut avoir accès aux données ?

Un accès limité

Seules les personnes intervenant dans le processus de recrutement peuvent accéder aux informations d'un candidat. Outre les administrations informées de l'embauche (exemple : assurance chômage, maladie, retraite, mutuelle...), seules les personnes chargées de la gestion du personnel peuvent consulter les informations des employés. Les supérieurs hiérarchiques peuvent accéder aux informations nécessaires à l'exercice de leurs fonctions (exemple : données d'évaluations, rémunération...).

> L'employeur ne peut révéler les coordonnées personnelles d'un employé que si la loi ou une décision de justice le prévoit (ex. : médecin contrôleur de la sécurité sociale, huissier disposant d'un titre exécutoire...).

Les délégués du personnel ont accès aux données figurant dans le registre unique du personnel (nom, nationalité, fonction occupée, date d'entrée dans l'organisme, etc.). Les autres instances (Comité d'entreprise, délégués syndicaux) peuvent obtenir certaines informations pour exercer leurs missions. Par exemple, l'employeur peut transmettre au Comité d'entreprise (CE), après information des employés, des données sur ceux qui ne s'y sont pas opposés. Ces informations permettront au CE de proposer des activités et des prestations adaptées.

Le recrutement et la gestion du personnel

Les organisations syndicales peuvent, après accord avec l'employeur, adresser aux employés des messages d'information syndicale par courrier électronique. Les employés peuvent s'y opposer à tout moment.

Un accès contrôlé

L'employeur doit assurer la sécurité des informations et garantir que seules les personnes habilitées en prennent connaissance. Les actions sur les données effectuées par les personnes habilitées doivent être enregistrées (savoir qui se connecte à quoi, quand et pour faire quoi).

Quelles garanties pour la vie privée ?

Le droit d'être informé

L'employeur doit informer les instances représentatives du personnel avant d'utiliser des techniques d'aide au recrutement ou des fichiers de gestion du personnel. Candidats comme employés doivent être informés :

- **de l'identité du responsable du fichier** (cabinet de recrutement ou service des ressources humaines),
- **de l'objectif poursuivi** (gestion des candidatures ou gestion du personnel),
- **de la base légale du dispositif** (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- **du caractère obligatoire ou facultatif des réponses** ainsi que des conséquences à leur égard d'un défaut de réponse,
- **des destinataires des informations** (autres cabinets de recrutements, par exemple),
- **de la durée de conservation des données**,
- **des conditions d'exercice de leurs droits** d'opposition (pour motif légitime), d'accès et de rectification,
- **de la possibilité d'introduire une réclamation** auprès de la CNIL.

Aucune information concernant un employé ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance.

Le droit d'accès d'un candidat à un emploi et d'un employé

Sur simple demande et sans avoir à la motiver, un candidat ou un employé peut obtenir une copie des données qui le concernent (recrutement, historique de carrière, rémunération, évaluation des compétences, dossier disciplinaire…).

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.

Les valeurs de classement annuel ou de potentiel de carrière sont communicables lorsqu'elles ont servi à prendre une décision. L'employeur n'est pas tenu de les communiquer lorsqu'elles sont encore prévisionnelles.

Une durée de conservation limitée

En cas d'issue négative à une candidature, le recruteur devra informer le candidat qu'il souhaite conserver son dossier, afin de lui laisser la possibilité d'en demander la destruction.

Si un candidat ne demande pas la destruction de son dossier, les données sont automatiquement détruites 2 ans après le dernier contact. Seul l'accord formel du candidat permet une conservation plus longue.

Les données relatives à un employé sont conservées le temps de sa présence dans l'organisme.

Une fois l'employé parti, certaines informations doivent être conservées par l'employeur sur un support d'archive (par exemple, 5 ans après le départ du salarié pour les bulletins de paie).

Quelle formalité ?

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en oeuvre de tous ces fichiers.

Les différents fichiers de recrutement ou de gestion du personnel doivent être inscrits au registre des activités de traitement tenu par l'employeur.

Quels recours ?

En cas de difficulté, vous pouvez saisir :

- **le service des plaintes de la CNIL,** en cas de difficultés pour accéder à votre dossier personnel, de collecte excessive ou de défaut de sécurisation des données,
- **les services de l'inspection du Travail,**
- **le procureur de la République.**

Les textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L1121-1 (droits et libertés dans l'entreprise)
  Article L1222-3 et L1222-4 (information des employés)
  Article L2323-47 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Travail &
Données personnelles

La géolocalisation des véhicules

Parce qu'ils coûtent peu cher et peuvent s'avérer très utiles, les dispositifs de géolocalisation sont fréquents dans le monde du travail. Attention toutefois, de nombreuses règles encadrent l'utilisation de ces outils afin que la vie privée des employés soit respectée.

Dans quels buts ?

Des dispositifs de géolocalisation peuvent être installés dans des véhicules utilisés par des employés pour :

- **Suivre, justifier et facturer une prestation de transport de personnes,** de marchandises ou de services directement liée à l'utilisation du véhicule. Par exemple : les ambulances dans le cadre de la dématérialisation de la facturation de l'assurance maladie.
- **Assurer la sécurité de l'employé, des marchandises ou des véhicules dont il a la charge,** et notamment retrouver le véhicule en cas de vol (par exemple, avec un dispositif inerte activable à distance à compter du signalement du vol).
- **Mieux allouer des moyens pour des prestations à accomplir en des lieux dispersés,** notamment pour des interventions d'urgence. Par exemple : identifier l'employé le plus proche d'une panne d'ascenseur ou l'ambulance la plus proche d'un accident.
- **Accessoirement, suivre le temps de travail,** lorsque cela ne peut être réalisé par un autre moyen.
- **Respecter une obligation légale ou réglementaire** imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés.
- **Contrôler le respect des règles** d'utilisation du véhicule définies par l'employeur.

À savoir

Les kilomètres parcourus pendant une période durant laquelle le véhicule ne doit pas être utilisé sont suffisants pour caractériser un abus et sa gravité, sans qu'il soit nécessaire de connaitre le trajet effectué.

Les utilisations à exclure

Un dispositif de géolocalisation installé dans un véhicule mis à la disposition d'un employé ne peut pas être utilisé :

- **Pour contrôler le respect des limitations de vitesse.**
- **Pour contrôler un employé en permanence.**
- **En particulier,** il ne peut pas être utilisé :

- Dans le véhicule d'un employé disposant d'une liberté dans l'organisation de ses déplacements (par exemple : VRP).

- Pour suivre les déplacements des représentants du personnel dans le cadre de leur mandat.
- Pour collecter la localisation en dehors du temps de travail (trajet domicile travail, temps de pause,etc.), y compris pour lutter contre le vol ou vérifier le respect des conditions d'utilisation du véhicule.

- **Pour calculer le temps de travail** des employés alors qu'un autre dispositif existe déjà.

Quelles garanties pour la vie privée ?

Les droits des employés

Les employés peuvent s'opposer à l'installation d'un dispositif de géolocalisation dans leur véhicule professionnel, dès lors que ce dispositif ne respecte pas les conditions légales posées par la CNIL ou d'autres textes. Les employés doivent être informés de l'installation de ce dispositif. Ils doivent avoir accès aux données les concernant enregistrées par l'outil (dates et heures de circulation, trajets effectués, etc). Les employés doivent pouvoir désactiver la collecte ou la transmission de la localisation géographique en dehors du temps de travail.

À savoir

L'employeur peut contrôler le nombre ou la durée des désactivations et, le cas échéant, demander des explications au conducteur et sanctionner les éventuels abus.

La géolocalisation des véhicules

Des destinataires précis

L'accès aux informations du dispositif de géolocalisation doit être limité au personnel habilité des services concernés, à l'employeur et au personnel habilité d'un client ou donneur d'ordre auprès duquel une prestation est justifiée.

Attention : le nom du conducteur ne doit pas être communiqué à un client ou à un donneur d'ordre, puisque cette information ne présente pas d'intérêt pour ces personnes, sauf si cette information présente un intérêt particulier et indispensable.

Ce qu'il ne faut pas faire !

Un salarié d'une société souhaitait obtenir de son employeur les relevés du dispositif de géolocalisation installé dans son véhicule à la suite d'un accident de la circulation. La société refusait que les salariés obtiennent une copie de ces documents. Saisie d'une plainte par le salarié, et après plusieurs courriers restés sans réponse, la société a été mise en demeure de fournir au salarié la copie de ses données. Faute de réponse satisfaisante de l'employeur, la CNIL a prononcé une sanction de 10 000 euros à son encontre.

La sécurité

Pour éviter notamment que des personnes non autorisées accèdent aux informations du dispositif, il est impératif de prendre des mesures de sécurité. Par exemple, l'accès au dispositif de suivi en temps réel sur un site internet doit se faire avec un identifiant et un mot de passe.

Il faut également impérativement prévoir :

- une politique d'habilitation,
- une sécurisation des échanges,
- une journalisation des accès aux données et des opérations effectuées.

Une étude des risques sur la sécurité des données est également souhaitable afin de définir les mesures les mieux adaptées.

À noter

Les outils ou logiciels développés par des prestataires restent sous la responsabilité de l'employeur qui doit vérifier que ces outils ou logiciels respectent les obligations légales, en particulier les mesures de sécurité (clause contractuelle sur les obligations du sous-traitant en matière de sécurité et de confidentialité des données).

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.

Une durée de conservation limitée

En principe, les informations obtenues par la géolocalisation ne doivent pas être conservées plus de **deux mois**. Toutefois, elles peuvent être conservées **un an** lorsqu'elles sont utilisées pour optimiser les tournées ou à des fins de preuve des interventions effectuées, lorsqu'il n'est pas possible de rapporter cette preuve par un autre moyen. Enfin, elles peuvent être conservées **cinq ans** lorsqu'elles sont utilisées pour le suivi du temps de travail.

L'information des employés

Les instances représentatives du personnel doivent être informées ou consultées avant toute décision d'installer un dispositif de géolocalisation dans les véhicules mis à la disposition des employés.

Chaque employé doit être par ailleurs informé :

- de l'identité du responsable de traitement
- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données issues du dispositif de géolocalisation,
- de son droit d'opposition pour motif légitime,
- de la durée de conservation des données,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'un avenant au contrat de travail ou d'une note de service, par exemple.

Quelle formalité

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre du dispositif.
Le système de géolocalisation doit être inscrit au registre des activités de traitement tenu par l'employeur.

Quels recours ?

Si un dispositif de géolocalisation ne respecte pas ces règles, vous pouvez saisir :

- Le service des plaintes de la CNIL
- Les services de l'inspection du Travail
- Le procureur de la République

Textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-47 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Travail &
Données personnelles

Les outils informatiques au travail

L'utilisation des outils informatiques s'est largement développée dans le monde du travail. 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.

Le contrôle de l'utilisation d'Internet et de la messagerie : dans quel but ?

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 »...)

Ce contrôle a pour objectif :

1. D'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie...)
2. 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...).

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.

À noter

Les marque-pages, « favoris » ou « bookmark » du navigateur ne constituent pas un espace personnel ou privé. Ajouter un site internet à ses « favoris » ne limite donc pas le pouvoir de contrôle de l'employeur.

Quelles garanties pour la vie privée ?

Les limites au contrôle de l'employeur

- l'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, c'est excessif,
- les « keyloggers » permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur. Sauf circonstance exceptionnelle liée à un fort impératif de sécurité, ce mode de surveillance est illicite,
- les logs de connexion ne doivent pas être conservés plus de 6 mois.

- **La protection des courriels personnels :**

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.

Un employeur 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.

Pour qu'ils soient protégés, les messages personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet « Personnel » ou « Privé »,
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé.

Cette protection n'existe plus si une enquête judiciaire est en cours (par exemple, si l'employé est accusé de vol de secrets de l'entreprise) ou si l'employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages.

En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'employeur à la messagerie. L'employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance des messages de l'employé.

- **Les fichiers**

Par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement.

Lorsque les fichiers sont identifiés comme personnels, l'employeur peut y accéder :

- en présence de l'employé ou après l'avoir appelé,
- en cas de risque ou évènement particulier, qu'il appartient aux juridictions d'apprécier.

- **La communication des mots de passe**

Les identifiants et mots de passe (session Windows, messagerie…) sont confidentiels et ne doivent pas être transmis à l'employeur. Toutefois, si un employé absent détient sur son poste des informations indispensables à la poursuite de l'activité, son employeur peut exiger la communication de ses codes si l'administrateur réseau n'est pas en mesure de fournir l'accès au poste.

L'information des employés

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité.

Chaque employé doit être notamment informé :

- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'une charte, annexée ou non au règlement intérieur, d'une note individuelle ou d'une note de service…

Quelle formalité

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en oeuvre des dispositifs de contrôle.

Les différents systèmes de contrôle des outils informatiques doivent être inscrits au registre des activités de traitement tenu par l'employeur.

Quels recours ?

En cas de difficulté, vous pouvez saisir :

- les services de l'inspection du Travail,
- le procureur de la République,
- le service des plaintes de la CNIL, sur les modalités de mise en œuvre d'un dispositif de contrôle de l'activité.

Textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-47 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.

Travail &
Données personnelles

L'accès aux locaux et le contrôle des horaires

Parce que les locaux professionnels ne sont pas ouverts à tous et que les employeurs comme les employés ont besoin de connaître les horaires effectués, les contrôles d'accès et du temps de travail existent depuis bien longtemps. Le développement des technologies facilite ces contrôles mais permet aussi de collecter bien plus d'informations sur les personnes concernées. Des limites à leur utilisation sont donc indispensables pour préserver les droits et libertés de chacun.

Dans quel but ?

L'employeur peut mettre en place des outils – y compris biométriques – de contrôle individuel de l'accès pour sécuriser :

- l'entrée dans les bâtiments,
- les locaux faisant l'objet d'une restriction de circulation.

Ces dispositifs peuvent concerner les employés comme les visiteurs.

Des dispositifs non biométriques peuvent également être utilisés pour gérer les horaires et le temps de présence des employés.

Quelles garanties pour la vie privée ?

Le système mis en place ne doit pas servir au contrôle des déplacements à l'intérieur des locaux.

Le dispositif ne doit pas entraver la liberté d'aller et venir des représentants du personnel dans l'exercice de leur mandat, ou être utilisé pour contrôler le respect de leurs heures de délégation.

Qui peut accéder aux données ?

Les informations ne sont accessibles qu'aux membres habilités des services gérant le personnel, la paie, ou la sécurité.

L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et éviter que des personnes qui n'ont pas qualité pour y accéder puissent en prendre connaissance. Ainsi, il doit prévoir des habilitations pour les accès informatiques avec une traçabilité des actions effectuées (savoir qui se connecte à quoi, quand et pour quoi faire).

Quelle durée de conservation ?

- Les données relatives aux accès doivent être supprimées **3 mois après leur enregistrement.**
- Les données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences, **doivent être conservées pendant 5 ans.**

L'information des salariés

Les instances représentatives du personnel doivent être informées ou consultées avant toute décision d'installer un dispositif de contrôle des horaires ou d'accès aux locaux.

Chaque employé doit être notamment informé :
- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données issues du dispositif,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'un avenant au contrat de travail ou d'une note de service, par exemple.

L'accès aux locaux et le contrôle des horaires

Quelles sécurités ?

Pour éviter notamment que des personnes non autorisées accèdent aux données du dispositif, il est impératif de prendre des mesures de sécurité. Par exemple, l'accès au logiciel de gestion du contrôle d'accès ou des horaires doit être limité aux personnes qui ont besoin d'en connaître et se faire avec un identifiant et un mot de passe.

Il faut également impérativement prévoir :

- une politique d'habilitation,
- une sécurisation des échanges,
- une journalisation des accès aux données et des opérations, effectuées.

Une étude des risques sur la sécurité des données est également souhaitable afin de définir les mesures les mieux adaptées, notamment lorsqu'un dispositif biométrique est mis en place.

Quelles formalités ?

Les dispositifs sans biométrie

Le contrôle d'accès sans biométrie est à privilégier, dès lors qu'un système de badge est suffisant ou que les locaux ne sont pas particulièrement sensibles.

Attention, la CNIL estime que la biométrie est un moyen disproportionné de contrôle des horaires des employés.

Les dispositifs avec biométrie

Le contrôle d'accès biométrique doit faire l'objet d'une analyse d'impact sur la protection des données (PIA). Cette démarche permet d'identifier les risques associés aux données personnelles concernées par le dispositif, et à en réduire soit la vraisemblance soit la gravité.

L'aide du fournisseur, de l'intégrateur ou de l'installateur du dispositif peut être utile.

Dans ces situations, l'employeur doit privilégier le stockage du gabarit biométrique de l'employé sur un support individuel.

Si l'organisme a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre de ce dispositif.
L'employeur doit inscrire ce dispositif de contrôle dans son registre des activités de traitement de données.

Quels recours ?

En cas de difficulté, vous pouvez saisir :

- le service des plaintes de la CNIL,
- l'inspection du Travail,
- le procureur de la République.

Textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-32 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Voir aussi

- Le contrôle d'accès biométrique sur les lieux de travail.
- L'analyse d'impact relative à la protection des données
- Guide de la sécurité des données personnelles

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.

Travail &
Données personnelles

La vidéosurveillance-vidéoprotection au travail

L'équipement des lieux de travail en caméra de surveillance est désormais largement partagé. S'ils sont légitimes pour assurer la sécurité des biens et des personnes, de tels outils ne peuvent pas conduire à placer les employés sous surveillance constante et permanente. Quelles règles les employeurs doivent-ils respecter ? Quels sont les droits des employés ?

Dans quel but ?

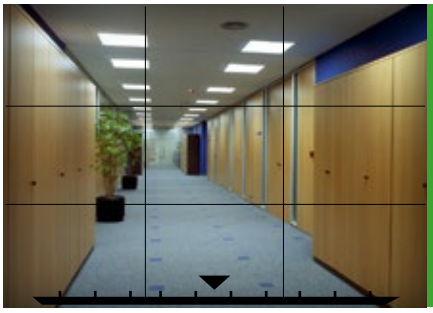
Un employeur ne peut pas installer des caméras dans ses locaux sans définir un objectif, qui doit être légal et légitime. Par exemple, des caméras peuvent être installées sur un lieu de travail à des fins de sécurité des biens et des personnes, à titre dissuasif ou pour identifier les auteurs de vols, de dégradations ou d'agressions.

Quelles précautions prendre lors de l'installation du dispositif ?

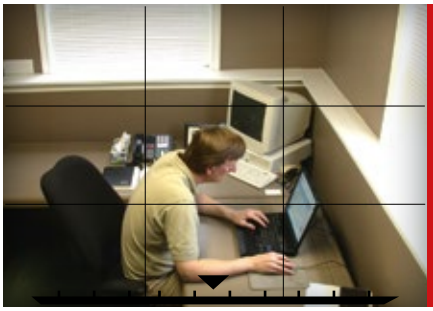
Les caméras peuvent être installées au niveau des **entrées et sorties des bâtiments**, des **issues de secours** et des **voies de circulation**. Elles peuvent aussi filmer les zones où de la marchandise ou des biens de valeur sont entreposés.
Elles ne doivent **pas filmer les employés sur leur poste de travail**, sauf circonstances particulières (employé manipulant de l'argent par exemple, mais la caméra doit davantage filmer la caisse que le caissier ; entrepôt stockant des biens de valeurs au sein duquel travaillent des manutentionnaires).
En effet, sur le lieu de travail comme ailleurs, les employés ont **droit au respect de leur vie privée**.
Les caméras ne doivent **pas non plus filmer les zones de pause ou de repos des employés, ni les toilettes**. Si des dégradations sont commises sur les distributeurs alimentaires par exemple, les caméras ne doivent filmer que les distributeurs et pas toute la pièce.
Enfin, elles ne doivent pas **filmer les locaux syndicaux** ou des représentants du personnel, ni leur accès lorsqu'il ne mène qu'à ces seuls locaux.
Si les images sont accessibles à distance, depuis internet sur son téléphone mobile par exemple, il faut sécuriser cet accès.

Qui peut consulter les images ?

Seules les personnes habilitées par l'employeur, dans le cadre de leurs fonctions, peuvent visionner les images enregistrées (par exemple : le responsable de la sécurité de l'organisme). Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéosurveillance.



Oui,
on peut installer des caméras dans un couloir à des fins de sécurité.



Non,
il est interdit de surveiller ainsi ses employés.

L'accès aux images doit être sécurisé pour éviter que tout le monde ne puisse les visionner.

Pendant combien de temps conserver les images ?

L'employeur doit définir la durée de conservation des images issues des caméras.
Cette durée doit être en lien avec l'objectif poursuivi par les caméras. En règle générale, conserver les images quelques jours suffit, sauf circonstances exceptionnelles à effectuer les vérifications nécessaires en cas d'incident et permet d'enclencher d'éventuelles procédures disciplinaires ou pénales. Si de telles procédures sont engagées, les images sont alors extraites du dispositif (après consignation de cette opération dans un cahier spécifique) et conservées pour la durée de la procédure.
La durée maximale de conservation des images ne doit pas être fixée en fonction de la seule capacité technique de stockage de l'enregistreur.

La vidéosurveillance-vidéoprotection au travail

Quelles formalités ?

Les formalités à accomplir peuvent varier en fonction des lieux qui sont filmés.

Lieu non ouvert au public

Si les caméras filment un lieu non ouvert au public (lieux de stockage, réserves, zones dédiées au personnel comme le fournil d'une boulangerie), aucune formalité auprès de la CNIL n'est nécessaire.
Si l'organisme qui a mis en place des caméras a désigné un Délégué à la protection des données (DPO), ce dernier doit être associé à la mise en oeuvre des caméras. Si le dispositif doit faire l'objet d'une analyse d'impact (AIPD), le DPO doit y être associé.
L'employeur doit inscrire ce dispositif de vidéosurveillance dans le registre des traitements de données qu'il doit tenir.

Lieu ouvert au public

Si les caméras filment un lieu ouvert au public (espaces d'entrée et de sortie du public, zones marchandes, comptoirs, caisses), le dispositif doit être autorisé par le préfet du département (le préfet de police à Paris). Le formulaire peut être retiré auprès des services de la préfecture du département ou téléchargé sur le site du ministère de l'Intérieur. Il peut également être rempli en ligne sur le site : https://www.televideoprotection.interieur.gouv.fr.

Auprès des instances représentatives du personnel

Les instances représentatives du personnel doivent être informées et consultées avant toute décision d'installer des caméras.

Quels recours ?

Si un dispositif de vidéosurveillance ne respecte pas ces règles, vous pouvez saisir :

- le service des plaintes de la Commission nationale de l'informatique et des libertés. La CNIL peut contrôler tous les dispositifs installés sur le territoire national, qu'ils filment les lieux fermés ou ouverts au public,
- les services de l'Inspection du Travail,
- les services de la préfecture, si les caméras filment des lieux ouverts au public,
- les services de police ou de gendarmerie,
- le procureur de la République.

La CNIL surveille les employeurs qui abusent

La CNIL a reçu une plainte d'un salarié concernant des caméras installées sur son lieu de travail.
Il indiquait que ce dispositif permettait au responsable de surveiller les salariés et d'écouter leurs conversations. Un contrôle a permis de confirmer ces faits.
Celui-ci comportait 8 caméras, (chacune équipée d'un microphone permettant l'écoute sonore et d'un haut-parleur) filmant 8 salariés, soit une caméra par salarié.
Ce dispositif était manifestement excessif, puisque le dirigeant de la société plaçait ses salariés sous une surveillance constante et permanente. La CNIL a mis en demeure le dirigeant de se mettre en conformité avec la loi, ce qu'il a fait.

Quelle information ?

Les personnes concernées (employés et visiteurs) doivent être informées, au moyen d'un panneau affiché de façon visible dans les locaux sous vidéosurveillance :

- de l'existence du dispositif,
- du nom de son responsable,
- de la base légale du dispositif (dans la quasi totalité des cas, l'intérêt légitime de l'employeur de sécuriser ses locaux),
- de la durée de conservation des images,
- de la possibilité d'adresser une réclamation à la CNIL,
- de la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant.

De plus, chaque employé doit être informé individuellement (au moyen d'un avenant au contrat de travail ou d'une note de service, par exemple).

Non, cette information n'est pas suffisante

Oui

Les textes de référence

- Le Règlement européen sur la protection des données personnelles (RGPD)
- **Le code de la sécurité intérieure, lorsque les caméras filment des lieux ouverts au public :**
  Articles L223-1 et suivants (lutte contre le terrorisme)
  Articles L251-1 et suivants, lorsque les caméras filment des lieux ouverts au public
- **Le code du travail :**
  Article L2323-47 (information/consultation des instances représentatives du personnel)
  Articles L1221-9 et L1222-4 (information individuelle des salariés)
  Article L1121-1 (principe de proportionnalité)
- **Le code civil :** Article 9 (protection de la vie privée)
- **Le code pénal :**
  Article 226-1 (enregistrement de l'image d'une personne à son insu dans un lieu privé)
  Article 226-18 (collecte déloyale ou illicite)
  Article 226-20 (durée de conservation excessive)
  Article 226-21 (détournement de la finalité du dispositif)
  Article R625-10 (absence d'information des personnes)

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.

Travail &
Données personnelles

L'écoute et l'enregistrement des appels

Les dispositifs d'écoute et d'enregistrement des conversations téléphoniques sur le lieu de travail sont installés à des fins de formation ou d'évaluation. Dans quelles conditions ces systèmes doivent-ils être utilisés ? Quelles sont les garanties au regard des droits et des libertés des salariés ?

Quelles utilisations possibles ?

L'écoute en temps réel et l'enregistrement sonore des appels sur le lieu de travail peuvent être réalisés en cas de **nécessité reconnue** et doivent être **proportionnés aux objectifs poursuivis**.

Ainsi, l'employeur peut installer un dispositif d'écoute et/ou d'enregistrement ponctuel des conversations téléphoniques pour :

- former ses salariés (par exemple, réutiliser des enregistrements comme support afin d'illustrer son propos lors de formations),
- les évaluer,
- améliorer la qualité du service (par exemple, en étudiant le type de réponse apporté au client),
- dans certains cas limités prévus par un texte légal, les appels peuvent servir de preuves à l'établissement d'un contrat ou à l'accomplissement d'une transaction.

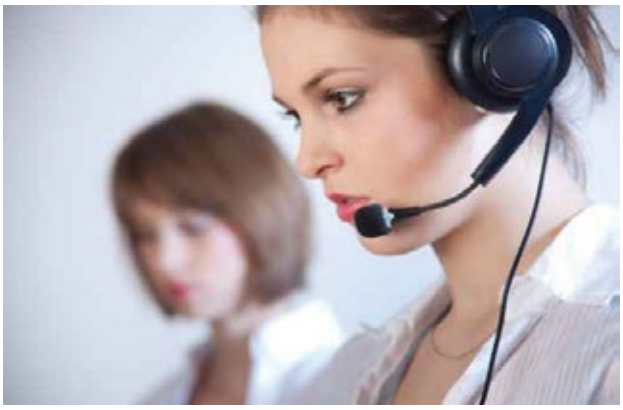
Des documents d'analyse (comptes-rendus ou grilles d'analyse) peuvent être rédigés sur la base des écoutes et enregistrements dès lors qu'ils s'inscrivent dans ces objectifs.

À cette occasion, l'employeur ne doit collecter et traiter que des informations nécessaires au but poursuivi (données d'identification du salarié et de l'évaluateur, informations techniques relatives à l'appel, évaluation professionnelle de l'employé).

Quelles limites à ces dispositifs ?

L'employeur ne peut pas mettre en place un dispositif d'écoute ou d'enregistrement **permanent ou systématique,** sauf texte légal (par exemple, pour les services d'urgence).

L'employeur ne peut pas non plus enregistrer tous les appels pour lutter contre les incivilités. Il doit choisir un moyen moins intrusif (par exemple opter pour un système permettant au salarié de déclencher l'enregistrement en cas de problème).



À noter

L'enregistrement des appels ne peut être couplé à un système de captures d'écran du poste informatique des salariés. Un tel système serait disproportionné et de nature à porter atteinte aux droits et libertés des salariés. Cette pratique, très intrusive, pourrait en effet conduire l'employeur à visualiser des informations qu'il n'a pas à connaître (par exemple : des e-mails personnels, ou liés à l'activité syndicale de représentants du personnel...).

Quelles garanties pour la vie privée ?

Les droits des employés

L'employeur doit mettre à disposition des salariés des lignes téléphoniques non reliées au système d'enregistrement, ou un dispositif technique leur permettant de couper l'enregistrement, pour les appels personnels. Il en va de même pour les appels passés par les représentants du personnel dans le cadre de l'exercice de leurs mandats.

Les personnes habilitées à écouter et accéder aux données

L'accès aux informations doit être limité aux services concernés par l'objectif poursuivi. Par exemple, si-l'enregistrement est mis en oeuvre à des fins de formation, seules pourront accéder aux données les personnes chargées de cette mission.

L'écoute et l'enregistrement des appels

La sécurité

Pour éviter notamment que des personnes non autorisées n'accèdent aux informations qu'elles n'ont pas à connaître, il est impératif de prendre des mesures de sécurité. Ainsi, l'employeur doit notamment mettre en place des habilitations pour les accès informatiques aux enregistrements, avec une traçabilité des actions effectuées (savoir qui se connecte à quoi, quand et pour quoi faire).

Des durées de conservation limitées

Sauf texte imposant une durée spécifique ou justification particulière, les enregistrements peuvent être conservés jusqu'à six mois au maximum. Les documents d'analyse peuvent quant à eux être conservés jusqu'à un an.

Une bonne pratique : les enregistrements « tampon »

Cette pratique consiste pour l'employeur, ou la personne habilitée, à écouter les enregistrements dans les jours suivant leur réalisation et à rédiger le(s) document(s) d'analyse nécessaire(s).
Les enregistrements sont ensuite supprimés à bref délai, l'employeur ne conservant que les documents d'analyse.

L'information des personnes

Les instances représentatives du personnel doivent être informées et consultées avant toute décision d'installer un dispositif d'écoute ou d'enregistrement des appels.

Les salariés ainsi que les interlocuteurs (clients, par exemple) doivent être notamment informés :

- de l'existence du dispositif,
- de l'identité du responsable de traitement,
- des finalités poursuivies,
- de la base légale du dispositif (obligation issue d'un texte légal par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données issues du dispositif,
- de la durée de conservation des données,
- de leur droit d'opposition pour motif légitime,
- de leurs droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Les interlocuteurs doivent être informés de leur droit d'opposition avant la fin de la conversation téléphonique, afin d'être en mesure d'exercer ce droit.

L'information des interlocuteurs s'effectue en deux temps :

- mention orale en début de conversation sur l'existence du dispositif, la finalité poursuivie, la possibilité de s'y opposer,
- renvoi vers un site Internet (et un onglet « mentions légales » par exemple) ou une touche « mentions légales » sur le téléphone pour obtenir une information exhaustive.

Au regard de la jurisprudence de la Cour de cassation en matière sociale, les salariés doivent être informés des périodes pendant lesquelles ils sont susceptibles d'être écoutés ou enregistrés.

Quelle formalité ?

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en oeuvre des écoutes ou des enregistrements des appels.

Le dispositif d'enregistrement ou d'écoute doit être inscrit au registre des activités de traitement tenu par l'employeur.

Quels recours ?

Si un dispositif d'écoute ou d'enregistrement ne respecte pas ces règles, vous pouvez saisir :

- le service des plaintes de la CNIL, sur les modalités de mise en oeuvre du dispositif,
- les services de l'inspection du Travail,
- le Procureur de la République.

Les textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L.1121-1 (droits et libertés dans l'entreprise)
  Articles L.1222-3 et L.1222-4 (information des salariés)
  Article L.2323-32 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.