Technologies de l'information et de la communication

L'employeur dispose du droit de surveiller et de contrôler l'activité de ses salariés au travail.

Cependant, cette surveillance reste encadrée par le Code du travail qui dispose, en son article L. 1112-1, que nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

De plus l'article 9 du Code civil consacre le droit de chacun au respect de sa vie privée.
L'employeur doit donc notamment tolérer que ses salariés utilisent à des fins personnelles le matériel informatique qu'il met à leur disposition pour un usage professionnel.

Le recours aux différents moyens rattachés aux technologies de l'information et de la communication (autocommutateurs téléphoniques, géolocalisation, vidéosurveillance…) nécessite le respect :

- de conditions d'information préalable, communes à tous ces dispositifs,
- et de conditions de fond,

que nous allons rappeler dans cette note d'information.

afaq ISO 9001 Qualité AFNOR CERTIFICATION

FFB GRAND PARIS
Direction des Affaires Sociales
10 rue du Débarcadère - 75852 PARIS Cedex 17
Téléphone 01 40 55 10 00 - Fax 01 40 55 10 81
www.grandparis.ffbatiment.fr
siret : 784 718 033 00011

I. Obligations préalables à la mise en place des technologies de l'information et de la communication (TIC) dans l'entreprise

1. Information et consultation des représentants du personnel

- **Les obligations à l'égard du Comité d'Hygiène de Sécurité et des Conditions de travail (CHSCT)**

Le CHSCT doit être consulté avant toute décision d'aménagement important, modifiant les conditions d'hygiène et de sécurité ou les conditions de travail et, notamment, avant toute transformation importante des postes de travail découlant de la modification de l'outillage, d'un changement de produit ou de l'organisation du travail[1].

Dès lors que l'on considère qu'un dispositif de surveillance ou de contrôle des salariés entre dans cette catégorie, le CHSCT doit donc être consulté.
Il faut également rappeler que le CHSCT doit être consulté, lorsque l'employeur envisage de mettre en œuvre des mutations technologiques importantes et rapides, sur :

- le projet d'introduction et lors de l'introduction de nouvelles technologies, sur les conséquences de ce projet ou de cette introduction sur la santé et la sécurité des travailleurs[2] ;
- le plan d'adaptation que l'employeur est chargé d'établir à cet effet[3].

- **Les obligations à l'égard du Comité d'Entreprise (CE)**

Le CE doit par ailleurs être informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens et les techniques permettant un contrôle de l'activité des salariés[4].

En outre, le CE doit être informé et consulté en cas d'introduction dans l'entreprise de nouvelles technologies susceptibles d'avoir des conséquences sur l'emploi ou les conditions de travail des salariés. Il doit également être consulté en cas d'introduction dans l'entreprise de traitements automatisés de gestion du personnel[5].

En revanche, l'information et la consultation du CE ne sont toutefois pas obligatoires lorsque l'employeur met en place des procédés de surveillance dans des locaux où les salariés ne travaillent pas[6] (entrepôt de marchandises, toit d'un immeuble, lieux non affectés au travail…).

[1] Article L. 4612-8 du Code du travail.
[2] Article L. 4612-9 du Code du travail. Dans les entreprises dépourvues de CHSCT, les délégués du personnel ou, à défaut, les salariés sont consultés.
[3] Article L. 4612-10 du Code du travail.
[4] Article L. 2323-32 du Code du travail.
[5] Articles L. 2323-13 et L. 2323-32 du Code du travail.
[6] Cass. soc. 31 janvier 2001, n° 98-44290 ; Cass. soc. 19 janvier 2012, n° 08-45092.

La consultation du CHSCT et du CE doivent dans tous les cas précéder la déclaration du dispositif à la Commission Nationale de l'Informatique et des Libertés (CNIL).

- **Sanctions en cas de non consultation des représentants du personnel**

Si l'employeur ne respecte pas son obligation de consulter les institutions représentatives du personnel, le dispositif de surveillance ou de contrôle des salariés doit être considéré comme illicite.

D'autre part, le fait pour l'employeur de méconnaître cette obligation consultative constitue un délit d'entrave.

2. Formalités déclaratives auprès de la CNIL

2.1. Les obligations déclaratives à l'égard de la CNIL

Les entreprises doivent déclarer préalablement à sa mise en œuvre tout **traitement automatisé de données à caractère personnel** sous peine de sanctions pénales[7].

De la même façon, la modification ou la suppression de traitements existants doit également faire l'objet d'une déclaration.

La déclaration à la CNIL est, en fait, un engagement solennel de l'entreprise que le traitement satisfait aux exigences de la loi.

Lorsque l'employeur souhaite mettre en œuvre un traitement automatisé de données à caractère personnel, trois situations sont envisageables :

- celle pour laquelle il doit procéder à une **déclaration** de conformité à une **norme simplifiée** ;
- celle pour laquelle le fichier doit faire l'objet d'une **déclaration dite normale** de conformité ;
- et celle pour laquelle aucune formalité n'est requise.

- **La déclaration simplifiée** n'est possible que pour certains dispositifs de contrôle pour lesquels la CNIL a édicté des normes dites « simplifiées »[8].

[7] Article 22 de la loi « Informatique et libertés » n° 78-17 du 6 janvier 1978.

[8] Normes simplifiées n° 46 pour un contrôle de l'utilisation d'internet ne permettant pas un contrôle individuel des salariés, n° 47 pour les autocommutateurs, n° 51 pour la géolocalisation, n° 57 pour les traitements automatisés de données à caractère personnel destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail, etc..

Les dispositifs de contrôle pouvant être soumis à une déclaration simplifiée sont notamment :

- ceux destinés à **contrôler le bon fonctionnement de l'informatique** sans possibilité de contrôle individuel des salariés ;
- ceux de **géolocalisation** ;
- ceux destinés au comptage des communications téléphoniques par **autocommutateur** ;
- ceux destinés à l'**écoute et à l'enregistrement ponctuel des conversations téléphoniques** sur le lieu de travail.

La déclaration simplifiée n'est possible que si ces quatre dispositifs respectent les normes que la CNIL a établies. A défaut, l'employeur devra établir une déclaration dite normale de conformité.

Cette déclaration simplifiée est composée de deux pages.

- **La déclaration normale** consiste pour l'employeur à prendre l'engagement que le traitement mis en œuvre répond aux exigences de la loi.

Dans cette déclaration, l'employeur doit notamment préciser l'identité du responsable du traitement, sa finalité, les données traitées, la durée de conservation des informations traitées, les dispositions prises pour assurer la sécurité du traitement, etc.

Cette déclaration normale est composée de 6 pages.

Conseil : les déclarations peuvent être réalisées en ligne sur le site internet de la CNIL (www.cnil.fr).

- Il existe des **dispenses de déclaration** pour certaines catégories de fichiers, parmi les catégories courantes de traitement qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés, comme les traitements de gestion de la paie et les fichiers de gestion des activités sociales et culturelles des comités d'entreprise.

  En outre, **la désignation d'un correspondant informatique et libertés** (CIL), chargé de garantir le respect des libertés individuelles dans l'entreprise, entraîne une dispense de déclaration préalable des traitements de données à caractère personnel. Cette désignation reste dans tous les cas facultative pour l'employeur.

- En cas de non-respect de la formalité de déclaration à la CNIL, l'employeur s'expose à une peine d'emprisonnement de cinq ans et une amende de 300 000 €.

  La CNIL, dotée de pouvoirs d'investigation, peut également sanctionner l'employeur qui ne respecte pas ses obligations (avertissement, mise en demeure, sanctions pécuniaires pouvant aller jusqu'à 150.000 euros ou 300.000 euros en cas de récidive, injonction de cesser la surveillance…).

Enfin, dans le cas où les formalités déclaratives ne sont pas remplies, le dispositif de surveillance ou de contrôle est illicite.

3. Information préalable individuelle des salariés

Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif (informatique ou non) qui n'a pas été porté à sa connaissance préalablement[9].

La licéité des collectes, traitements automatisés de données nominatives, et des contrôles de tous ordres est subordonnée à l'information préalable individuelle du salarié. En pratique, il est conseillé de procéder à cette information notamment par courrier remis en main propre, messagerie électronique avec accusé de réception, LRAR[10].

Si l'obligation d'information des salariés n'est pas respectée, l'employeur ne pourra pas sanctionner le salarié, puisqu'il ne pourra se prévaloir des preuves rassemblées de façon illicite[11].

Cette information porte sur les éléments suivants[12] :

- finalité du dispositif ;
- identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
- informations collectées ;
- destinataires des données enregistrées ;
- modalités d'exercice du droit d'accès, d'opposition et de rectification du salarié de ces données.

Les salariés doivent être informés même si le procédé de surveillance est matériellement visible (Cass. soc. 7 juin 2006, n° 04-43866).

Le défaut d'information des salariés est puni d'une amende prévue pour les contraventions de cinquième classe, soit 1500 euros et 3000 euros en cas de récidive[13].

ATTENTION :

Dans tous les cas, si l'employeur ne respecte pas ses obligations d'information préalable, il s'expose à :

- des dommages-intérêts si un préjudice a été subi par le salarié ;
- l'annulation d'une sanction par les juridictions civiles dans le cas où la faute sanctionnée aurait été établie par un dispositif de contrôle considéré comme un mode de preuve illicite[14].

9 Article L. 1222-4 du Code du travail.
10 L'affichage est insuffisant pour caractériser une information individuelle (Cass. soc. 8 mars 2005, n° 02-47123).
11 Cass. Soc., n° 06-11.942 du 3 juin 2008.
12 Article 32 de la loi « Informatique et libertés ».
13 Article R. 625-10 du Code pénal.

II. L'utilisation des TIC

1. Contrôle de l'utilisation de l'ordinateur sur le lieu de travail

• Les fichiers informatiques

Les dossiers et fichiers créés par un salarié grâce à son outil de travail informatique, mis à sa disposition pour l'exécution de son travail, sont présumés avoir un caractère professionnel[15]. L'employeur peut y avoir accès hors sa présence.

Cependant, **le salarié a la possibilité d'identifier ses fichiers comme « personnels »** afin d'en préserver la confidentialité : **l'employeur ne pourra alors accéder à ces fichiers qu'en présence du salarié, sauf risque ou événement particulier pour l'entreprise[16]**.
Le fait qu'un fichier porte le prénom du salarié, les initiales du salarié ou que le fichier soit contenu dans un ordinateur protégé par un mot de passe, ne lui permet pas d'être considéré comme un fichier personnel. L'employeur peut y accéder en l'absence du salarié et s'en servir comme preuve pour le sanctionner[17].

Bien entendu, le salarié ne saurait se laisser tenter par l'idée de qualifier tous ses fichiers de « personnel » afin d'empêcher son employeur d'y accéder : l'employeur pourrait identifier un volume anormal de fichiers personnels pouvant justifier d'éventuelles sanctions. Si le salarié avoue, ensuite, avoir abusivement qualifié ses fichiers de « personnel » pour en protéger l'accès, il pourrait se voir reprocher une violation de l'exécution de bonne foi de son contrat de travail[18].

• Les connexions internet

Les connexions internet effectuées pendant le temps de travail, grâce à l'outil informatique mis à disposition par l'employeur, sont présumées avoir un caractère professionnel[19]. L'employeur peut donc également les rechercher hors la présence du salarié, afin de les identifier.
Ce principe peut être rappelé aux salariés par le biais d'une charte informatique, du règlement intérieur ou d'une note de service.

---

14 Cass. soc. 20 novembre 1991, n° 88-43120.
15 Cass. Soc., n° 04-48.025 du 18 octobre 2006.
16 Cass. Soc., n° 03-40.017 du 17 mai 2005. Si le contrôle est justifié par un risque ou évènement particulier pour l'entreprise, telle que la suspicion d'actes de concurrence déloyale ou d'appartenance à un réseau pénalement répréhensible, le contrôle peut se faire sans le salarié.
17 Cass. Soc., n° 08-44.840 du 8 décembre 2009.
18 Article L. 1222-1 du Code du travail.
19 Cass. Soc., n° 06-45.800 du 9 juillet 2008.

- **La messagerie électronique professionnelle**

Comme en matière d'utilisation personnelle de l'ordinateur et d'internet, les principes suivants peuvent être rappelés :

- **sauf à être identifiée comme personnelle**, la correspondance émise ou reçue sur la messagerie professionnelle du salarié est par nature professionnelle et peut donc être lue par l'employeur ;
- afin de préserver le secret des correspondances, les salariés sont invités à signaler dans l'objet de leur message, le caractère personnel de leurs correspondances ;
- l'employeur peut procéder à un contrôle, en termes de volume, de l'utilisation personnelle et professionnelle faite par le salarié de la messagerie électronique de l'entreprise (taille des messages, volume des pièces jointes, etc.) ; car l'abus peut justifier une sanction disciplinaire.

L'utilisation personnelle de la messagerie électronique professionnelle relève de la tolérance.

L'arrêt Nikon[20] a consacré un droit à une vie privée sur les lieux et pendant les temps professionnels.

En outre, les juges ont précisé que le principe du respect des correspondances, inhérent au droit au respect de la vie privée, ne saurait s'effacer au prétexte que l'utilisation non professionnelle de l'outil informatique aurait été prohibée. En d'autres termes, la violation par le salarié du règlement intérieur ou d'une charte informatique n'autorise pas l'entreprise à violer les droits fondamentaux de la personne.

Le salarié peut donc communiquer avec ses proches, passer un appel non professionnel, envoyer un mail à un ami…

Une interdiction totale d'utiliser Internet à des fins privées semble à première vue une restriction disproportionnée. Il convient donc de prendre en compte la notion de respect du principe du secret des correspondances.

Comme pour les fichiers informatiques, l'employeur pourra toujours contrôler les courriers électroniques personnels dans le cas d'un danger menaçant l'entreprise (éventuel acte de terrorisme ou piratage de données essentielles, concurrence par des procédés déloyaux…).

L'employeur peut également recourir à l'article 145 du Code de procédure civile et solliciter du juge des requêtes une mesure d'instruction préventive. Sur requête de l'employeur qui souhaite avoir connaissance d'un courriel d'un salarié pour établir et préserver des preuves, le président du tribunal de grande instance va nommer par ordonnance un huissier pour effectuer un constat et prendre connaissance du courriel. Mais cette procédure est subordonnée à l'existence d'un motif légitime et doit être nécessaire à la protection des droits de la partie qui les sollicite (par exemple, en cas de soupçon d'actes de concurrence déloyale).

Il est prudent pour l'employeur de définir les règles d'utilisation de la messagerie électronique dans une charte informatique.

[20] Cass. Soc., n° 99-42.942 du 2 octobre 2001.

- **Les SMS**

Les SMS (« short message service ») envoyés ou reçus par le salarié au moyen du téléphone mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme personnels.

Dans le droit fil de la jurisprudence sur les messages électroniques, la Cour de cassation a ainsi décidé, dans un arrêt du 10 février 2015, que l'employeur est en droit d'accéder aux SMS envoyés et reçus via un téléphone professionnel, dès lors qu'ils ne sont pas identifiés comme « personnels ».

- **Les réseaux sociaux**

Des publications de propos injurieux ou de dénigrement tenus par un salarié sur des réseaux sociaux peuvent-elles faire l'objet de sanctions par l'employeur, alors que le salarié agit en dehors du temps de travail avec un ordinateur lui appartenant ?

Les propos tenus sur le « mur » **Facebook** du profil privé d'une salariée, accessible à ses seuls « amis » ou « contacts », en nombre très restreint, ne constituent pas des injures publiques selon la 1ère chambre civile de la Cour de cassation[21].

En effet, dans cette affaire, ceux-ci n'étaient accessibles qu'aux seules personnes agréées par la salariée, en nombre très restreint, lesquelles formaient une « communauté d'intérêt ».

Cette décision émane non pas de la chambre sociale de la Cour de cassation, mais de la première chambre civile. La chambre sociale ne s'est quant à elle pas encore prononcée dans le cadre des affaires « Facebook ».

2. Contrôle de l'utilisation du téléphone au travail

- **Contrôle par autocommutateur**

L'employeur a la possibilité de mettre en place un dispositif permettant une maîtrise des dépenses liées à l'utilisation professionnelle et privée des services de téléphonie, par le biais d'autocommutateurs téléphoniques qui permettent d'enregistrer la durée, le coût et les numéros des appel émis par les salariés.

Attention ! La mise en place d'un autocommutateur est un dispositif de traitement de données individuelles : il doit donc faire l'objet d'une déclaration préalable à la CNIL et répondre aux prescriptions de la norme simplifiée n° 47.

[21] Cass. 1re civ., 10 avr. 2013, n° 11-19.530.

La norme simplifiée n° 47 prévoit notamment :

❖ Finalités

- la gestion de la dotation en matériel téléphonique et la maintenance du parc téléphonique ;
- la gestion de l'annuaire téléphonique interne ;
- la gestion technique de la messagerie interne de l'organisme ;
- le remboursement des services de téléphonie utilisés à titre privé par les employés lorsque le caractère privé de l'utilisation de ces services est déterminé par les employés eux-mêmes ;
- la maîtrise des dépenses liées à l'utilisation professionnelle des services de téléphonie ;
- la maîtrise des dépenses liées à l'utilisation effectuée à titre privé des services de téléphonie.

❖ Informations collectées et traitées

- identité de l'utilisateur du service téléphonique : nom, prénom et numéro de ligne ;
- situation professionnelle : fonction, service, adresses professionnelles y compris électroniques ;
- utilisation des services de téléphonie : numéro de téléphone appelé, service utilisé, opérateur appelé, nature de l'appel, durée, date et heure de début et de fin de l'appel, éléments de facturation.

❖ Durée de conservation

Les données à caractère personnel relatives à l'utilisation des services de téléphonie ne peuvent être conservées au-delà du délai d’un an courant à la date de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie.

❖ Destinataires des informations

En fonction des finalités, les destinataires des informations peuvent être :

- pour les données relatives à l'annuaire téléphonique : l'ensemble du personnel ;
- pour les données relatives à la messagerie interne : le titulaire du compte de messagerie concerné ;
- pour les données relatives à la consommation des services téléphoniques : les personnels habilités des services comptables ou financiers chargés de l'élaboration des relevés de communication, les agents disposant du poste téléphonique concerné et, dans les conditions prévues à l'article 6 de la présente norme, les supérieurs hiérarchiques des personnels concernés et les personnels du service du personnel en cas d'utilisation manifestement abusive constatée à l'occasion de l'établissement des relevés non détaillés ;
- pour l'ensemble des données : les personnels des services techniques chargés de la mise en œuvre et de la maintenance du service téléphonique dans le strict cadre de leurs attributions.

- **Contrôle par le biais de la facture détaillée**

L'employeur peut utiliser les factures détaillées de téléphone, sans avoir à effectuer de formalités d'information préalables à l'égard des représentants du personnel ou des salariés.

La production par l'employeur des relevés de facturation téléphonique constitue donc un mode de preuve licite[22].

La Cour de cassation a validé le licenciement pour faute grave d'un salarié ayant, malgré les remontrances de son employeur, persisté à utiliser son téléphone professionnel de manière « continuelle et journalière » quasiment exclusivement à des fins privées et en appelant des numéros surtaxés sans lien avec son activité professionnelle[23]. Même solution à l'égard d'une salariée ayant utilisé de façon répétée, sur une durée de 5 mois, le téléphone de l'entreprise pour passer des communications internationales pour des durées souvent supérieures à 15 minutes, à l'insu de celle-ci[24].

La CNIL précise qu'en principe, les quatre derniers chiffres des numéros appelés sont occultés sauf dans deux cas :

- quand un remboursement est demandé au salarié pour des services de téléphonie utilisés à titre privé ;
- quand l'employeur constate une utilisation manifestement anormale au regard de l'utilisation moyenne constatée au sein de l'entreprise des services de téléphonie.

- **Ecoute ou enregistrement des conversations téléphoniques**

L'écoute ou l'enregistrement des paroles prononcées par une personne, sans le consentement de celle-ci, constituent une atteinte à l'intimité de la vie privée et sont réprimés par l'article 226-15 du Code pénal[25].

A titre ponctuel[26], l'enregistrement des conversations téléphoniques peut être autorisé. Les écoutes et enregistrements sur le lieu de travail se multipliant, la CNIL a allégé par une délibération publiée au JO du 6 janvier 2015 les formalités déclaratives pour les entreprises souhaitant mettre en place de tels dispositifs.

Attention ! La mise en place d'un dispositif d'écoute et d'enregistrement des appels est un dispositif de traitement de données individuelles : il doit donc faire l'objet d'une déclaration préalable à la CNIL et répondre aux prescriptions de la norme simplifiée n° 57.

[22] Cass. soc., 11 mars 1998, n° 96-40.147 - Cass. soc. 15 mai 2001, n° 99-42.937, n° 2086 FS - P + B.
[23] Cass. soc., 24 sept. 2013, n° 12-16.943.
[24] Cass. soc., 13 nov. 2013, n° 12-18.280.
[25] Le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
[26] L'enregistrement permanent ou systématique des appels sur le lieu de travail est exclu.

La norme simplifiée n° 57 prévoit notamment :

❖ Finalités

- La formation des employés ;
- L'évaluation des employés ;
- L'amélioration de la qualité du service.

❖ Informations collectées et traitées

- les données d'identification de l'employé et de l'évaluateur ;
- les informations techniques relatives à l'appel (date, heure et durée de l'appel) ;
- l'évaluation professionnelle de l'employé.

❖ Destinataires et personnes habilitées à traiter les données

Les personnes chargées de la formation des employés, de leur évaluation et de l'amélioration de la qualité du service peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel collectées.

❖ Durées de conservation

Les enregistrements ne doivent pas être conservés au-delà de six mois à compter de leur collecte. La durée de conservation des documents d'analyse (comptes rendus et grilles d'analyse) établis dans le cadre d'une écoute directe ou différée des appels est fixée à un an maximum.

Cas particulier des salariés protégés

Selon la CNIL, toute utilisation des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat est interdit.

La géolocalisation

Il faut savoir que la jurisprudence est extrêmement sévère à l'égard des dispositifs GPS, lorsqu'ils sont utilisés à des fins de surveillance permanente des salariés : la Cour de cassation assimile en effet ce procédé à celui de la filature, condamnant un tel moyen de surveillance des salariés, en ce qu'il porte atteinte à la vie privée[27].

Attention ! La mise en place d'un dispositif de géolocalisation doit faire l'objet d'une déclaration préalable à la CNIL et répondre aux prescriptions de la norme simplifiée n° 51.

[27] Cass. Soc., n° 00-42.401 du 26 novembre 2002.

La norme simplifiée n° 51 prévoit notamment :

❖ **Finalités**[28]

- la sûreté ou la sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge ;
- la gestion en temps réel des interventions auprès des clients ;
- l'amélioration du processus de production ;
- le suivi du temps de travail des salariés, **à la double condition** que le salarié ne dispose pas d'une liberté dans l'organisation de son travail et que le suivi ne puisse être fait par d'autres moyens.

Il résulte que :

- la géolocalisation ne peut être utilisée pour contrôler la durée de travail des salariés autonomes
- la géolocalisation ne peut être utilisée pour contrôler la durée du travail si ce suivi peut être réalisé par d'autres moyens.

L'employeur doit donc être très prudent lorsqu'il utilise la géolocalisation pour contrôler le temps de travail des salariés.

Attention : lorsque l'employeur a effectué une déclaration simplifiée de la géolocalisation, il s'engage à respecter la norme simplifiée n° 51 selon laquelle le suivi du temps de travail ne peut être qu'une finalité accessoire à l'une des trois autres finalités (sûreté/sécurité, gestion des interventions ou amélioration du processus de production).
A défaut, l'employeur devra effectuer une déclaration normale.

❖ **Informations collectées et traitées**

- l'identification de l'employé : nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule ;
- les données relatives aux déplacements des employés : données de localisation issues de l'utilisation d'un dispositif de géolocalisation, historique des déplacements effectués ;
- les données complémentaires associées à l'utilisation du véhicule : vitesse de circulation du véhicule, nombre de kilomètres parcourus, durées d'utilisation du véhicule, temps de conduite, nombre d'arrêts.

S'agissant du cas particulier de la vitesse, la CNIL estime qu'aucun contrôle des vitesses maximales ne peut être effectué par la géolocalisation car l'employeur n'est pas autorisé à mettre en œuvre des techniques visant à faire apparaître des données relatives aux infractions du Code de la route.

[28] Adaptées au secteur du Bâtiment.

Conseil : la CNIL recommande la désactivation du système de géolocalisation embarqué dans les véhicules de fonction en dehors des horaires de travail ou lors des temps de pause.

❖ Destinataires et personnes habilitées à traiter les données

L'accès des données collectées doit être limité aux seules personnes habilitées à les recevoir et à les consulter (gérant de l'entreprise, services des ressources humaines ou service comptable par exemple).

❖ Durées de conservation

Selon la CNIL, la conservation des données est en principe de deux mois. Elle peut être portée à un an si la conservation des données constitue le seul moyen de preuve de la prestation ou si l'historique des déplacements est conservé à des fins d'optimisation des tournées.

Dans le cadre du suivi du temps de travail, seules les données relatives aux horaires effectués peuvent être conservées 5 ans.

Cas particulier des salariés protégés

Selon la CNIL, toute utilisation des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat est interdit.

La vidéosurveillance

Dans le Bâtiment, la vidéosurveillance a essentiellement pour finalité la sécurité des biens et des personnes.

❖ Déclaration à la CNIL

La mise en place de la vidéosurveillance doit faire l'objet d'une déclaration normale à la CNIL dès lors que :

- Les images font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage ;
- Le responsable du traitement ou les personnes ayant accès aux enregistrements peuvent identifiées les personnes filmées.

❖ Information des salariés

La vidéosurveillance ne peut pas être installée à l'insu des salariés dans les lieux de travail. L'employeur doit donc informer au préalable ses salariés, quel que soit le leur lieu de travail et le responsable du dispositif de surveillance[29].

A défaut d'information préalable, la vidéosurveillance ne pourra pas être utilisée comme mode de preuve à l'appui d'une sanction disciplinaire ou d'un licenciement.

En revanche, dans les locaux dans lesquels les salariés ne travaillent pas (comme un entrepôt ou un toit, l'employeur peut, sans en informer préalablement les représentants du personnel et les salariés, mettre en place un dispositif de surveillance. L'employeur peut alors même utiliser la vidéosurveillance des locaux autres que des lieux de travail (mise en place sans information préalable des salariés) à l'appui d'une sanction disciplinaire. Il s'agit d'un mode de preuve licite[30].

❖ Finalités

Le dispositif de vidéosurveillance doit être justifié par la nature de la tâche à accomplir. Le plus souvent, la finalité du dispositif est la sécurité des biens et des personnes.

La Cour de cassation a également précisé que les salariés devaient être informés de l'installation de la vidéosurveillance mais aussi de sa finalité.

❖ Condition de proportionnalité

Le dispositif de vidéosurveillance ne doit pas être disproportionné par rapport au but recherché. Selon la CNIL, le respect du principe de proportionnalité suppose de tenir compte de l'emplacement, de l'orientation, des périodes de fonctionnement des caméras et de la nature des tâches accomplies par les salariés.

A titre d'exemple, la CNIL a décidé que le principe de proportionnalité n'était pas respecté lorsque :

- Les caméras filment en continu des lieux réservés au personnel dans lesquels aucune marchandise n'est stockée alors que la vidéosurveillance a été mise en place pour éviter les vols (CNIL délibération n° 2009-201 du 16 avril 2009) ;
- Les salariés sont placés sous surveillance constante (l'employeur avait accès aux images à distance et notamment de chez lui), générale (les caméras filmaient les postes de travail des salariés) et permanente (jour et nuit) alors que la vidéosurveillance a été mise en place pour assurer la sécurité des salariés travaillant la nuit et le week-end (CNIL délibération n° 2010-112 du 22 avril 2010) ;
- Les caméras pouvant être déclenchées à tout moment, filment à la fois les écrans d'ordinateurs et les salariés et sont équipées de microphones permettant d'écouter leurs conversations alors que la vidéosurveillance a été installée pour des raisons de sécurité (CNIL délibération du 16 décembre 2011 n° 2011-036).

---

[29] Dans un arrêt du 10 janvier 2012, la Cour de cassation a décidé que l'employeur devait informer les salariés de la mise en place de la vidéosurveillance chez le client et de la finalité qui pourrait en être faite. Dans cette affaire, une société de nettoyage avait fait intervenir ses salariés chez un client, lequel était équipé d'un dispositif de vidéosurveillance.

[30] Cass. soc., 31 janvier 2001, n° 02-46295 et Cass. soc., 19 janvier 2010, n° 08-45092.

❖ **Destinataires et personnes habilitées à traiter les données**

Les images enregistrées ne peuvent être visionnées que par les seules personnes dûment habilitées à cet effet.

La CNIL a par exemple décidé qu'un système de vidéosurveillance rendant possible le visionnage des images à distance en temps réel par la simple saisie de l'adresse IP de la caméra, sans saisie d'un mot de passe et d'un identifiant, ne respectait pas l'article 34 de la loi « Informatique et libertés ».

❖ **Durées de conservation**

Selon la CNIL, la durée de conservation des images enregistrées à l'aide d'un dispositif de vidéosurveillance, ne devrait pas excéder quelques jours. Cette durée ne peut en tout état de cause s'étendre au-delà d'un mois (CNIL délibération du 22 avril 2010 et décision du 16 décembre 2011).

Tableau récapitulatif des principales formalités déclaratives auprès de la CNIL

Finalités du fichier	Formalités déclaratives	Conditions particulières
Paye Déclarations fiscales et sociales obligatoires (déclarations aux organismes de protection sociale, de retraite, DADS, DUE, DOETH…), y compris celles qui sont réalisées à partir de www.net-entreprises.fr. Tenue des registres obligatoires (registre unique du personnel…). Tenue des comptes individuels relatifs à l'intéressement et à la participation. Statistiques non nominatives liées à l'activité salariée dans l'entreprise.	Aucune	Respecter les termes de la dispense n° 2 (employeurs privés) du 9 décembre 2004. **Attention !** Les transferts de données vers un pays tiers à l'Union Européenne ne sont pas dispensés.
Comptabilité générale	Aucune	Respecter les termes de la dispense n° 80-34 du 21 octobre 1980.
Traitements mis en œuvre par le comité d'entreprise, ou les délégués du personnel pour la gestion de leurs activités sociales et culturelles.	Aucune	Respecter les termes de la dispense n° 10 du 17 octobre 2006.
• Gestion des contrôles d'accès aux locaux. • Gestion des horaires. • Gestion de la restauration d'entreprise.	Déclaration simplifiée. Si désignation d'un correspondant informatique et libertés : aucune.	Respecter la norme simplifiée n° 42. Cette norme ne concerne pas les traitements recourant à un procédé de reconnaissance biométrique, qui sont soumis à une procédure d'autorisation.
Fichiers courants de gestion des ressources humaines : • Gestion administrative (dossiers professionnels, annuaires, élections professionnelles, convocations) ; • Mise à disposition d'outils informatiques (suivi et maintenance, annuaires informatiques, messagerie électronique, intranet) ; • Organisation du travail (agenda professionnel, gestion des tâches) ; • Gestion des carrières (évaluation, validation des acquis, mobilité) ; • Gestion de la formation.	Déclaration simplifiée. Si désignation d'un correspondant informatique et libertés : aucune.	Respecter la norme simplifiée n° 46. Cette norme exclut notamment : • les traitements permettant le contrôle individuel de l'activité des employés ; • les dispositifs ayant pour objet l'établissement du profil psychologique des employés ; • les transferts de données vers un pays tiers à l'Union Européenne.

Finalités du fichier	Formalités déclaratives	Conditions particulières
Traitements automatisés de données à caractère personnel, destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail	Déclaration simplifiée.	Respecter la norme simplifiée n° 57
Mise en œuvre de services de téléphonie fixe et mobile sur les lieux de travail. Gestion des communications (annuaire interne, gestion des dotations, messagerie téléphonique interne, maîtrise des dépenses liées à l'utilisation des services de téléphonie…).	Déclaration simplifiée. Si désignation d'un correspondant informatique et libertés : aucune.	Respecter la norme simplifiée n° 47
Mise en œuvre de services destinés à géolocaliser les véhicules utilisés par les salariés.	Déclaration simplifiée. Si désignation d'un correspondant informatique et libertés : aucune.	Respecter la norme simplifiée n° 51
Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la Commission, notamment : • annuaires du personnel sur internet ; • traitements informatiques permettant un contrôle de l'activité professionnelle des salariés (surveillance des connexions internet ou de la messagerie électronique, géolocalisation) ; • traitements de vidéosurveillance ; • traitements de recrutement (bases de données de CV ou de candidats). Traitements comportant un transfert de données vers un pays tiers à l'Union Européenne.	Déclaration normale. Si désignation d'un correspondant informatique et libertés : aucune. Autorisation	Utiliser le formulaire de déclaration normale téléchargeable sur le site de la CNIL (www.cnil.fr; rubrique déclarer, mode d'emploi). Pour les fichiers de recrutement : se référer à la recommandation n° 02-017 du 21 mars 2002.

Finalités du fichier	Formalités déclaratives	Conditions particulières
Dispositifs biométriques : reconnaissance du contour de la main pour assurer le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail.	Autorisation unique	Respecter les termes de l'autorisation unique AU-008.
Dispositifs biométriques : reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels.	Autorisation unique	Respecter les termes de l'autorisation unique AU-007.
Dispositifs biométriques : reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail.	Autorisation unique	Respecter les termes de l'autorisation unique AU-019.
Autres dispositifs biométriques.	Autorisation	
Dispositifs d'alerte professionnelle dans le domaine financier, comptable, bancaire et de la lutte contre la corruption.	Autorisation unique	Respecter les termes de l'autorisation unique AU-004.
Autres dispositifs d'alerte professionnelle.	Autorisation	Un dispositif permettant de signaler des violations autres que comptables ou financières (ex : harcèlement, atteinte aux droits de propriété intellectuelle, violation d'un code de bonne conduite…).