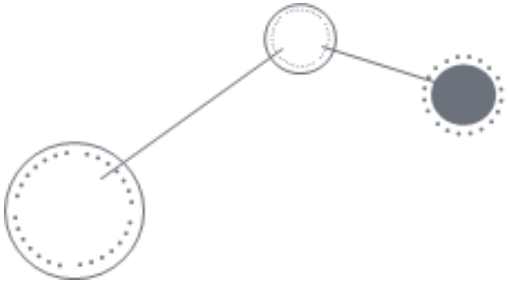

3 sujets en droit du travail à connaître et à maîtriser

chapitre1

Introduction

Matière complexe, sujet aux changements et aux interprétations, le droit du travail nécessite une veille constante, source de charge de travail.

Pour vous aider, ce document aborde dans le détail 3 thématiques majeures à connaître pour les salariés et les représentants du personnel :

1. Le droit de contrôle de l’employeur sur les salariés
2. La gestion de l’accident du travail
3. Inaptitude d’un salarié : l’absence de reclassement

Sommaire

1. Le droit de contrôle de l’employeur sur les salariés

2. La gestion de l’accident du travail

3. Inaptitude d’un salarié : l’absence de reclassement

1. Le droit de contrôle de l'employeur sur les salariés

Afin de garantir la bonne marche de son entreprise, l'employeur contrôle la bonne exécution du travail par les salariés.

L'essor des nouvelles technologies lui offre un large éventail de procédés de contrôle et de surveillance tels que les caméras vidéo, les autocommutateurs, les badges électroniques, etc. Il doit cependant veiller au respect de certaines conditions lors de la mise en œuvre de ces moyens, afin de ne pas porter atteinte aux libertés individuelles des salariés.

De façon générale, le contrôle de l'employeur sur les salariés ne peut pas s'opérer par un stratagème ou un dispositif de surveillance clandestin qui sera considéré comme déloyal.

Exemples

*L'employeur ne peut pas missionner de faux clients pour venir constater les compétences professionnelles d'un salarié vendeur, ou encore pour venir constater que le salarié exerce une autre activité dans un restaurant (**Cass. soc., 18 mars 2008, n° 06-45.093**). Il ne peut pas non plus organiser un stratagème pour piéger le salarié à son insu (**Cass. soc., 19 novembre 2014, n° 13-18.749** : cas de l'employeur qui organise une mise en*

scène à l'aide d'un faux client et d'un autre salarié de l'entreprise pour piéger une vendeuse en parfumerie).

*Il ne peut pas faire appel à une société de surveillance pour contrôler l'utilisation des distributeurs de boissons et de sandwichs (**Cass. soc., 15 mai 2001, n° 99-42.219**) ou à un détective privé pour faire suivre les salariés (**Cass. soc., 4 février 1998, n° 95-43.421)**.*

*De même, il ne peut pas utiliser des lettres piégées, diffusant une encre bleue en cas d'ouverture, à l'insu d'un salarié facteur, pour prouver que ce dernier ouvre les lettres (**Cass. soc., 4 juillet 2012, n° 11-30.266**).*

En revanche, l'employeur peut de façon licite :

- organiser la surveillance d'un salarié sur les lieux de travail par son supérieur hiérarchique, même en l'absence d'information préalable du salarié (***Cass. soc., 26 avril 2006, n° 04-43.582***) ;
- organiser un simple contrôle de l'activité d'un salarié par l'employeur ou par un service interne à l'entreprise chargé de cette mission, même en l'absence d'information et de consultation préalable du comité d'entreprise (CSE à terme) (***Cass. soc., 4 juillet 2012, n° 11-14.241, et 5 novembre 2014, n° 13-18.427*** : cas d'un

rapport d'enquête réalisée par des cadres dans une entreprise de transports en commun pour mesurer la pénibilité du travail, qui peut être utilisé pour sanctionner un contrôleur de bus qui s'absente de son poste pendant son temps de travail).

1/ La collecte d'informations personnelles sur le salarié

Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance à un syndicat, ou des informations relatives à la santé ou à la vie sexuelle des salariés.

De même, l'employeur ne peut pas imposer aux salariés, dans le règlement intérieur de l'entreprise, d'indiquer tout changement dans leur situation familiale (**circ. DRT 91/17 du 10 septembre 1991**).

En revanche, la question de la validité de la clause du contrat de travail imposant au salarié d'informer l'employeur de tout changement de sa situation personnelle (notamment les changements d'adresse, d'état civil ou de situation familiale) n'est pas définitivement tranchée par la jurisprudence : en effet, une décision de la cour d'appel de Versailles considère que ces clauses sont illicites (***CA Versailles, 14 octobre 2015, n° 14/01865***), alors

que la même juridiction avait admis une solution inverse auparavant : au sujet d'une clause prévoyant l'obligation pour le salarié d'informer l'employeur d'un changement d'adresse (***CA Versailles, 11 février 1993, n° 92/2873***).

La Commission nationale de l'informatique et des libertés (CNIL) estime ainsi que la collecte des informations suivantes n'est pas pertinente :

- la date d'entrée en France ;
- la date de naturalisation ;
- les modalités d'acquisition de la nationalité française ;
- la nationalité d'origine ;
- les numéros d'immatriculation ou d'affiliation aux régimes de Sécurité sociale ;
- le détail de la situation militaire sous la forme « objecteur de conscience, ajourné, réformé, motifs d'exemption ou de réformation, arme, grade » ;
- l'adresse précédente ;
- l'entourage familial du candidat (nom, prénom, nationalité, profession et employeur du conjoint, ainsi que nom, prénom, nationalité, profession, employeur des parents, des beaux-parents, des frères et sœurs, et des enfants) ;
- l'état de santé, la taille, le poids, la vue ;

- les conditions de logement (propriétaire ou locataire) ;
- la vie associative ;
- la domiciliation bancaire, les emprunts souscrits, les défauts de paiement.

Le **règlement du Parlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel** et à la libre circulation de ces données met en place un nouvel acteur, le « *délégué à la protection des données* » (DPO)

Il remplace le correspondant informatique et libertés dont la désignation était facultative.

Contrairement au correspondant informatique et libertés, le délégué à la protection des données est obligatoirement désigné dans toutes les entreprises :

- dont les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leur finalité, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- ou dont les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données

à caractère personnel et de données relatives à des condamnations pénales et à des infractions.

Sa désignation est obligatoire depuis le 25 mai 2018.

Depuis cette date, toutes les entreprises de plus de 250 salariés ont l'obligation de tenir un registre des traitements de données.

Les entreprises de moins de 250 salariés bénéficient d'une dérogation : elles ne doivent tenir un registre que lorsqu'il existe dans l'entreprise des traitements non occasionnels, des traitements susceptibles de comporter un risque pour les droits et libertés des personnes, et des traitements qui portent sur des données sensibles.

Les salariés doivent être informés par tout moyen du traitement de leurs données personnelles.

Cette information porte notamment sur les modalités du traitement, sa finalité, les destinataires des données, la durée de conservation, et le droit d'accès à ces informations.

Ainsi, le traitement automatisé des données à caractère personnel permettant d'assurer un suivi de l'activité journalière et des événements liés à l'exploitation de la flotte d'un aéroport est licite dès lors que les salariés ont été informés préalablement de l'existence de ce traitement, de sa finalité, des destinataires des données collectées, et de leurs droits

d’accès, de rectification et de suppression dès sa date de création, que le dispositif ne comporte aucune donnée portant sur d’éventuelles sanctions, et qu’aucun rapprochement entre les données collectées et celles permettant de gérer les dossiers professionnels des salariés n’est effectué (***Cass. soc., 13 juin 2018, n° 16-25.301***).

La CNIL recommande d’intégrer un rappel des règles de protection des données personnelles dans le règlement intérieur.

2/ Le contrôle des vestiaires, bureaux et effets personnels des salariés

L’employeur peut faire procéder à des fouilles des armoires ou des vestiaires, ou à la fouille corporelle, à condition qu’elles soient motivées par l’intérêt légitime de l’entreprise :

- pour des raisons de sécurité collective ;
- ou justifiées par la recherche d’objets volés.;

Le consentement du salarié est nécessaire, et il doit être averti de son droit d’opposition à un tel contrôle ainsi que de son droit d’exiger la présence d’un témoin (autre membre du personnel). En cas de refus du salarié, vous devez recourir à un officier de police judiciaire, seul habilité à procéder à la fouille.

Le salarié doit impérativement être informé du droit de s'opposer à l'ouverture de ses effets personnels ou d'exiger la présence d'un témoin : à défaut, le licenciement pour faute grave en raison du vol commis sera jugé sans cause réelle et sérieuse, car la preuve irrégulièrement obtenue ne pourra pas être utilisée par l'employeur (***CA Paris, 11 septembre 2013, n° 11/10392).***

Une clause prévoyant que la direction se réserve le droit de faire ouvrir à tout moment les armoires individuelles des salariés ne peut pas figurer dans le règlement intérieur car elle porte atteinte aux droits des personnes et aux libertés individuelles (***CE, 12 juin 1987, n° 72388***).

Un employeur qui fouille une armoire individuelle à l'insu du salarié et sans raison légitime ne peut pas invoquer les résultats de cette fouille comme preuve d'une faute, cette preuve ayant été obtenue de façon illicite :

Jurisprudence

- *l'employeur ne peut procéder à l'ouverture de l'armoire individuelle d'un salarié que dans les cas et conditions prévus par le règlement intérieur, et en présence de l'intéressé ou après l'en avoir informé. À défaut, le licenciement d'un salarié prononcé pour détention de canettes de bière à l'intérieur de*

*son armoire personnelle est dépourvu de cause réelle et sérieuse (**Cass. soc., 11 décembre 2001, n° 99-43.030**).*

- *l'employeur ne peut pas écouter les enregistrements réalisés par un salarié sur son dictaphone personnel en son absence, et utiliser ces derniers à l'appui d'un licenciement disciplinaire (**Cass. soc., 23 mai 2012, n° 10-23.521**).*
- *en revanche, répond aux exigences posées par la loi l'ouverture d'un casier opérée par un employeur en présence d'un représentant du personnel, le salarié ayant été informé 3 semaines à l'avance de l'ouverture de son casier, et les partenaires sociaux ayant été avertis. En conséquence, le résultat de la fouille (détention illicite d'objets publicitaires appartenant à l'entreprise) peut être retenu à l'encontre du salarié et constitue une cause réelle et sérieuse de licenciement (**Cass. soc., 15 avril 2008, n° 06-4.902**).*

Toutefois, la présence et le consentement du salarié ne sont pas nécessaires lorsque l'employeur contrôle un coffre individuel permettant le dépôt des fonds de caisse, donc affecté à un usage exclusivement professionnel, dès lors que les possibilités de contrôle de celui-ci par l'employeur sont prévues par le règlement intérieur (***Cass. soc., 2 février 2011, n° 09-68.719***).

De même, les documents et dossiers papier qui sont détenus par les salariés dans un bureau de l'entreprise peuvent être librement consultés par l'employeur, sauf s'ils sont identifiés comme personnels ou privés, ou encore s'ils sont contenus dans un tiroir ou une armoire fermée à clé (***Cass. soc., 4 juillet 2012, n° 11-12.330***).

Enfin, lorsque le salarié indique que le casier dont l'ouverture lui est demandée n'est pas le sien, l'employeur peut procéder à l'ouverture, même hors de sa présence, sans qu'une infraction au règlement intérieur ni aux droits du salarié ne puisse être invoquée (***Cass. soc., 31 octobre 2013, n° 12-18.993***).

Par ailleurs, les fichiers clients ne doivent pas contenir de commentaires excessifs : bien souvent, en effet, ces derniers contiennent une zone de libre expression où les salariés ont la possibilité d'inscrire leurs commentaires. Une décision de la CNIL rappelle que si le recours à l'utilisation de zones de commentaires libres n'est pas interdit dans la mesure où il permet un suivi des dossiers des clients, les informations renseignées doivent être objectives et en relation avec la prestation commerciale. En particulier, elles ne doivent pas porter atteinte à l'image de la personne. Il appartient à l'entreprise de prendre toutes les mesures pour que leurs salariés respectent effectivement ces règles. En l'espèce, l'entreprise a été mise en demeure par la CNIL de se conformer à la loi dans un délai de 3 mois car ses fichiers comportaient de nombreux commentaires excessifs sur ses clients, par

exemple : « n’a pas de cerveau », « cliente avec problème cardiaque », « client alcoolique », ou encore des propos insultants (***décision CNIL n° 2015-063 ; communiqué CNIL du 23 juillet 2015***).

3/ Le contrôle par vidéosurveillance

Le contrôle par vidéosurveillance n’est pas réglementé par le droit du travail. Une seule indication nous est donnée concernant l’obligation d’informer et de consulter le CSE préalablement à la décision de mise en œuvre des moyens et techniques permettant le contrôle des salariés (C**. trav., art. L. 2323-47**).

Selon le ministère du Travail, le contrôle par vidéosurveillance est accepté s’il est justifié par des préoccupations de sécurité.

La CNIL rappelle également que l’installation d’un dispositif de vidéosurveillance sur les lieux de travail doit être motivée par un objectif de sécurité. En effet, les 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.

L’objectif premier de la vidéosurveillance n’est donc pas de contrôler les horaires et l’activité des salariés. Le dispositif de vidéosurveillance ne doit pas filmer en continu les postes de travail des salariés, sauf en cas de circonstances particulières liées à la prévention des atteintes aux biens et aux personnes.

La présence de caméras filmant l’accès aux salles de pause des salariés n’est pas autorisée car elles surveillent les entrées et sorties d’un espace dédié au temps libre de ces derniers (***CNIL, décision n° 2014-001 du 15 janvier 2014***, et communiqué du 3 février 2014 sur les conditions de mise en œuvre des dispositifs biométriques et de vidéosurveillance).

Qui plus est, la CNIL, au-delà de la finalité du dispositif de surveillance, vérifie systématiquement :

- si l’information des personnes surveillées a été suffisante ;
- si la durée de conservation des données n’est pas excessive ;
- si l’accès à ces données est sécurisé (***CNIL, décision n° 2013-029 12 juillet 2013, et communiqué du 12 septembre 2013***).

Cela étant, les tribunaux se sont positionnés à l’égard de la validité de la vidéosurveillance comme mode de preuve pour sanctionner un salarié.

Ainsi, un tel dispositif est licite (c'est-à-dire légal) pour contrôler et surveiller l'activité des salariés pendant leur temps de travail, à condition que ces derniers aient été informés préalablement par l'employeur.

Par conséquent, est dépourvu de cause réelle et sérieuse le licenciement d'un salarié dès lors que l'employeur a déposé plainte pour des faits de vols en se fondant sur les images de la vidéosurveillance, et que l'audition du salarié par les services de gendarmerie est consécutive à cette exploitation des images de vidéosurveillance, illicite en raison de l'absence d'information du salarié sur l'existence de ce système de surveillance (***Cass. soc., 20 septembre 2018, n° 16-26.482***). En revanche, l'utilisation de l'enregistrement vidéo par l'employeur, à titre de preuve dans le litige l'opposant à un salarié, ne présente pas un caractère illicite dans la mesure où ce salarié ne pouvait pas ignorer que son image pouvait faire l'objet d'une captation au moyen d'un dispositif de surveillance qui n'était ni clandestin ni déloyal. En effet, des affiches informaient le public aux entrées du magasin que le site était placé sous vidéoprotection, le système de vidéosurveillance avait été autorisé par arrêté préfectoral et déclaré à la CNIL, et les représentants du personnel avaient été informés et consultés sur le dispositif (***Cass. soc., 7 novembre 2018, n° 16-26.126***).

Lorsque les caméras permettent également de collecter le son, l'employeur doit en informer les salariés (***CNIL, décision n° 2014-001 du 15 janvier 2014, et communiqué du 3 février 2014***).

La CNIL rappelle les modalités de mise en place d'un dispositif de vidéosurveillance : avant toute mise en place du dispositif, les représentants du personnel doivent être consultés et les salariés informés de façon personnelle (avenant au contrat de travail ou par une note de service, par exemple).

Une simple information orale par le chargé de recrutement ne suffit pas, et la CNIL estime en outre que l'information doit être réalisée dès la mise en place du dispositif pour les salariés présents, et dès l'entretien d'embauche pour les salariés nouvellement embauchés (***CNIL, délibération n° 2013-139 du 30 mai 2013***).

Depuis l'entrée en vigueur du **règlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)**, l'employeur n'est plus tenu de déclarer ce dispositif à la CNIL. Cependant, du fait que ce traitement risque de porter atteinte aux droits et aux libertés des salariés, l'employeur doit réaliser une étude d'impact complète préalablement à sa mise en place.

Lorsque les caméras sont installées dans un lieu ou un établissement ouvert au public (commerce, zone marchande, par exemple), l'installation de la vidéosurveillance nécessite l'obtention d'une autorisation préfectorale prise après avis de la commission départementale de la vidéoprotection.

Dans les lieux dits « mixtes », c'est-à-dire un lieu ouvert au public qui comporte également des zones privées (par exemple un supermarché), l'employeur doit également saisir le préfet (**circ. du Premier ministre du 14 septembre 2011**).

Les caméras peuvent être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation, des zones où de la marchandise ou des biens de valeur sont entreposés. En revanche, elles ne doivent pas filmer :

- les employés sur leur poste de travail, sauf circonstances particulières (caissier, entrepôt stockant des biens de valeur, etc.) ;
- les espaces de pause, de repos, et les toilettes ;
- les locaux syndicaux et ceux des représentants du personnel (y compris leur accès) ;
- les accès aux zones réservées au personnel (vestiaires, salle de repos).

Seules les personnes habilitées, et dans le cadre de leurs fonctions, peuvent visionner les images enregistrées (le responsable de la sécurité, par exemple). La CNIL rappelle que ces personnes doivent être sensibilisées et formées aux règles de mise en œuvre d'un système de vidéosurveillance.

La CNIL limite la conservation des images filmées à 1 mois. Elle rappelle qu'en règle générale, conserver les images quelques jours suffit à effectuer les vérifications nécessaires en cas d'incident, et permet d'enclencher d'éventuelles procédures disciplinaires ou pénales. Dans ce cas, les images sont extraites du dispositif (après consignation de cette opération dans un cahier spécifique) et conservées pour la durée de la procédure.

La vidéosurveillance doit être signalisée aux salariés et aux visiteurs dans les locaux au moyen d'un panneau d'affichage qui rappelle :

- l'existence du dispositif ;
- le nom de son responsable ;
- la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant.

Le message « Établissement sous vidéosurveillance » n'est pas suffisant. La CNIL précise que le message suivant est conforme : *« ÉTABLISSEMENT SOUS VIDÉO-SURVEILLANCE : Cet*

établissement est placé sous vidéosurveillance pour des raisons de sécurité des biens et des personnes. Vous pouvez exercer votre droit d'accès aux images vous concernant. Pour tout renseignement, s'adresser au responsable de la sécurité au (numéro de téléphone). »

Jurisprudence

*De façon générale, tout enregistrement fait à l'insu du salarié ne peut pas constituer un mode de preuve licite, c'est-à-dire qu'il ne sera pas retenu par les juges pour prouver une faute du salarié (**Cass. soc., 29 janvier 2008, n° 06-45-814**).*

Les membres du CSE disposent d'un droit d'alerte lorsqu'ils estiment que les procédés de surveillance utilisés dans l'entreprise portent atteinte aux libertés individuelles des salariés (**C. trav., art. L.2313-2**).

Remarque

Si l'employeur a le droit de contrôler l'activité de ses salariés pendant le temps de travail s'il les a préalablement informés, il n'est pas tenu de les informer de la mise en place d'un système de vidéosurveillance dans des entrepôts de marchandises où les salariés ne travaillent pas. Par conséquent, un enregistrement vidéo constatant la faute d'un salarié,

auteur de vols répétés dans un entrepôt de marchandises, est un élément de preuve licite, même si le salarié n'était pas informé de ce dispositif de surveillance (***Cass. soc., 31 janvier 2001, n° 98-44.290, et 19 janvier 2010, n° 08-45.092***). De même, une vidéosurveillance destinée à assurer uniquement la sécurité d'un magasin, et mise en place sans consultation des représentants du personnel, peut être utilisée pour établir une faute du salarié commise dans le cadre de sa vie personnelle (***Cass. soc., 26 juin 2013, n° 12-16.564***).

Lorsque la CNIL demande à l'employeur de justifier la mise en place du dispositif et que ce dernier ne répond pas, elle estime, qu'à défaut de justification, la vidéosurveillance apporte des restrictions non justifiées (***CNIL, délibération n° 2013-139 du 30 mai 2013***).

Le contrôle par une société de surveillance extérieure est-il possible ?

Si l'employeur peut, afin de garantir la bonne marche de son entreprise, contrôler et surveiller l'activité de ses salariés pendant leur temps de travail, il ne doit cependant pas le faire à leur insu.

Ainsi, constitue un mode de preuve illicite le rapport d'une société de surveillance extérieure à l'entreprise qui procédait au contrôle de l'utilisation du distributeur de

boissons et de sandwichs par les salariés, ce contrôle n'ayant pas été porté à la connaissance des salariés (***Cass. soc., 15 mai 2001, n° 99-42.219***).

De même, l'employeur ne peut pas faire appel à un détective privé pour faire suivre les salariés sans qu'ils le sachent (***Cass. soc., 4 février 1998, n° 95-43.421***).

4/ Le contrôle des salariés par l'outil informatique

L'employeur peut contrôler l'utilisation d'Internet et de la messagerie électronique par ses salariés à condition de les en informer au préalable et de consulter le comité d'entreprise (devenant à terme le CSE). Il peut également en limiter et en mesurer l'utilisation : dispositifs de filtrage de sites, détection de virus, encadrement de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « antispam », etc.).

Ce contrôle a pour objectif :

- d'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de Troie, etc.) ;

- 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, etc.).

Toutefois, cette surveillance ne doit pas porter atteinte de façon excessive au droit du salarié au respect de sa vie privée. Ainsi, le contrôle ne doit pas porter sur une analyse individuelle du contenu des messages ou des sites visités, mais il peut porter sur la fréquence ou le volume des messages, ou sur le temps de connexion.

De manière générale, le contrôle opéré par l'employeur doit présenter un lien avec l'activité professionnelle : il n'est ainsi pas possible de mettre en place un dispositif de surveillance uniquement pour vérifier que le salarié ne commet pas d'infractions qui ne présentent aucun lien avec l'activité professionnelle. Par exemple, l'employeur ne peut pas utiliser un système de traitement informatisé des données qui recherche les infractions à caractère pédopornographique que pourraient commettre les salariés lorsqu'ils utilisent les ordinateurs professionnels de l'entreprise.

L'interdiction des dispositifs « keyloggers »

La cybersurveillance est très encadrée : outre l'accès aux fichiers et mails personnels du salarié, qui ne peuvent pas être ouverts hors de sa présence, la CNIL considère qu'un

dispositif « keylogger », qui permet d'enregistrer toutes les frappes effectuées par un salarié sur son clavier, ne peut pas être utilisé dans un contexte professionnel, à l'exception d'impératifs forts de sécurité, et avec une information spécifique des personnes concernées (**communiqué CNIL du 20 mars 2013**).

Les « keyloggers » sont des dispositifs de surveillance, parfois téléchargeables gratuitement depuis le Web, qui se lancent automatiquement à chaque démarrage de la session de l'utilisateur, à son insu. Une fois lancés, ils permettent, selon les versions, d'enregistrer toutes les actions effectuées par les salariés sur leur poste informatique sans que ceux-ci s'en aperçoivent.

Toute frappe saisie sur le clavier et tout écran consulté sont enregistrés avec un horodatage.

Des alertes peuvent être automatiquement envoyées à la personne ayant installé le dispositif lorsque le salarié ainsi surveillé saisit sur son clavier un mot prédéterminé.

La CNIL considère que ce type de logiciel conduit celui qui l'utilise à pouvoir exercer une surveillance constante et permanente sur l'activité professionnelle des salariés concernés, mais aussi sur leur activité personnelle résiduelle et tolérée effectuée à partir du poste informatique.

La CNIL précise, en outre, que la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 punit 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.

Protection des fichiers et mails personnels

Il est interdit à l'employeur de prendre connaissance des messages adressés à un salarié par une personne extérieure à l'entreprise lorsqu'une indication portée dans l'objet du message confère indéniablement à ce dernier un caractère privé.

Les fichiers et courriels qui présentent un caractère privé ne peuvent pas être ouverts par l'employeur, sauf hypothèse d'une autorisation spécifique d'un juge en cas de motif légitime apporté par l'employeur, par exemple des actes de concurrence déloyale.
L'ouverture s'effectuera alors par un huissier de justice en présence du salarié.

Les courriels et fichiers professionnels (c'est-à-dire non identifiés comme personnels), en revanche, peuvent être ouverts. Toutefois, une clause du règlement intérieur peut limiter la marge de manœuvre de l'employeur en exigeant la présence d'un salarié ou de témoins (***Cass. soc., 26 juin 2012, n° 11-15.310***) : dans ce cas, l'employeur doit s'y conformer, même

pour les fichiers et mails professionnels, lorsque la clause ne distingue pas selon que ceux-ci ont été ou non identifiés comme personnels.

Le raisonnement est le même lorsque la procédure d'ouverture de ces fichiers est décrite dans la charte informatique de l'entreprise : l'employeur doit toujours respecter la procédure la plus favorable au salarié.

C'est au salarié d'identifier les messages et les fichiers qui lui sont personnels. À défaut d'une telle identification, les messages provenant de la messagerie électronique mise à la disposition du salarié par l'entreprise sont présumés être professionnels (***Cass. soc., 16 mai 2013, n° 12-11.866***).

Dans le même sens, les courriels stockés sur le disque dur de l'ordinateur professionnel du salarié, mais échangés entre salariés à partir de leur boîte mail personnelle, ne sont pas identifiés comme personnels du seul fait qu'ils émanent initialement de la messagerie électronique personnelle du salarié (***Cass. soc., 19 juin 2013, n° 12-12.138***). En revanche, des mails échangés entre des salariés de l'entreprise à partir de leurs adresses électroniques personnelles respectives restent des messages privés ; dès lors, par exemple, même si ces messages critiquent l'employeur, ce dernier ne pourra pas s'en prévaloir pour sanctionner les salariés.

Ainsi, lorsque des messages électroniques stockés sur le disque dur de l'ordinateur professionnel du salarié proviennent de sa messagerie personnelle, distincte de la messagerie professionnelle dont il dispose pour les besoins de son activité, ces messages doivent être écartés des débats car leur production en justice porte atteinte au secret des correspondances (***Cass. soc., 26 janvier 2016, n° 14-15.360***). L'employeur ne pourra donc pas utiliser ces messages pour prouver la faute d'un salarié.

Les juges semblent généralement considérer qu'un courriel ou un fichier qui n'est pas identifié comme personnel est professionnel.

Toutefois, même lorsque le fichier n'est pas identifié comme personnel, l'employeur ne pourra pas l'utiliser s'il s'avère qu'il relève de la vie privée du salarié. Par exemple, des courriers à caractère érotique entre deux salariés d'une même entreprise (***Cass. soc., 5 juillet 2011, n° 10-17.284***).

Exemples

Des fichiers restent professionnels si le salarié s'est contenté de les enregistrer sous son prénom. De même, les fichiers trouvés dans un répertoire nommé avec les initiales du salarié, lequel comportait un sous-répertoire nommé « personnel » et un autre nommé

*avec le nom de famille de ce salarié, sont professionnels (**Cass. soc., 21 octobre 2009, n° 07-43.877**).*
*Des fichiers intitulés « essais divers », « essais divers B », « essais divers restaurés » sont aussi professionnels. De même, la seule dénomination « mes documents » donnée à un fichier ne lui confère pas un caractère personnel (**Cass. soc., 10 mai 2012, n° 11-13.884**) : en effet, il s'agit d'un répertoire mis en place automatiquement dans le système d'exploitation informatique de l'ordinateur.*

De même, le fait de renommer le disque dur de l'ordinateur « données personnelles » ne peut pas conférer un caractère personnel à l'intégralité des données qu'il contient (***Cass. soc., 4 juillet 2012, n° 11-12.502, et CEDH, 22 février 2018, n° 588/13***).

Cette jurisprudence vise à faire échec aux salariés qui tentent de protéger l'intégralité des données contenues sur leur ordinateur, mis à disposition par l'employeur, du contrôle de ce dernier.

L'employeur peut également consulter et lire la clé USB du salarié lorsque celle-ci est connectée à son ordinateur professionnel (***Cass. soc., 12 février 2013, n° 11-28.649***). *A contrario*, lorsque la clé USB n'est pas connectée à l'ordinateur, il ne peut pas en consulter le contenu sans la présence du salarié.

Notez-le

Déterminer si une clé USB est personnelle ou professionnelle peut s'avérer délicat : il convient donc d'inciter les salariés à identifier leurs clés personnelles en les étiquetant de leur nom ou de la mention « personnelle », et en prévoyant un dispositif d'ouverture par mot de passe.

Notons également que 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.

Cela étant, pour éviter les atteintes à la vie privée, il est préférable d'inciter les salariés à identifier leurs fichiers (création d'un répertoire personnel, règle d'identification des messages, etc.). Il est recommandé d'identifier clairement son répertoire par des intitulés tels que « personnel », « fichier/document personnel/privé », « privé », etc.

Une décision a sanctionné un employeur qui avait écouté le dictaphone personnel du salarié placé sous son ordinateur de travail : les juges ont considéré que l'employeur ne pouvait procéder à ces écoutes qu'en présence du salarié. La solution aurait été différente

si le dictaphone avait été mis à disposition par l'employeur (***Cass. soc., 23 mai 2012, n° 10-23.521***).

La protection des fichiers et mails personnels est levée si une enquête judiciaire est en cours (par exemple, si le salarié 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 du salarié.

Communication des mots de passe

Les identifiants et mots de passe (session Windows, messagerie, etc.) sont confidentiels et ne doivent pas être transmis à l'employeur. Toutefois, si un salarié 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.

Par ailleurs, le manque de sécurisation des mots de passe pour accéder aux données personnelles peut être sanctionné par la CNIL : elle a ainsi infligé une amende à une entreprise où les mots de passe pour accéder aux ordinateurs et aux données personnelles

étaient composés de cinq caractères seulement, correspondants pour la plupart au prénom et nom de famille des salariés (***CNIL, délibération n° 2013-139 du 30 mai 2013***).

Limites au pouvoir de contrôle de l'employeur

De façon plus générale, la CNIL précise que :

- l'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses salariés ;
- les « keyloggers » qui permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur sont, sauf circonstance exceptionnelle liée à un fort impératif de sécurité, illicites ;
- les logs de connexion ne doivent pas être conservés plus de 6 mois.

Que peut faire l'employeur afin de concilier le contrôle de l'activité des salariés et la protection des libertés fondamentales ?

En pratique, afin d'éviter les abus de l'usage d'Internet et de la messagerie par les salariés, il est intéressant de mettre en place une charte de l'outil informatique au sein des entreprises. À titre d'exemple, la CNIL propose les clauses suivantes :

- « *seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle* » ;
- *« une consultation ponctuelle et raisonnable pour un motif personnel de sites Internet dont le contenu n'est pas contraire à l'ordre public et ne met pas en cause l'intérêt et la réputation de l'entreprise est tolérée ».*

Jurisprudence

*Le salarié qui consulte Internet à des fins non professionnelles pour une durée totale de 41 heures dans le mois ne satisfait pas à cette notion d'utilisation raisonnable de l'outil (**Cass. soc., 18 mars 2009, n° 07-44.247**). De même, commet également une faute grave le salarié qui, pendant son temps de travail, se connecte plus de 10 000 fois en 1 mois sur des sites Internet non liés à son activité professionnelle (sites de voyages ou de tourisme, de comparaisons de prix, de marques de prêt-à-porter, de sorties et d'événements régionaux, ainsi qu'à des réseaux sociaux et au site d'un magazine féminin) (**Cass. soc., 26 février 2013, n° 11-27.372**).*

*Un salarié qui se connecte quotidiennement sur des réseaux sociaux et consulte plusieurs fois par jour sa messagerie personnelle pendant les heures de travail commet une faute qui justifie son licenciement (**CA Pau, 13 juin 2013, n° 11/02759**).*

S'il y a une tolérance permettant des connexions personnelles, l'utilisation abusive d'Internet à des fins personnelles peut constituer une faute grave : est ainsi justifié le licenciement pour faute grave d'un salarié dont la connexion sur Internet et divers réseaux sociaux, pour s'adonner à une passion personnelle, dépassait 20 % de son temps de travail (***CA Rennes, 20 novembre 2013, n° 12/03567***).

Concernant la messagerie, la CNIL propose de mentionner dans la charte : *« qu'un usage raisonnable dans le cadre de nécessités de la vie courante et familiale est toléré, à condition que son utilisation n'affecte pas le trafic normal des messages professionnels ».* Elle suggère également de faire figurer dans cette même charte, le principe retenu pour distinguer les e-mails professionnels de ceux personnels (qualification de l'objet, création d'un répertoire spécifique, etc.).

Cette charte devra être régulièrement mise à jour afin de tenir compte de l'évolution des nouvelles technologies.

L’employeur peut parfaitement intégrer cette dernière au règlement intérieur en respectant la procédure adéquate. Attention, s’il met en place des procédures de contrôle assorties de garantie en faveur des salariés, il doit s’y conformer.

Remarque

Si le salarié se livre à des actes de concurrence déloyale en utilisant l’ordinateur de l’entreprise, l’employeur peut saisir, sur la base de preuves précises et concordantes, le juge des référés (juge de l’urgence) pour obtenir la cessation de ce trouble manifestement illicite, ainsi que la saisie du disque dur afin de pouvoir se constituer des preuves licites dans le cadre d’un licenciement.

Le contrôle des salariés sur les réseaux sociaux

Les juges considèrent ce mode de communication comme faisant partie *a priori* de l’espace public : il appartient donc aux salariés d’y respecter l’obligation de loyauté.

Par ailleurs, les propos tenus sur les pages personnelles ou le « mur » Facebook perdent leur caractère privé lorsqu’ils sont accessibles à un très grand nombre.

L'employeur peut donc sanctionner ceux qui y tiennent des propos injurieux envers l'entreprise ou leur supérieur hiérarchique car les conversations n'ont pas de caractère privé à partir du moment où le salarié n'a pas réglé les paramètres de confidentialité existants pour en limiter l'accès (***CA Rouen, 15 novembre 2011, n° 11/01830***).

Notez-le

Les propos tenus par les salariés sur les réseaux sociaux peuvent également, le cas échéant, constituer un délit d'injure publique, réprimé pénalement lorsqu'ils sont accessibles à tous (***Cass. 1re civ., 10 avril 2013, n° 11-19.530***). Lorsque les propos sont accessibles à tous, le salarié peut être sanctionné et condamné, le cas échéant, à verser des dommages et intérêts à son employeur (***CA Reims, 24 octobre 2012, n° 11/01249***).

En revanche, lorsque le salarié s'exprime sur ces réseaux dans un cadre privé et que les paramètres de confidentialité ont été réglés, l'employeur qui prend connaissance des propos viole le respect de la vie privée du salarié, et cette correspondance ne peut pas être sanctionnée.

Ainsi, des propos injurieux et offensants diffusés sur le compte ouvert par un salarié sur Facebook, et accessibles uniquement à un groupe fermé de 14 personnes agréées par celui-

ci, relèvent d'une conversation de nature privée et ne constituent pas une faute grave (***Cass. soc., 12 septembre 2018, n° 16-11.690***).

Sont justifiés :

- l'avertissement à un salarié journaliste qui publie des propos insultants envers sa hiérarchie sur le mur Facebook d'une amie également salariée de l'entreprise (***CA Reims, 9 juin 2010, n° 09/03209***) ;
- le licenciement pour faute grave de salariés ayant tenu sur leur mur Facebook des propos vexatoires, visibles par tous, dénigrant leur supérieur et évoquant l'idée de lui rendre la vie impossible (***conseil de prud'hommes Boulogne-Billancourt, 19 novembre 2010, n° 09/00316 et 09/00343***) ;
- le licenciement d'un conducteur routier qui a tenu sur son mur Facebook des propos diffamatoires et insultants à l'encontre des dirigeants et de l'entreprise, alors qu'il n'avait pas activé les critères de confidentialité du compte et avait pris ainsi le risque de donner de la publicité aux propos qu'il pensait privés ; la faute grave est néanmoins écartée du fait du faible risque que les clients aient eu connaissance de ces propos (***CA Lyon, 24 mars 2014, n° 13/03463***).

N’est pas justifié le licenciement d’un salarié qui s’est interrogé, sur un site Internet quasiment confidentiel, sur le licenciement de l’un de ses collègues dans le cadre d’une situation de conflit, sans que les propos incriminés soient injurieux ou vexatoires (***Cass. soc., 6 mai 2015, n° 14-10.781***).

Attention également : lorsque le procès-verbal de constat d’huissier établi à la demande de la société rapporte des informations extraites du compte Facebook d’un salarié et obtenues à partir du téléphone portable d’un autre salarié, informations réservées aux personnes autorisées, l’employeur ne peut pas y accéder sans porter une atteinte disproportionnée et déloyale à la vie privée du salarié (***Cass. soc., 20 décembre 2017, n° 16-19.609***).

La CNIL a publié sur son site Internet une fiche à destination des salariés qui utilisent des réseaux sociaux, en leur recommandant d’adapter les paramètres de confidentialité en fonction des informations et des personnes avec lesquelles ils souhaitent les faire partager. (www.cnil.fr).

Tableau des procédés de surveillance

<table>
<tr><th rowspan="2">Procédé</th><th rowspan="2">Objet</th><th colspan="2">Mise en œuvre</th></tr>
<tr><th>Dans tous les cas</th><th>Formalités supplémentaires</th></tr>
<tr><td>Badge</td><td>Contrôler le temps de travail et lutter contre le vol.</td><td rowspan="4">Le dispositif doit être :
- justifié par la tâche à accomplir ;
- proportionné au but recherché.
L’information des membres du CSE est obligatoire. Le règlement intérieur de l’entreprise doit être adapté en conséquence.
L’employeur peut</td><td></td></tr>
<tr><td>Fouille</td><td>Lutter contre le vol.</td><td>Consentement du salarié nécessaire.
Information de son droit de s’y opposer et d’exiger la présence d’un témoin.</td></tr>
<tr><td>Contrôle de l’ordinateur et des messageries électroniques</td><td>Contrôler le travail du salarié.</td><td>Possibilité d’accéder librement aux postes informatiques (sauf fichiers/messages identifiés comme personnels).</td></tr>
<tr><td>Contrôle des communications téléphoniques</td><td>Contrôler le travail du salarié.</td><td>Relevés téléphoniques occultant les 4 derniers chiffres.</td></tr>
</table>

Vidéo-surveillance	Contrôler le travail du salarié et lutter contre le vol.	donc ouvrir les fichiers et mails sans la présence du salarié, sauf si ce dernier les a identifiés comme personnels. Une clause du règlement intérieur peut toutefois imposer la présence du salarié. Interdiction (sauf impératifs de sécurité) des dispositifs « keyloggers » enregistrant les frappes des salariés sur leur clavier.	Quand l'entreprise est ouverte au public (commerce) : obtention d'une autorisation préfectorale après avis de la commission départementale de la vidéoprotection.
Géolocalisation PS/GSM	Contrôler le travail et les déplacements du salarié.		Conditions strictes à respecter. L'employeur doit permettre au salarié d'avoir accès aux données de géolocalisation (***délib. CNIL, n° 2012-213 du 22 juin 2012***). Il est interdit de géolocaliser le salarié pendant ses trajets entre le domicile et le travail ainsi que pendant ses temps de pause : l'employeur doit lui permettre de désactiver le dispositif (***délibération CNIL n° 2015-165 du 4 juin 2015***).

to be continued...