LIVRE BLANC

RGPD, email, caméra… 25 idées reçues sur le contrôle des salariés

Auteur : Sophie VALAZZA, avocate au barreau de Toulon • Juin 2022

TISSOT éditions

Introduction

De manière générale, le monde de l'entreprise est largement favorable à l'introduction des technologies de l'information et de la communication (TIC) qui permettent d'accroître la productivité, de repenser la relation de travail et favorisent l'émergence de nouveaux modes d'organisation du travail.

À travers des problématiques diverses (contrôle et surveillance, modalités d'utilisation par le salarié, télétravail, collecte et transmission des données personnelles, etc.), les TIC ont eu pour effet de modifier l'équilibre contractuel entre l'employeur et le salarié et de diluer les repères temporels et spatiaux du contrat de travail.

C'est la raison pour laquelle le droit est aujourd'hui pleinement saisi de cette question et qu'un système de règles a été organisé afin d'encadrer les droits de l'employeur et de protéger les libertés du salarié, sous le contrôle du juge national et européen et de la Commission nationale de l'informatique et des libertés (CNIL), garante de la protection des données personnelles.

Les contenus de ce livre blanc peuvent faire l'objet de modifications législatives, réglementaires ou encore jurisprudentielles. N'hésitez pas à vous référer au Code du travail, à votre (vos) convention(s) collective(s) ainsi qu'à la publication Tissot Social Entreprise Activ pour être à jour en permanence des évolutions du droit du travail.

Sommaire

Retrouvez dans ce livre blanc toutes les bonnes réponses aux affirmations suivantes :

1. RGPD : l'employeur peut refuser de donner suite à une demande d'accès du salarié aux informations qui le concernent

2. RGPD : le droit à l'effacement des données personnelles ne peut pas être limité par l'employeur

3. RGPD : l'employeur ne peut pas révéler les coordonnées personnelles du salarié

4. L'employeur peut lire l'ensemble des courriels qui émanent de la messagerie professionnelle du salarié

5. L'employeur peut exiger de recevoir la copie automatique de tous les messages écrits ou reçus par les salariés

6. L'employeur ne peut pas mettre en place un dispositif keylogger permettant d'enregistrer à distance toutes les actions effectuées sur un ordinateur

7. L'employeur peut exiger du salarié qu'il communique son mot de passe

8. L'employeur ne peut pas exiger du salarié qu'il réponde aux courriels en dehors de son temps de travail

9. L'employeur peut interdire toute utilisation personnelle des outils de communication de l'entreprise

10. L'employeur ne peut pas consulter la clé USB personnelle du salarié

11. Le salarié peut donner un caractère privé à l'intégralité des fichiers, courriels et documents contenus dans son ordinateur professionnel

12. L'employeur ne peut sanctionner les propos tenus par le salarié sur des réseaux sociaux que si la page est ouverte au public

13. L'employeur peut écouter toutes les communications téléphoniques passées par le salarié sur son téléphone professionnel

14. L'employeur ne peut pas coupler l'écoute des conversations téléphoniques à un système de capture de l'écran professionnel du salarié

15. Les enregistrements « tampons » constituent une pratique licite

16. L'employeur ne peut pas contrôler les communications des représentants du personnel

17. L'employeur peut contraindre le salarié à présenter un badge pour accéder aux locaux de l'entreprise

18. Les caméras de vidéosurveillance ne doivent pas filmer les espaces de pause ou de repos ni les salariés à leur poste de travail

19. Les caméras de vidéosurveillance peuvent comporter des microphones

20. Seul le responsable sécurité de l'entreprise a accès aux images de vidéo-surveillance

21. Le dispositif de géolocalisation du véhicule ne peut pas être utilisé pour contrôler les horaires de travail des salariés et le respect des limitations de vitesse

22. L'employeur peut utiliser les données de géolocalisation pour sanctionner le salarié

23. L'employeur peut imposer le télétravail

24. En cas de télétravail, l'employeur ne peut pas installer de dispositif de surveillance du domicile du salarié

25. L'employeur peut avoir accès au dossier pénal du salarié

1. RGPD : l'employeur peut refuser de donner suite à une demande d'accès du salarié aux informations qui le concernent

VRAI

Le règlement général sur la protection des données (RGPD) impose à l'employeur de ne collecter que les données personnelles des salariés qui sont pertinentes, au regard des finalités poursuivies. Cela implique que l'employeur détermine les motifs du traitement pour chaque type de donnée et soit en mesure, à tout moment, d'en justifier la légitimité.

En contrepartie, le salarié dispose non seulement d'un droit d'accès aux informations qui le concernent, mais également d'un droit de rectification d'une donnée qui serait erronée et d'un droit d'opposition et d'effacement du traitement.

Ainsi, un salarié est en droit d'accéder aux données relatives à son recrutement, à son historique de carrière, à l'évaluation de ses compétences professionnelles (entretiens annuels d'évaluation, notation), à ses demandes de formation et aux éventuelles évaluations de celles-ci, à son dossier disciplinaire, à l'utilisation de son badge de contrôle d'accès aux locaux, à ses données issues d'un dispositif de géo-localisation, et plus généralement à tout élément ayant servi à prendre une décision à son égard (une promotion, une augmentation, un changement d'affectation, des valeurs de classement annuel, etc.).

Néanmoins, le droit d'accès n'est pas illimité et l'employeur peut, dans certaines hypothèses, refuser de transmettre les données ou les documents sollicités :

– si le droit d'accès porte atteinte aux droits des tiers ;

Par exemple, l'employeur peut refuser de délivrer la copie d'un courriel qui met en cause un des collègues du salarié ou encore transmettre des images issues de caméras de vidéosurveillance où le salarié est entouré de personnes tierces (clients de l'entreprise par exemple).

– si le droit d'accès porte atteinte au secret des affaires ou à la propriété intellectuelle ;

– si la demande du salarié est manifestement infondée ou abusive.

Par exemple, un salarié qui multiplie les demandes de communication de données sans que cela ne soit justifié.

2. RGPD : le droit à l'effacement des données personnelles ne peut pas être limité par l'employeur

FAUX

Le droit à l'effacement des données personnelles a été mis en place par le RGPD et permet au salarié de demander à son employeur d'effacer l'ensemble des données collectées qui le concernent.

Pourtant ce droit n'est pas sans conditions et ne concerne en réalité que les données qui ne sont plus nécessaires au regard de la finalité poursuivie par le traitement.

Ainsi, le droit à l'effacement ne s'applique pas :

– lorsque la conservation des données répond à une obligation légale ou lorsqu'il s'agit de documents qui doivent être obligatoirement conservés par l'entreprise pendant une certaine durée.

EXEMPLES :

Le numéro de Sécurité sociale du salarié est obligatoire pour établir sa fiche de paie, il ne peut donc faire l'objet d'un effacement.

Les fiches de paie doivent être conservées pendant 5 ans.

De manière générale, la plupart des documents relatifs à la gestion du personnel ont une durée de conservation légale afin notamment de permettre à l'employeur de faire face à un contrôle de l'URSSAF ou de l'inspection du travail.

Au-delà de cette obligation, l'employeur a intérêt à les conserver le plus longtemps possible et peut donc opposer ce motif au salarié qui sollicite l'effacement de ses données ;

– lorsque le traitement mis en œuvre présente un caractère d'intérêt général ;

– lorsque le traitement est nécessaire dans le cadre d'un procès.

EXEMPLE :

L'employeur peut refuser d'accéder à une demande d'effacement si elle le prive d'éléments nécessaires à sa défense dans le cadre d'un procès contre le salarié.

3. RGPD : l'employeur ne peut pas révéler les coordonnées personnelles du salarié

VRAI et FAUX

En phase d'embauche, seules les personnes qui interviennent dans le processus de recrutement peuvent accéder aux informations personnelles relatives au candidat.

Une fois le contrat de travail conclu, seules les personnes en charge de la gestion des ressources humaines ont accès à ces informations, en plus des administrations concernées (caisses d'assurance maladie, de retraite, mutuelle, etc.).

Le supérieur hiérarchique du salarié ne peut avoir accès qu'aux informations qui sont nécessaires à l'exercice des attributions, comme par exemple les données relatives à l'évaluation.

Les représentants du personnel ont, quant à eux, accès aux informations qui figurent dans le registre unique du personnel (nom, date d'entrée, fonction, nationalité, etc.) et l'employeur ne peut leur transmettre d'autres informations que si le salarié ne s'y oppose pas.

EXEMPLE :

Communiquer le nombre et l'âge des enfants du salarié au comité social et économique afin que celui-ci lui puisse proposer les prestations et activités adaptées.

Il appartient donc au service RH de s'assurer que ce consentement a bien été recueilli et que le salarié ne s'oppose pas à la transmission d'informations. Bien entendu, il convient de lui indiquer dans quel cadre ces informations seront transmises et il est interdit de prévoir par avance une autorisation générale de transmission des données.

Enfin, l'employeur peut, dans certaines circonstances, être obligé de révéler les coordonnées d'un salarié lorsqu'il s'agit d'une obligation légale ou lorsque cela résulte d'une décision de justice.

EXEMPLE :

Ainsi l'employeur est contraint de divulguer les données personnelles du salarié au médecin contrôleur de la Sécurité sociale, à un officier de police judiciaire intervenant dans le cadre d'une enquête pénale, à un huissier qui dispose d'un titre exécutoire, etc.

En dehors de ces hypothèses, toute communication d'informations relatives à un salarié est interdite si elle n'a pas été préalablement autorisée par ce dernier.

4. L'employeur peut lire l'ensemble des courriels qui émanent de la messagerie professionnelle du salarié

FAUX

Il convient de distinguer les deux types de courriers électroniques qui sont susceptibles de figurer dans la messagerie professionnelle du salarié :

– les courriels professionnels (qui sont en lien avec l'emploi du salarié) : ils peuvent être ouverts par l'employeur dans la mesure où ils concernent directement l'entreprise ;

– les courriels personnels (qui sont étrangers au fonctionnement de l'entreprise) : ils bénéficient du secret des correspondances et ne peuvent pas être consultés par l'employeur (Cass. soc., 26 janvier 2016, n° 14-15.360).

Les courriels qui émanent de la messagerie professionnelle du salarié, qu'ils aient été envoyés ou reçus, sont présumés avoir un caractère professionnel et l'employeur est en droit de les ouvrir sans la présence du salarié, sauf si ce dernier les a identifiés comme personnels (Cass. soc., 15 décembre 2010, n° 08-42.486).

Sont considérés comme « personnels » les messages identifiés par une mention spécifique telle que « personnel », « privé » ou « perso ».

En revanche, les mentions « mes documents », « confidentiel », « prénom du salarié » ou les initiales du salarié ne suffisent pas à identifier ces courriels comme constituant des messages personnels.

Le principe de secret des correspondances personnelles s'applique même si l'employeur a interdit d'utiliser les outils informatiques de l'entreprise à des fins personnelles.

La protection des courriels personnels cesse si une enquête judiciaire est en cours (par exemple lorsque le salarié est accusé de vol des secrets industriels de l'employeur) ou si l'employeur a obtenu une décision de justice qui l'autorise à accéder aux messages.

Pour éviter tout problème, le service RH a tout intérêt à inciter les salariés à identifier leurs messages personnels :

– en précisant dans leur objet « Personnel » ou « Privé » ;

– en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

ATTENTION :

Dans tous les cas, l'employeur doit avoir préalablement informé les salariés d'un contrôle de leurs messageries professionnelles, dans les mêmes conditions que tout dispositif de surveillance. À défaut, le dispositif est illicite et ne pourra pas être utilisé à l'appui d'une sanction disciplinaire ou pour motiver un licenciement. En outre, l'employeur risque d'être sanctionné par la CNIL (en pourcentage du chiffre d'affaires) et encourt également des sanctions civiles et pénales pour atteinte à la vie privée (jusqu'à 1 an d'emprisonnement et 45 000 euros d'amende).

5. L'employeur peut exiger de recevoir la copie automatique de tous les messages écrits ou reçus par les salariés

FAUX

Le principe du secret des correspondances privées s'applique à la messagerie professionnelle du salarié, y compris lorsque l'employeur en a interdit l'utilisation à des fins personnelles.

Exiger d'être en copie de tous les courriels émis ou reçus par ses salariés porte forcément atteinte au droit au respect de la vie privée et des correspondances.

Il s'agit d'un procédé de surveillance manifestement excessif et qui n'est pas justifié.

6. L'employeur ne peut pas mettre en place un dispositif keylogger permettant d'enregistrer à distance toutes les actions effectuées sur un ordinateur

VRAI

Les logiciels keylogger permettent d'enregistrer toutes les frappes que le salarié effectue sur son ordinateur. Il s'agit donc d'un dispositif de contrôle particulièrement intrusif qui n'est pas autorisé sauf dans des hypothèses exceptionnelles, par exemple si l'employeur justifie d'un fort impératif de sécurité comme par exemple en cas de suspicion de divulgation des secrets industriels de l'entreprise ou d'acte de concurrence déloyale (communiqué CNIL, 20 mars 2013).

ATTENTION :

Est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende l'utilisation, mais aussi la vente, de certains dispositifs de captation de données informatiques à l'insu des personnes concernées (C. pén., art. 226-3).

7. L'employeur peut exiger du salarié qu'il communique son mot de passe

VRAI

Afin de garantir le respect des droits des salariés, mais également d'assurer une certaine traçabilité des interventions sur les outils informatiques de l'entreprise, la CNIL préconise que chaque salarié dispose d'un mot de passe individuel suffisamment complexe qui doit être changé tous les 3 mois.

La CNIL considère également que les identifiants et mots de passe (session Windows, messagerie, etc.) sont confidentiels et ne doivent pas être transmis à l'employeur.

Les mots de passe sont personnels et permettent de savoir ce qu'un utilisateur donné a pu faire sur le réseau de l'entreprise. Le fait d'utiliser le mot de passe de quelqu'un d'autre peut être préjudiciable au salarié.

Toutefois, les tribunaux considèrent que la communication du mot de passe d'un salarié à son employeur est possible dans certains cas particuliers.

L'employeur peut avoir connaissance du mot de passe d'un salarié absent si ce dernier détient sur son poste informatique des informations nécessaires à la poursuite de l'activité de l'entreprise et qu'il ne peut pas accéder à ces informations par d'autres moyens.

En effet, l'utilisation d'un mot de passe ne doit pas avoir pour effet de bloquer tout accès de l'employeur à l'outil informatique qu'il met à disposition du salarié.

L'ordinateur professionnel doit être accessible à l'employeur, que le salarié soit ou non présent sur le lieu de travail. Les documents, fichiers et messages qu'il contient sont d'ailleurs présumés être professionnels et l'employeur y a donc légitimement accès.

La Cour de cassation reconnaît que le licenciement pour faute grave des salariés qui refusent délibérément de communiquer leur mot de passe à l'employeur lorsqu'ils sont en congés ou en arrêt maladie est justifié lorsque cela révèle une volonté de bloquer le fonctionnement de l'entreprise (Cass. soc., 23 mai 2012, n° 11-11.522, et 19 février 2014, no 12-27.611).

Dès lors, un salarié qui refuse de communiquer son code est fautif dans la mesure où il entrave le bon fonctionnement de l'entreprise. L'utilisation du mot de passe ne doit en effet pas avoir pour fonction de soumettre l'accès aux fichiers à l'autorisation du salarié ni d'en interdire l'accès à l'employeur.

Cependant, attention, le fait d'utiliser le mot de passe du salarié pour accéder à son ordinateur ne permet pas pour autant à l'employeur de consulter les fichiers qui y ont été identifiés comme « personnels » ou « privés ». Ces derniers restent protégés par le principe de secret des correspondances privées.

8. L'employeur ne peut pas exiger du salarié qu'il réponde aux courriels en dehors de son temps de travail

VRAI

Les horaires de travail du salarié sont strictement encadrés et l'employeur ne peut exiger que le salarié accomplisse des tâches professionnelles en dehors de ce temps de travail.

Lorsque l'employeur impose malgré tout au salarié de répondre aux courriels professionnels en dehors du temps de travail, le salarié est en droit d'exiger le paiement de ces temps qui sont alors qualifiés d'heures supplémentaires.

Ainsi, le salarié s'il dispose des preuves de courriels reçus en dehors des heures de travail par copie d'écran peut obtenir un rappel de salaire au titre de ces heures supplémentaires et cela engendre également l'infraction de travail dissimulé.

Mais parfois la situation est moins évidente car c'est le salarié qui prend lui-même l'initiative de solliciter son employeur en dehors des heures de travail.

C'est la raison pour laquelle l'employeur a tout intérêt à encadrer les conditions d'utilisation des outils professionnels de communication qu'il met à disposition des salariés, afin d'éviter tout débordement.

Les sollicitations professionnelles en dehors des horaires de travail liés au NTIC se sont en effet multipliées et les contentieux sont nombreux, à la fois sur le terrain des heures supplémentaires, mais également sur celui du stress et de l'intrusion de la vie privée.

L'encadrement passe nécessairement par la mise en place de périodes de « trêve » des messageries professionnelles (courriels, mais également messagerie vocale, SMS, messagerie instantanée, etc.) qui correspondent au minimum au temps de repos du salarié.

Ce droit à la déconnexion est d'ailleurs imposé par la réglementation puisque les entreprises de 50 salariés et plus sont tenues de mettre en place des instruments de régulation de l'outil numérique.

Cette question est désormais intégrée à la négociation annuelle sur l'égalité professionnelle entre les femmes et les hommes, et sur la qualité de vie au travail.

Ces mesures visent à assurer le respect des temps de repos et de congés ainsi que l'équilibre entre vie professionnelle et vie personnelle et familiale.

9. L'employeur peut interdire toute utilisation personnelle des outils de communication de l'entreprise

FAUX

La CNIL estime que l'employeur ne peut pas interdire de manière générale et absolue l'utilisation du matériel informatique professionnel à des fins personnelles.

L'utilisation de ce matériel à des fins personnelles doit être raisonnable et, en ce qui concerne les connexions à Internet, les consultations ponctuelles de sites ne concernent, sur le lieu de travail, que ceux dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs.

La jurisprudence européenne a, quant à elle, réaffirmé le principe selon lequel « les instructions de l'employeur ne peuvent réduire à néant l'exercice de la vie privée sociale sur le lieu de travail » (CEDH, 5 septembre 2017, Req. 61496/08, Barbulescu/Roumanie, et 22 février 2018, Req. 588-13, Libert/France).

En l'espèce, réglementer ne veut donc pas dire interdire et il est bien évident que l'employeur a tout intérêt à encadrer l'utilisation de ces outils de manière à limiter et à réduire leur utilisation privée, que ce soit dans le règlement intérieur ou dans une charte informatique.

Il ne pourra en revanche y édicter une interdiction générale et absolue d'utilisation du matériel à des fins autres que professionnelles.

10. L'employeur ne peut pas consulter la clé USB personnelle du salarié

FAUX

Lorsque la clé USB du salarié est connectée à l'ordinateur professionnel, la même présomption que pour les fichiers et documents qui sont contenus dans le disque dur de cet ordinateur est applicable.

Dès lors que les fichiers qui sont stockés sur la clé USB ne sont pas identifiés comme personnels, l'employeur peut librement les consulter hors la présence du salarié (Cass. soc., 12 février 2013, n° 11-28.649).

ATTENTION :

La présomption du caractère professionnel ne s'applique pas lorsque la clé n'est pas connectée à l'ordinateur professionnel : l'employeur ne peut pas exiger de se la faire remettre pour en consulter le contenu. Il s'agit d'une violation à la fois du droit à la vie privée, mais également du droit de propriété (Cass. soc., 5 juillet 2017, n° 16-12.386).

11. Le salarié peut donner un caractère privé à l'intégralité des fichiers, courriels et documents contenus dans son ordinateur professionnel

FAUX

Renommer le disque dur de son ordinateur professionnel en « données personnelles » ne suffit pas pour conférer un caractère privé aux fichiers qui y sont contenus et bénéficier de la protection inhérente aux documents personnels (CEDH, 22 février 2018, n° 588/13).

En effet, le salarié ne peut pas utiliser à des fins privées l'intégralité du disque dur de l'ordinateur mis à sa disposition par l'employeur, qui est censé contenir en premier lieu des données professionnelles.

D'autre part, le terme de « données personnelles » est un terme générique qui peut désigner des dossiers professionnels traités personnellement par le salarié et pas forcément de manière explicite des éléments relevant de la vie privée.

Dans le même sens, dénommer un répertoire ou un fichier « Mes documents » ou par le prénom ou les initiales du salarié ne suffit pas à identifier son contenu comme personnel (Cass. soc., 21 octobre 2009, n° 07-43.877, 8 décembre 2009, n° 08-44.840, et 10 mai 2012, n° 11-13.884).

12. L'employeur ne peut sanctionner les propos tenus par le salarié sur des réseaux sociaux que si la page est ouverte au public

VRAI

Déterminer si les propos tenus par le salarié sur Internet ou sur les réseaux sociaux sont de nature publique ou privée donne lieu à un abondant contentieux.

La jurisprudence s'attache traditionnellement à vérifier le paramétrage du compte pour considérer que :

– lorsque les propos sont tenus sur une page ouverte au public, ils présentent un caractère public : l'employeur peut alors sanctionner le salarié qui tient des propos excessifs ou injurieux ;

– lorsque les propos, en revanche, sont tenus sur un page ou un réseau social dont l'accès a été restreint à un nombre limité de correspondants, ils relèvent de la sphère privée et ne peuvent pas être sanctionnés.

Ainsi, des propos injurieux tenus par une salariée sur sa directrice mais accessibles aux seules personnes agréées par l'intéressée, en nombre très restreint, ne constituent pas des injures publiques (Cass. 1re civ., 10 avril 2013, n° 11-19.530).

De même, lorsque les propos sont diffusés à travers un groupe privé, dont l'accessibilité est restreinte aux seuls membres et que ces derniers sont peu nombreux (par exemple 14 personnes), ils présentent un caractère privé et l'employeur ne peut pas les sanctionner (Cass. soc., 12 septembre 2018, n° 16-11.690).

Pour conférer un caractère privé aux propos tenus, la jurisprudence vérifie donc, outre les paramètres de confidentialité du compte, s'ils ont été diffusés ou non à un nombre restreint de personnes.

En effet, certains propos, même tenus dans le cadre d'un groupe fermé accessible uniquement à des personnes agréées, peuvent être diffusés à des dizaines voire des centaines de personnes. Dans ce cas, il est probable qu'en cas de contentieux le juge considère qu'ils aient perdu leur caractère privé.

La jurisprudence sanctionne de manière systématique toute intrusion de l'employeur dans la sphère privée du salarié.

L'employeur peut être condamné à des dommages et intérêts pour atteinte à la vie privée lorsqu'il tente de recueillir les propos tenus sur la page personnelle du salarié alors que ce dernier en a limité l'accès, par exemple lorsque l'employeur utilise le téléphone portable d'un autre salarié de l'entreprise qui a accès à ce réseau (Cass. soc., 20 décembre 2017, n° 16-19.609).

En revanche, la publication par un salarié d'images sur LinkedIn provenant de documents internes à l'entreprise, peut justifier son licenciement disciplinaire pour non-respect du secret professionnel et de l'obligation contractuelle de confidentialité figurant dans son contrat (CA Paris, 23 février 2022, n° 19/07192).

De même, en cas de licenciement sans cause réelle et sérieuse, les juges pourront utiliser la page LinkedIn du salarié pour évaluer le montant de dommages et intérêts (Cass. soc., 30 mars 2022, n° 20-21.665).

13. L'employeur peut écouter toutes les communications téléphoniques passées par le salarié sur son téléphone professionnel

VRAI

L'écoute en temps réel ou l'enregistrement sonore des appels téléphoniques passés par les salariés à leur poste de travail peuvent être réalisés en cas de nécessité et doivent être proportionnés aux objectifs poursuivis.

Ainsi, l'employeur peut installer un dispositif d'écoute et/ou d'enregistrement ponctuel 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, pour servir de preuves à l'établissement d'un contrat ou à l'accomplissement d'une transaction.

Cependant, il existe plusieurs limites au dispositif mis en place :

– les salariés doivent être préalablement informés, comme pour tout dispositif de surveillance, de même que les représentants du personnel ;

– l'employeur ne peut pas mettre en place ce dispositif en permanence (sauf lorsque c'est une obligation légale) : il ne peut donc enregistrer tous les appels y compris lorsque la finalité poursuivie est de lutter contre les incivilités ;

– l'employeur doit prévoir un dispositif permettant au salarié de couper l'écoute ou l'enregistrement pour les appels personnels ;

– les enregistrements doivent être conservés 6 mois maximum ;

– l'accès aux informations doit être limité aux personnes habilitées.

La CNIL préconise également que les salariés aient accès au compte rendu de la conversation enregistrée afin de pouvoir formuler des observations.

14. L'employeur ne peut pas coupler l'écoute des conversations téléphoniques à un système de capture de l'écran professionnel du salarié

VRAI

Le couplage des actions informatiques et des conversations téléphoniques consiste à enregistrer l'image de ce qui apparaît à l'écran de l'ordinateur du salarié à travers des captures d'écran, parallèlement à l'enregistrement des conversations téléphoniques.

Ce dispositif peut toutefois conduire à capter par inadvertance des éléments d'ordre privé (courriels personnels, conversations de messageries instantanées, etc.).

C'est la raison pour laquelle la CNIL l'interdit et considère en effet que, quelle que soit la finalité poursuivie, une capture d'écran est susceptible de n'être ni pertinente ni proportionnée puisqu'il s'agit d'une image figée d'une action isolée de l'employé, qui ne reflète pas fidèlement son travail.

En revanche, est autorisé le couplage entre l'enregistrement des conversations téléphoniques et l'enregistrement vidéo de l'écran, sous certaines conditions strictes et uniquement lorsqu'il est utilisé pour le seul objectif de formation du personnel.

Il est alors impératif que l'enregistrement vidéo se déclenche au décrochage du combiné téléphonique et s'achève dès le raccrochage.

15. Les enregistrements « tampons » constituent une pratique licite

VRAI

Il s'agit même d'une pratique recommandée par la CNIL.

Cela consiste pour l'employeur ou la personne habilitée à écouter les enregistrements dans les jours suivant leur réalisation et à rédiger les documents d'analyse nécessaires.

Les enregistrements sont alors supprimés et l'employeur ne conserve que les documents d'analyse qui les retracent.

16. L'employeur ne peut pas contrôler les communications des représentants du personnel

VRAI

L'employeur ne peut pas contrôler les conversations téléphoniques des représentants du personnel et syndicaux : ces derniers doivent disposer d'une ligne téléphonique déconnectée de tout autocommutateur puisque l'employeur n'a pas le droit d'intercepter les communications ni d'identifier les correspondants des représentants du personnel (Cass. soc., 4 avril 2012, n° 10-20.845).

L'employeur, de ce fait, ne peut pas non plus analyser les relevés téléphoniques des lignes utilisées par les représentants du personnel.

Toutefois, le droit à la confidentialité est limité aux communications téléphoniques passées par les salariés protégés dans le cadre de leur mission légale.

L'employeur peut en revanche tout à fait contrôler et intercepter les communications passées par le salarié pour accomplir son travail et en identifier les correspondants.

En pratique, le salarié protégé disposera de deux lignes téléphoniques : la première utilisée pour accomplir son travail et que l'employeur peut contrôler, la seconde exclusivement utilisée pour exercer les missions légales dont il est investi, pour laquelle la confidentialité s'applique.

ATTENTION :

La mise en place de ce système de contrôle peut constituer pour le salarié protégé un changement des conditions de travail qui nécessite de recueillir son accord.

EXEMPLE :

Le recours à un nouveau logiciel équipé d'un système de double écoute destiné à vérifier la qualité des interventions téléphoniques d'un salarié protégé qui exerce les fonctions de conseiller commercial constitue un changement des conditions de travail et ne peut pas être imposé par l'employeur (Cass. soc., 13 décembre 2017, n° 15-29.116).

17. L'employeur peut contraindre le salarié à présenter un badge pour accéder aux locaux de l'entreprise

VRAI

L'employeur peut mettre en place des outils de contrôle individuel de l'accès aux locaux de l'entreprise pour sécuriser l'entrée dans les bâtiments ou les locaux qui font l'objet d'une restriction de circulation. Ces dispositifs concernent aussi bien les salariés que les visiteurs. La CNIL autorise même la mise en œuvre de dispositifs biométriques.

L'employeur peut également mettre en place des dispositifs pour gérer les horaires et le temps de travail des salariés. Ces dispositifs ne peuvent pas, en revanche, être biométriques.

ATTENTION :

Les salariés doivent être préalablement informés, comme pour tout dispositif de surveillance, de même que les représentants du personnel.

Le système mis en place ne doit pas servir au contrôle des déplacements à l'intérieur des locaux (sauf exception tenant à la sécurité : site nucléaire, chimique, etc.).

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

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

Les données relatives aux accès doivent être supprimées 3 mois après leur enregistrement et les données utilisées pour le suivi du temps de travail doivent être conservées pendant 5 ans.

18. Les caméras de vidéosurveillance ne doivent pas filmer les espaces de pause ou de repos ni les salariés à leur poste de travail

VRAI

Le dispositif de vidéosurveillance doit répondre à l'objectif précis d'assurer la sécurité des biens et des personnes. Il ne doit pas être utilisé pour contrôler les faits et gestes des salariés.

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.

En revanche, elles ne doivent pas filmer les salariés sur leur poste de travail, sauf circonstances particulières : employé de banque qui manipule de l'argent par exemple, entrepôt stockant des biens de valeurs où travaillent des manutentionnaires. Dans ce cas particulier, la caméra doit s'attacher à filmer davantage la zone à sécuriser, la caisse, que le salarié).

Les caméras ne doivent pas non plus être installées dans les zones de pause, repos et les toilettes.

Il est également interdit de filmer dans les locaux syndicaux ou ceux réservés aux représentants du personnel.

Même lorsque le salarié est filmé sur son poste de travail, le dispositif de vidéosurveillance ne doit pas filmer en continu le salarié, sauf en cas de circonstances particulières liées à la prévention des atteintes aux biens et aux personnes. En soi, la vidéosurveillance d'un salarié filmé en continu pour contrôler le respect des règles d'hygiène et le temps de travail dans un lieu où il travaille seul est disproportionnée.

19. Les caméras de vidéosurveillance peuvent comporter des microphones

FAUX

Le dispositif de vidéosurveillance doit répondre à l'objectif précis d'assurer la sécurité des biens et des personnes. Son utilisation doit être proportionnée au but recherché.

Il n'est donc pas judicieux, en plus de filmer, de prévoir une écoute ou un enregistrement sonore des locaux.

Ce dispositif est particulièrement intrusif pour les salariés et ne présente, sauf exception, aucun intérêt au regard de l'impératif de sécurité poursuivi.

C'est la raison pour laquelle la CNIL a sanctionné à plusieurs reprises des dispositifs de vidéosurveillance qui associaient l'enregistrement de l'image et du son car elle a considéré que la finalité poursuivie était en réalité de surveiller les salariés et d'écouter leurs conversations.

EXEMPLE :

Une entreprise met en œuvre un dispositif comportant huit caméras, (chacune équipée d'un microphone permettant l'écoute sonore et d'un haut-parleur) filmant huit salariés, soit une caméra par salarié. Ce dispositif est manifestement excessif, puisque le dirigeant de la société place ses salariés sous une surveillance constante et permanente.

20. Seul le responsable sécurité de l'entreprise a accès aux images de vidéosurveillance

VRAI et FAUX

Seules les personnes habilitées par l'employeur, dans le cadre de leurs fonctions, peuvent visionner les images enregistrées dans le cadre du dispositif de vidéosurveillance.

Ce dispositif répondant à un objectif de sécurité, c'est donc les personnes qui sont responsables de cette question au sein de l'entreprise qui ont accès aux images : responsable sécurité, gardien, etc.

Lorsque l'entreprise ne dispose pas de service spécifique lié à la sécurité, il est toutefois admis que ce soit l'employeur en personne qui visionne les images.

ATTENTION :

Dans tous les cas, ces personnes doivent être formées et sensibilisées aux modalités de mise en œuvre du dispositif.

De manière générale, vous ne pouvez pas utiliser le droit à l'image du salarié (photographies, vidéos) sans avoir recueilli son consentement, qu'il s'agisse de supports internes à l'entreprise (trombinoscope, intranet, affiches, etc.) ou de supports destinés à des fins commerciales ou publicitaires (site internet, dépliant, poster, campagne de communication, etc.). Dans tous les cas, le salarié a droit à des dommages et intérêts si son consentement n'a pas été recueilli. Cette règle s'applique également aux anciens salariés.

21. Le dispositif de géolocalisation du véhicule ne peut pas être utilisé pour contrôler les horaires de travail des salariés et le respect des limitations de vitesse

VRAI et FAUX

Le contrôle d'un salarié par un système de géolocalisation permet à l'employeur de collecter un certain nombre de données par le biais du système GPS.

La CNIL admet que ce dispositif soit mis en place pour divers objectifs :

– faciliter le suivi des prestations réalisées par l'entreprise ;

– assurer la sécurité des salariés ou des marchandises transportées ;

– respecter une obligation légale ou réglementation (en fonction de la nature des biens transportés) ;

– améliorer l'organisation des déplacements au sein de l'entreprise (optimiser les tournées des techniciens par exemple) ;

– contrôler les règles d'utilisation du véhicule mis à disposition du salarié (notamment lorsque l'employeur en interdit l'usage privé).

En ce qui concerne le contrôle des horaires de travail, la CNIL admet que la géolocalisation puisse être utilisée pour suivre le temps de travail du salarié lorsque cela ne peut pas être réalisé par un autre moyen (CE, 15 décembre 2017, n° 403776, et Cass. soc., 19 décembre 2018, n° 17-14.631).

EXEMPLES :

Une entreprise qui contrôle la durée des temps d'intervention des techniciens itinérants à partir de leur déclaration d'intervention et dispose, en cas de doute, de la possibilité de les corroborer en interrogeant ses clients pour vérifier les heures d'arrivée et de départ des salariés ne peut pas mettre en place un dispositif de géolocalisation au motif que ce dernier constitue un moyen de contrôle plus efficace.

De même, le seul fait qu'un système autodéclaratif et un mécanisme de contrôle du temps de travail par un responsable ne soient pas adaptés au but recherché ne suffit pas à justifier le recours à la géolocalisation.

ATTENTION :

Dans tous les cas, ce dispositif ne peut toutefois pas être mis en place pour les salariés qui disposent d'une liberté dans l'organisation de leur travail (salariés en forfait jours par exemple), pour lesquels l'employeur n'a pas à contrôler les horaires de travail.

Enfin, il est par ailleurs interdit d'utiliser la géolocalisation pour contrôler le respect des limitations de vitesse.

Sachez que le chronotachygraphe (appareil de contrôle installé dans un véhicule de transport routier, qui enregistre la vitesse et le temps de conduite du véhicule) ne présente pas la même finalité que la géolocalisation. Il constitue un dispositif de traitement automatisé des données à caractère personnel et doit être déclaré à la CNIL. Cependant, la jurisprudence considère que l'absence de déclaration ne prive pas l'employeur du droit d'utiliser les données produites par l'appareil pour, par exemple, sanctionner le salarié. En effet, l'installation de chronotachygraphes dans les véhicules de transport routier est obligatoire, en vertu d'une réglementation européenne, sous peine de sanctions pénales, et les salariés ne peuvent prétendre en conséquence en ignorer l'existence.

En revanche, la mise en place d'un chronotachygraphe dans un véhicule qui n'est pas assujetti à l'obligation d'en posséder un (véhicule non destiné au transport routier), doit faire l'objet d'une information des salariés.

22. L'employeur peut utiliser les données de géolocalisation pour sanctionner le salarié

VRAI

Il importe cependant que le dispositif ait été mis en œuvre régulièrement.

En effet, préalablement à la mise en place du système de géolocalisation, l'employeur doit en informer les salariés concernés, de manière individuelle, ainsi que les représentants du personnel.

La finalité du traitement, les catégories de données de localisation traitées, la durée de conservation de ces données, les destinataires des données, l'existence d'un droit d'accès et de rectification et d'un droit d'opposition et leurs modalités d'exercice doivent être portés à la connaissance des salariés.

De plus, un système de géolocalisation ne peut pas être utilisé par l'employeur pour d'autres finalités que celles qui ont été portées à la connaissance des salariés. Si tel est le cas, le dispositif n'est pas conforme.

Lorsque les formalités d'information n'ont pas été respectées ou que le dispositif n'est pas conforme au RGPD l'employeur ne peut pas prendre de sanction disciplinaire fondée sur les données issues de la géolocalisation.

EXEMPLE :

Est sans cause réelle et sérieuse le licenciement fondé sur des données de géolocalisation recueillies de manière illicite et utilisées par l'employeur pour démontrer la présence du salarié dans l'entreprise lors de connexions Internet sur des sites pornographiques. En l'espèce, le dispositif de géolocalisation n'avait pas été soumis à la consultation des représentants du personnel, n'avait pas fait l'objet d'une information individuelle préalable des salariés (Cass. soc., 3 octobre 2018, n° 16-23.968).

23. L'employeur peut imposer le télétravail

VRAI et FAUX

Le télétravail est une forme d'organisation qui permet à un salarié de travailler ailleurs que dans les locaux de son entreprise, de manière régulière et volontaire, grâce aux technologies de l'information et de la communication (TIC).

Il peut être mis en place dans le cadre d'un accord collectif ou, à défaut, dans le cadre d'une charte élaborée par l'employeur après avis du comité social et économique (CSE) s'il existe.

Il reste toutefois possible de mettre en place le télétravail sans accord collectif ni charte, par accord entre l'employeur et le salarié.

En effet, si vous êtes d'accord avec votre salarié pour qu'il fasse du télétravail, vous pouvez formaliser cet accord par tout moyen (contrat de travail, lettre, e-mail, etc.).

Que ce soit lors de l'embauche ou en cours d'exécution du contrat, le télétravail ne peut pas être imposé au salarié.

Afin d'éviter tout litige, il est toutefois recommandé de prévoir le télétravail dans le contrat de travail (télétravail dès l'embauche) ou dans un avenant (télétravail en cours de contrat).

Il existe cependant des circonstances exceptionnelles qui permettent à l'employeur, de manière temporaire, de mettre en place le télétravail sans avoir à recueillir l'accord du salarié pour assurer la continuité de l'activité de l'entreprise et garantir la protection des salariés : épidémies, intempéries, pics de pollution, inondations, etc. Mais cette situation est exceptionnelle.

Ainsi, dans le cadre de la crise sanitaire liée à l'épidémie de coronavirus, la mise en œuvre du télétravail a été impérative lors des périodes de confinement puis de reprise épidémique.

24. En cas de télétravail, l'employeur ne peut pas installer de dispositif de surveillance du domicile du salarié

FAUX

Dans le cadre de la mise en place du télétravail, l'employeur peut prévoir des modalités de contrôle du temps et de régulation de la charge de travail, ainsi que les plages horaires durant lesquelles il peut habituellement contacter le télétravailleur (systèmes autodéclaratifs (par le biais d'un logiciel de gestion des horaires installés sur l'ordinateur), systèmes de surveillance informatisés destinés à calculer le temps de connexion, etc.).

Si un système de surveillance des salariés est mis en place, il doit être pertinent et proportionné au but recherché, et le dispositif doit faire l'objet d'une consultation des représentants du personnel et de l'information préalable du salarié.

Ainsi, même en cas de télétravail, le dispositif de contrôle doit répondre aux mêmes exigences que s'il avait été mis en place dans l'entreprise.

Lorsque le salarié travaille depuis son domicile, l'employeur est chargé de fournir, d'installer et d'entretenir les équipements nécessaires pour assurer un travail régulier, sauf si le salarié utilise son propre matériel.

Dans ces conditions, l'accès au domicile personnel du salarié peut s'imposer mais l'employeur doit en faire au préalable la demande par écrit et le salarié devra donner son accord.

En toute hypothèse, le domicile du salarié faisant partie intégrante de l'intimité de la vie privée, la mise en œuvre de la demande d'accès de l'employeur ne peut pas porter atteinte au droit du salarié à mener une vie personnelle et familiale normale.

25. L'employeur peut avoir accès au dossier pénal du salarié

VRAI et FAUX

Il convient de distinguer le casier judiciaire qui porte la mention des éventuelles condamnations pénales de la personne et l'éventuel dossier pénal, ouvert en cas d'infraction constatée, de suspicion d'infraction, de poursuite devant un tribunal ou de mesure d'instruction judiciaire.

Il n'existe pas de texte spécifique prévoyant ou interdisant la vérification des casiers judiciaires des salariés, et l'employeur peut donc demander à un candidat ou à un salarié de produire l'extrait de son casier lors d'un entretien, par exemple afin de vérifier ses antécédents judiciaires.

Toutefois, il ne peut pas en conserver une copie ni permettre que ces données fassent l'objet d'un traitement spécifique. La CNIL recommande ainsi que la mention des vérifications des casiers effectuées dans le fichier de gestion du personnel soit indiquée sous la forme « oui/non ».

ATTENTION :

Certains métiers dits « sensibles » organisent de manière un peu plus stricte une procédure de vérification, par l'employeur ou par certaines autorités délivrant des agréments (par exemple, pour les agents de sécurité ou les assistantes maternelles), des casiers judiciaires des salariés (bulletins B2 ou B3). Ces procédures peuvent ainsi prévoir la durée pendant laquelle l'employeur est tenu de conserver l'extrait du casier judiciaire (une durée de 3 mois est communément retenue). En l'absence de précisions dans le texte, le document ne doit pas être conservé.

En ce qui concerne le dossier pénal l'analyse est différente. En cas d'infraction, de poursuite pénale ou de mise en examen, l'employeur ne peut pas avoir accès au dossier pénal du salarié sauf dans l'hypothèse où ce dossier mentionne des faits commis dans le cadre de son travail.

Dans ce cas, l'employeur peut alors y avoir légitimement accès, et ce, pour différentes raisons :

– soit parce qu'il est victime ou partie civile (par exemple, en cas de détournement par le salarié de fonds de l'entreprise) ;

– soit parce qu'il est entendu comme coauteur des faits (par exemple en cas d'accident impliquant un manquement à la sécurité).

INNOVATION RH

Tissot Social Entreprise ACTIV

La solution de droit du travail la plus complète du marché.

Dans le cadre de l'abonnement à **Tissot Social Entreprise ACTIV**, accédez à :

- + de 120 dossiers thématiques
- les **procédures** et documents interactifs
- le **Code du travail** et l'accès à plus de 6 000 textes officiels
- 1 **convention collective**
- la base de **modèles**
- les **alertes** de mise à jour

Votre allié pour une gestion du personnel facilitée !

Accédez à la base complète de dossiers

Ayez une vision globale et approfondie
Plus de 120 dossiers classés par thèmes, pour maîtriser l'ensemble des informations à connaître sur un sujet concret.

Obtenez des réponses personnalisées

Laissez-vous guider
Les procédures interactives vous apportent une réponse personnalisée car chaque cas est unique, chaque situation différente.

Sécurisez vos décisions

Soyez sereins
Vous êtes sûr(e) de respecter la réglementation en vigueur grâce aux mises à jour permanentes de nos contenus.

Passez à l'action avec Tissot Social Entreprise ACTIV, rendez-vous maintenant sur : https://tiss.fr/se

Pour aller plus loin

Aux Éditions Tissot nous proposons aussi…

- **Les dossiers traitant d'un sujet précis.**
- **Les supports de communication à distribuer ou à afficher.**
- **Tissot Information Juridique par téléphone.**
- **Les conventions collectives les plus à jour du marché.**
- **Les affiches et registres obligatoires.**
- **L'assistant RH dont vous avez toujours rêvé !**

TISSOT éditions

Pour plus d'infos rendez-vous sur
www.editions-tissot.fr
Tél. : 04 50 64 08 08 - commercial@editions-tissot.fr
editionstissot @editionstissot Editions Tissot