LIAISONS SOCIALES QUOTIDIEN

DOSSIER N°
216 / 2020

// le dossier pratique

La surveillance de l'activité des salariés

Droits et obligations de l'employeur, moyens de surveillance

Vidéosurveillance, géolocalisation, traçage informatique, identifications biométriques… Les dispositifs de surveillance des salariés font partie de l'environnement de travail. Le Code du travail n'étant guère explicite sur ces sujets, il n'est pas facile de savoir précisément ce que peuvent faire les employeurs en la matière. Nous publions ici une synthèse des règles légales et jurisprudentielles applicables, ainsi que des positions de la Cnil.

Dossier mis à jour par Florence Lefrançois, avocate au Barreau de Tours

À CLASSER SOUS
LIBERTÉS INDIVIDUELLES 03 / 20

1 Droits et obligations de l'employeur

EST-IL PERMIS DE SURVEILLER LES SALARIÉS ?

L'employeur, responsable de la bonne marche de l'entreprise, dispose d'un **pouvoir de direction** et de son corollaire, le pouvoir disciplinaire. Il en résulte qu'il peut **contrôler et surveiller** l'activité de ses salariés pendant le temps de travail, comme le rappelle régulièrement la jurisprudence *(Cass. soc., 14 mars 2000, n° 98-42.090; Cass. soc., 4 juillet 2012, n° 11-30.266)*.

Mais cette surveillance ne doit **pas** se faire **par** le **biais** d'un **procédé clandestin**, à l'insu des salariés *(Cass. soc., 10 janvier 2012, n° 10-23.482 ; Cass. soc., 18 octobre 2017, n° 16-16.462)*. L'employeur ne peut davantage mettre en œuvre des **stratagèmes destinés à piéger** les salariés *(Cass. soc., 4 juillet 2012, n° 11-30.266*: l'employeur avait piégé des lettres par un système répandant de l'encre bleue pour démasquer le salarié qui les ouvrait au centre de tri ; *Cass. soc., 19 novembre 2014, n° 13-18.749*: l'employeur, cherchant à établir des erreurs de caisse par une vendeuse, avait fait appel à la directrice des magasins et à un tiers pour effectuer des achats en se présentant comme de simples clients).

De plus, quelle que soit la **méthode de surveillance** utilisée, celle-ci doit être **justifiée** par la nature de la tâche à accomplir et **proportionnée** au but recherché *(C. trav., art. L. 1121-1)*. Le pouvoir de surveillance de l'employeur doit en effet se concilier avec le respect des libertés individuelles et de la vie privée des salariés. Ainsi, la filature d'un salarié de la sortie de son domicile jusqu'à son retour pendant sept jours, dans le cadre de soupçons d'une activité de concurrence déloyale, est disproportionnée par rapport à l'atteinte faite à sa vie privée *(Cass. 2e civ., 17 mars 2016, n° 15-11.412)*.

FAUT-IL INFORMER LES SALARIÉS ?

Une information obligatoire

Selon l'article L. 1222-4 du Code du travail, aucune information concernant personnellement un salarié ne peut être collectée par un **dispositif** qui n'a pas été **porté préalablement** à sa **connaissance**.

Ainsi, le recours à une société de surveillance extérieure afin de procéder au contrôle de l'utilisation par les salariés des distributeurs de boissons et sandwichs doit être préalablement porté à la connaissance des salariés *(Cass. soc., 15 mai 2001, n° 99-42.219)*.

À NOTER Il a toutefois été admis par la Cour européenne des droits de l'Homme que des circonstances particulières pouvaient permettre de mettre en place un dispositif de surveillance sans information préalable des salariés : l'existence de soupçons de graves irrégularités, en l'occurrence, soupçons de vol réalisés par les caissières d'un supermarché, a ainsi été jugée comme légitimant la possibilité de mettre en place un dispositif de vidéosurveillance clandestin *(CEDH, grande chambre, 17 octobre 2019, aff. 1874/13)*.

On notera également que l'**information préalable** des salariés n'est **pas requise** en cas de **contrôle** de l'activité sur le **temps**

et le **lieu de travail par** leur **supérieur hiérarchique** *(Cass. soc., 26 avril 2006, nº 04-43.582)*, ou par un **service interne** à l'entreprise chargé de cette mission *(Cass. soc., 5 novembre 2014, nº 13-18.427*: dans cette affaire, des cadres étaient chargés d'observer les amplitudes et horaires de travail des équipes de contrôle dans un service public de transport ; *CE, 13 juillet 2020, nº 417.972*: pour un dispositif de contrôle de facturation d'actes médicaux d'une caisse d'assurance maladie). Il a été jugé dans le même sens que « la simple surveillance d'un salarié sur son lieu de travail par un inspecteur des recettes, même en l'absence d'information préalable de l'intéressé, ne constitue pas en soi un mode de preuve illicite » *(Cass. soc., 3 mai 2007, nº 05-44.612 F-D)*.

La mise en œuvre d'un **audit interne** ponctuel destinée à analyser l'organisation du travail au sein d'un service n'est pas non plus assimilée à dispositif de contrôle de l'activité des salariés *(Cass. soc., 12 juillet 2010, nº 09-66.339)*.

À NOTER La solution ne semble toutefois pas être identique lorsque l'audit a pour objet d'appréhender les fonctions d'une salariée et de vérifier qu'elle n'exerce pas un pouvoir qui excède ce que sa fonction lui permet : en l'occurrence, la Cour de cassation n'a pas expressément écarté l'application de l'article L. 1222-4 du Code du travail, mais a jugé que, même si la salariée n'avait pas été préalablement informée de la mission d'audit, elle n'avait pas été tenue à l'écart des travaux réalisés aux fins d'entretiens avec elle et de sondage sur des pièces comptables ou juridiques. Elle semble ainsi retenir que l'information de la salariée a bien été faite *(Cass. soc., 26 janvier 2016, nº 14-19.002)*.

Comment procéder ?

Le Code du travail ne précise pas comment procéder à cette information. La Cour de cassation a, pour sa part, reconnu une information valable s'agissant d'un **mémo** circularisé sous forme papier, adressé à l'ensemble des salariés et disponible de manière constante sur l'intranet de l'entreprise *(Cass. soc., 13 juin 2018, nº 16-25.301)*.

Une **remise en main propre contre décharge ou un envoi par courrier recommandé avec accusé de réception** permet de prouver la bonne communication et est donc **indispensable**.

Sur le contenu de l'information à donner, il doit, à notre sens, être **conforme** aux exigences du règlement général sur la protection des données (**RGPD**) : outre l'information sur l'existence du dispositif, l'employeur doit notamment préciser les finalités du dispositif, ainsi que le responsable du traitement et le destinataire des données et l'ensemble des droits dont le salarié dispose sur l'usage de ces données *(v. ci-après)*.

En tout état de cause, cette **information** doit être **complète** *(Cass. soc., 10 janvier 2012, nº 10-23.482*, à propos d'une entreprise sanctionnée pour avoir informé le personnel de la présence de caméras de surveillance, mais sans préciser que ces dernières permettaient de contrôler leurs heures d'arrivée et de départ ; *Cass. soc., 3 novembre 2011, nº 10-18.036*, à propos d'un dispositif de géolocalisation qui était utilisé pour d'autres fins que celles portées à la connaissance des salariés).

Quelles sanctions à défaut d'information des salariés ?

Faute d'information préalable d'un salarié sur l'existence et les modalités d'un dispositif de surveillance, les **preuves recueillies ne pourront être alléguées** à son **encontre** *(Cass. soc., 10 janvier 2012, préc.)*.

FAUT-IL CONSULTER LE COMITÉ SOCIAL ET ÉCONOMIQUE ?

Dans les entreprises de 50 salariés et plus, la **consultation** préalable du comité social et économique (CSE) s'impose en cas de **mise en œuvre de moyens ou techniques** permettant un **contrôle** de l'**activité** des salariés *(C. trav., art. L. 2312-37 et L. 2312-38)*. Le comité social et économique doit être informé de l'ensemble des **finalités** du dispositif : ainsi, un outil de traçabilité mis en place au sein d'une banque pour assurer le contrôle des opérations et procédures internes, la surveillance et la maîtrise des risques, mais qui permet également de restituer l'ensemble des consultations effectuées par les salariés, ne peut être utilisé pour vérifier si le salarié procède à la consultation de comptes autres que ceux des clients de son portefeuille dès lors que le comité social et économique n'a pas été informé et consulté sur l'utilisation de ce dispositif à cette fin *(Cass. soc., 11 décembre 2019, nº 18-11.792)*.

Signalons toutefois, comme c'est le cas pour l'obligation d'information préalable des salariés *(v. ci-dessus)* que le simple contrôle de l'activité d'un salarié par un service interne à l'entreprise chargé de cette mission ne requiert pas l'information et la consultation préalable du comité social et économique *(Cass. soc., 4 juillet 2012, nº 11-14.241 F-D)*.

Si l'employeur omet de consulter le comité social et économique préalablement à la mise en place d'un dispositif de surveillance, il s'expose par ailleurs à une condamnation pour **délit d'entrave** *(C. trav., art. L. 2317-1)*.

De plus, les éléments recueillis par le biais de ce procédé seront considérés comme des **moyens de preuve illicite** *(Cass. soc., 2 novembre 2016, nº 15-20.540 ; Cass. soc., 11 décembre 2019, précité)*.

À NOTER La consultation ou l'information du comité social et économique n'est pas envisagée par le Code du travail dans les entreprises de moins de 50 salariés.

QUELLES SONT LES EXIGENCES LIÉES À LA PROTECTION DES DONNÉES PERSONNELLES ?

Si la loi Informatique et libertés a longtemps imposé une déclaration voire une autorisation des dispositifs de surveillance auprès de la Commission nationale de l'informatique et des libertés (Cnil), l'entrée en vigueur du règlement de l'Union européenne 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, autrement appelé RGPD *(Règl. UE nº 2016/679, 27 avril 2016, JOUE L119, 4 mai 2016)* a profondément remanié les règles de protection des données personnelles.

La loi informatique et libertés a, par suite été modifiée *(L. nº 78-17, 6 janvier 1978, JO 7 janvier ; modifiée par L. nº 2018-493, 20 juin 2018, JO 21 juin ; Ord. nº 2018-1225, 12 décembre 2018, JO 13 décembre)*.

La protection des données s'inscrit désormais dans une logique de **responsabilisation** de l'**employeur** en tant que responsable du traitement. Il doit ainsi veiller à ce que les **dispositifs** de surveillance qu'il met en place **respectent** les règles définies par le **RGPD**.

À NOTER Dans les développements à venir, nous avons maintenu les références aux positions issues de délibérations de la Cnil antérieures à l'entrée en vigueur de ces nouvelles règles, dès lors qu'elles apparaissent conformes aux nouvelles règles et restent d'actualité.

Sachez par ailleurs que, dans l'attente de la définition de référentiels, la Cnil a maintenu les anciennes normes simplifiées et les autorisations uniques afin de pouvoir s'y référer pour définir les durées de conservations des données, les personnes habilitées à accéder aux données, les données pouvant être recueillies, etc.

Principes devant être respectés par le dispositif de contrôle

Comme tout traitement de données à caractère personnel, le dispositif de contrôle doit respecter les six principes posés par la réglementation *(Règl. UE n° 2016/679, 27 avril 2016, art. 5 ; L. n° 78-17, 6 janvier 1978, art. 4)*.
Les **données** collectées doivent ainsi être :
– **traitées de manière licite, loyale et transparente** au regard de la personne concernée ;
– **collectées pour des finalités déterminées, explicites et légitimes** et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
– **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités définies ;
– **exactes et tenues à jour si nécessaire**. Des mesures raisonnables doivent être prises pour que des données inexactes soient effacées ou rectifiées sans tarder ;
– **conservées sous une forme permettant l'identification des personnes concernées** pendant une durée qui n'excède pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
– **traitées de façon à garantir une sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.
Par ailleurs, le traitement de données doit être assis sur une base juridique. Dans les relations de travail, il n'est considéré comme licite que s'il remplit au moins une des conditions suivantes *(Règl. UE n° 2016/679, 27 avril 2016, art. 6 ; L. n° 78-17, 6 janvier 1978, art. 5)* :
– la **personne concernée** doit avoir consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
– le **traitement** doit être nécessaire à l'exécution d'un **contrat** auquel la personne concernée est partie, ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
– le traitement est nécessaire au respect d'une **obligation légale** à laquelle le responsable de traitement est soumis ;
– le traitement est nécessaire aux **fins des intérêts légitimes** poursuivis par le responsable du traitement, à moins que ne prévalent les intérêts ou les ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel.

Information des salariés

En application du principe de transparence, l'employeur informe les salariés sur *(Règl. UE n° 2016/679, 27 avril 2016, art. 13 et 14)* :
– l'identité et les coordonnées du **responsable** du **dispositif de contrôle**, et le cas échéant, du délégué à la protection des données ;
– les **finalités du dispositif** de contrôle installé et la base juridique qui le justifie ;
– le ou les **destinataires des données** recueillies ;
– la **durée de conservation** des données recueillies par le biais de ce dispositif ;
– le **droit** de demander l'**accès** aux données, leur **rectification**, leur **effacement** ou la limitation du traitement, le droit de **s'opposer** au traitement ;
– le droit d'introduire une **réclamation** auprès de la Cnil.

LE CONTRÔLE PAR CHRONOTACHYGRAPHE

Installé dans les véhicules de transports routiers, le chronotachygraphe est un appareil qui a pour objet de collecter et d'enregistrer des données personnelles relatives à la conduite du salarié (sa vitesse, ses temps de conduite, ses temps de pause). Contrairement aux autres moyens de surveillance, l'employeur est ici tenu, en vertu d'un règlement communautaire et sous peine de sanctions pénales, d'assurer la mise en place et l'utilisation d'un chronotachygraphe, dans tous les véhicules de transport de neuf personnes ainsi que dans les véhicules de marchandises de plus de 3,5 tonnes *(Règl. UE n° 165/2014, 4 février 2014)*.
Compte tenu de l'existence de cette obligation légale, la Cnil avait allégé les formalités déclaratives des entreprises de transport en les dispensant de l'obligation de déclaration préalable du dispositif *(Délib. Cnil n° 2014-235, 27 mai 2014, JO 21 juin)*.
Les déclarations et autorisations préalables ayant désormais disparu, il n'en demeure pas moins que l'employeur doit respecter les obligations issues de la réglementation sur la protection des données personnelles.

Registre des activités de traitement et analyse d'impact relative à la protection des données

Dans les **entreprises de 250 salariés et plus**, l'employeur doit mettre en place un **registre** des **activités de traitement**, au sein duquel il doit intégrer les dispositifs de surveillance et de contrôle *(Règl. UE n° 2016/679, 27 avril 2016, art. 30)*.

À NOTER **Dans les entreprises de moins 250 salariés, on notera que le registre des activités de traitement s'impose également dès lors que le dispositif de contrôle est susceptible de comporter un risque pour les droits et libertés des personnes concernées et qu'il n'est pas occasionnel *(Règl. UE n° 2016/679, 27 avril 2016, art. 30)*.**

Pour les dispositifs de surveillance susceptibles d'engendrer un **risque élevé** pour les **droits et libertés** des personnes concernées, l'employeur doit également établir une **analyse d'impact** relative à la protection des données *(Règl. UE n° 2016/679, 27 avril 2016, art. 35 ; L. n° 1978-17, 6 janvier 1978, art. 62)*. Ainsi, l'analyse d'impact s'impose pour tous les traitements ayant pour finalité de **surveiller de manière constante** l'**activité** des **salariés** *(Délib. Cnil n° 2018-327, 11 octobre 2018, JO 6 novembre)*.
En revanche, il n'est pas nécessaire de procéder à une étude d'impact pour les dispositifs dont l'objet est de gérer les contrôles d'accès physiques et les horaires, en dehors de tout dispositif biométrique *(Délib. Cnil n° 2019-118, 12 septembre 2019, JO 22 octobre)*.

Sanction du non-respect de la réglementation RGPD

Compte tenu du caractère récent de la réglementation issue du RGPD, la Cour de cassation n'a, à notre connaissance, pas encore eu à aborder la question de l'incidence du non-respect de la réglementation sur la protection des données personnelles.
La violation de ces règles expose évidemment l'employeur à une **intervention** de la **Cnil** qui, dans un

premier temps, sensibilisera le contrevenant en l'invitant à prendre des **mesures correctives**, **puis**, à défaut, pourra se montrer plus coercitive par **mise en demeure**, **ou injonction de mise en conformité sous astreinte**, voire par le prononcé d'**amendes administratives** *(L. nº 78-17, 6 janvier 1978, art. 20)*.
Des **sanctions pénales** sont également encourues *(v. l'encadré ci-dessous)*.
Sur le plan de la preuve, il y a tout lieu de penser que la jurisprudence relative aux conséquences du défaut de dépôt de l'ancienne déclaration auprès de la Cnil s'appliquera : les **éléments recueillis** *via* le **dispositif de surveillance illicite** seront des **éléments de preuve irrecevables** *(Cass. soc., 8 octobre 2014, nº 13-14.991 ; Cass. soc., 2 novembre 2016, nº 15-20.540)*. De même, il ne pourra être reproché à un salarié de refuser de déférer à une exigence de l'employeur en application du dispositif de contrôle mis en place *(Cass. soc., 6 avril 2004, nº 01-45.227)*.

2 Précisions sur les différents moyens de surveillance

LES CONTRÔLES PAR BADGES

Ces dispositifs permettent de **contrôler** les **entrées** et **sorties** du personnel, mais aussi les **horaires** de travail.

QUELS RISQUES EN CAS DE RECOURS ILLICITES AUX SYSTÈMES DE SURVEILLANCE ?

Les salariés ou les organisations syndicales peuvent, en cas d'utilisation illicite ou abusive de systèmes de surveillance, saisir le service des plaintes de la Cnil, l'inspection du travail ou le procureur de la République, voire les services de la préfecture, de la police ou de la gendarmerie si des caméras filment des lieux ouverts au public.
Par ailleurs, certaines infractions sont passibles de sanctions pénales, notamment :
– enregistrement de l'image d'une personne à son insu dans un lieu privé, captation de paroles prononcées à titre privé ou confidentiel, captation de la localisation en temps réel ou différé d'une personne sans le consentement de celle-ci : un an d'emprisonnement et 45 000 € d'amende *(C. pén., art. 226-1)* ;
– atteinte à la vie privée par les personnes morales : amende de 225 000 € et interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement leur activité professionnelle *(C. pén., art. 226-7)* ;
– atteinte au secret des correspondances : un an d'emprisonnement et 45 000 € d'amende *(C. pén., art. 226-15)* ;
– mise en œuvre d'un traitement de données à caractère personnel ne respectant pas les obligations générales issues du RGPD, notamment en matière de sécurité des données : cinq ans d'emprisonnement et 300 000 € d'amende *(C. pén. art. 226-18)* ;
– collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite : cinq ans d'emprisonnement et 300 000 € d'amende *(C. pén., art. 226-18-1)* ;
– durée de conservation excessive de données à caractère personnel : cinq ans d'emprisonnement et 300 000 € d'amende *(C. pén., art. 226-20)*.
Rappelons également que ne pas consulter le comité social et économique peut constituer un délit d'entrave.

À quelles conditions ?

L'emploi de badges n'est pas interdit, notamment si l'employeur justifie d'**impératifs de sécurité**.
Il peut permettre de sécuriser l'accès à l'entrée des bâtiments, ou encore à des locaux faisant l'objet de restrictions de circulation. En revanche, il ne peut pas servir au contrôle des déplacements à l'intérieur des locaux *(Fiche Cnil : « L'accès aux locaux et le contrôle des horaires »)*.
S'agissant d'un salarié investi d'un mandat représentatif, le Conseil d'État a même jugé que le fait de s'abstenir, de manière systématique, d'utiliser les badges en usage dans l'entreprise en dépit de plusieurs mises en garde constituait un comportement fautif de nature à justifier son licenciement *(CE, 8 août 2002, nº 109749)*.
Le badgeage ne doit cependant pas empêcher les représentants du personnel qui en disposent d'exercer leur droit de circulation *(Cass. soc., 26 septembre 2007, nº 06-11.425)*.

Et les dispositifs biométriques ?

Prudence si le dispositif de badgeage utilise des données biométriques (empreinte digitale, iris, voix, visage par exemple). Il s'agit en effet de **données sensibles**, et la **Cnil** a adopté un **règlement** relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail *(Délib. Cnil nº 2019-001, 10 janvier 2019, JO 28 mars)*.
Le **recours** à des dispositifs biométriques doit ainsi être justifié par des impératifs de sécurité auxquels ne pourraient pas répondre d'autres dispositifs d'identification ou d'autres mesures organisationnelles. Il ne peut être envisagé que :
– pour le **contrôle d'accès** à des **locaux** limitativement identifiés comme devant faire l'objet d'une **restriction de circulation** ;
– pour le contrôle d'accès à des **appareils et applications** informatiques professionnels limitativement **identifiés**.
Lorsqu'il est mis en place, le dispositif biométrique ne peut **permettre de recueillir que** les **données** suivantes :
– l'**identité** : nom, prénoms, photographie, enregistrement brut (photo, enregistrement audio, etc.) de la caractéristique biométrique et gabarit d'une ou plusieurs caractéristiques biométriques, numéro d'authentification ou numéro de support individuel, coordonnées professionnelles, clés de chiffrement ;
– la **vie professionnelle** : numéro de matricule interne, corps ou service d'appartenance, grade, identité ou dénomination sociale de la personne (physique ou morale) ayant la qualité d'employeur ;
– l'**accès aux locaux** : accès, zones et plages horaires autorisés ;
– l'**accès aux outils de travail** : matériels ou applicatifs concernés, plages horaires et modalités d'accès autorisées.
Le **dispositif** doit prévoir un **accès limité** aux données biométriques et aux données personnelles recueillies. Il doit être **encadré** par des **mesures de sécurité élevées.**
Les **durées de conservation** des données biométriques sont très réduites : elles ne peuvent être traitées que le temps nécessaire au calcul du gabarit correspondant, et les données biométriques dérivées ne peuvent être conservées que sous forme de gabarit chiffré ne permettant pas de recalculer la caractéristique biométrique d'origine. Les données de journalisation peuvent quant à elles être conservées au maximum six mois à compter

de leur date d'enregistrement. Les données d'identification doivent quant à elles être supprimées au plus tard dans les six mois suivant la date de retrait d'habilitation de la personne ou de cessation de ses fonctions.

Quid de l'accès et de la conservation des données ?

Pour la Commission nationale de l'informatique et des libertés, les informations fournies par les badges ne doivent être accessibles qu'aux **membres habilités** des **services gérant** le **personnel**, la **paie** ou la **sécurité** *(Fiche Cnil : « L'accès aux locaux et le contrôle des horaires »)*.
L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et empêcher que des personnes qui n'ont pas qualité pour y accéder puissent en prendre connaissance. Ainsi, il doit prévoir des **habilitations** pour les accès informatiques avec une **traçabilité** des actions effectuées (savoir qui se connecte à quoi, quand et dans quel but).
Les données relatives aux accès doivent être supprimées trois mois après leur enregistrement.
Les données utilisées pour le suivi du temps de travail peuvent être conservées pendant cinq ans.

LA VIDÉOSURVEILLANCE

À quelles conditions ?

En cas de mise en place d'un système de vidéosurveillance dans l'entreprise, toutes les conditions évoquées précédemment doivent être respectées, notamment la **légitimité** et le **caractère proportionné** du dispositif au but recherché.
Sur ce dernier point, la **Cnil refuse** que des **salariés** soient **filmés en continu** sur leurs lieux de travail **sauf circonstances particulières** (personnes exposées à un risque d'une particulière gravité). Elle a ainsi condamné l'utilisation par une entreprise d'une caméra de vidéosurveillance filmant en permanence les agents installés dans le PC de sécurité d'une galerie commerçante, en considérant que cette surveillance était « disproportionnée au regard de la finalité de sécurité des biens et des personnes de l'immeuble » *(Délib. Cnil n° 2012-475, 3 janvier 2013)*. De même, elle a jugé disproportionné un dispositif de vidéosurveillance mis en place par un centre commercial en raison de son ampleur : 240 caméras filmant même les accès aux toilettes, salle de pause, vestiaires et cabinet médical, mettant ainsi les salariés sous une surveillance permanente à leur poste de travail. Le système était, en outre, détourné de sa finalité puisque les données étaient également utilisées pour contrôler les horaires de travail des salariés *(Délib. Cnil n° 2013-029, 12 juillet 2013 ; Délib. Cnil n° 2013-217, 17 juillet 2013)*.

À NOTER Bien qu'adoptées avant l'entrée en vigueur du Règlement général de protection des données, ces délibérations restent, à notre sens, d'actualité, au regard des principes applicables en matière de protection des données.

De plus, le système de vidéosurveillance ne doit pas être clandestin *(v. ci-après)*.

À NOTER Dans certains cas, selon les circonstances, l'installation de caméras de surveillance pourrait faire présumer l'existence d'un harcèlement moral *(Cass. soc., 14 mars 2012, n° 11-10.663*, à propos de la mise en place d'un système de vidéosurveillance dans le seul magasin où travaillait la salariée, responsable de ce magasin*)*.

Où placer les caméras ?

Selon la Cnil *(Cnil, Fiche pratique « La vidéosurveillance - vidéoprotection au travail », accessible sur www.cnil.fr)*, les **caméras** peuvent être installées au niveau des **entrées et sorties** des bâtiments, des **issues de secours et des voies de circulation**.
En revanche, elles ne doivent **pas filmer** les employés sur leur **poste de travail**, **sauf circonstances particulières** (employé manipulant de l'argent par exemple, mais alors la caméra doit davantage filmer la caisse que le caissier, entrepôt stockant des biens de valeurs au sein duquel travaillent des manutentionnaires). En effet, sur le lieu de travail comme ailleurs, les employés ont droit au respect de leur vie privée.
Les caméras ne doivent **pas** non plus **filmer** les **zones de pause ou de repos** des employés, ou les **toilettes** *(Délib. Cnil n° 2014-307, 17 juillet 2014 ; Délib. Cnil n° 2014-001, 15 janvier 2014 ; Délib. Cnil n° 2014-014, 16 janvier 2014)*.
Par exemple, si des dégradations sont commises sur les distributeurs alimentaires, les caméras ne doivent filmer que les distributeurs et non toute la pièce.
Enfin, les caméras ne doivent **pas filmer** les **locaux syndicaux** ou des représentants du personnel, ni leur accès lorsqu'il ne mène qu'à ces seuls locaux.

Quelles formalités ?

Information et consultation du comité social et économique

Comme pour les autres dispositifs de surveillance, l'**employeur** doit **préalablement informer** les **salariés** et le **comité social et économique** de la **mise en place** d'une **vidéosurveillance** dans l'entreprise. Ont ainsi été jugés constitutifs d'un moyen de preuve illicite les enregistrements provenant de caméras installées par l'employeur pour empêcher les vols par la clientèle, dès lors que ce système de vidéosurveillance était également utilisé pour contrôler les salariés sans information et consultation préalables du comité social et économique *(Cass. soc., 7 juin 2006, n° 04-43.866)*. Mais il ne suffit pas d'informer les salariés et le comité social et économique de l'existence de caméras, il faut aussi les **informer** des **finalités** du dispositif, et **préciser** expressément que les caméras pourront être **utilisées pour contrôler** l'activité professionnelle. Une information insuffisante rend les enregistrements inutilisables à cette fin, même s'ils s'avèrent accablants pour certains salariés *(Cass. soc., 10 janvier 2012, n° 10-23.482)*.
Sous peine d'inopposabilité des enregistrements recueillis, l'employeur qui met des salariés à la disposition d'une société cliente doit les informer de l'existence d'une vidéosurveillance installée sur le site de cette dernière dès lors qu'elle permet de contrôler leur activité *(Cass. soc., 10 janvier 2012, n° 10-23.482)*.
S'agissant des modalités d'information des salariés et du comité social et économique, des affichettes apposées dans un magasin ne sont pas suffisantes *(Cass. soc., 7 juin 2006, n° 04-43.866)*.

À NOTER L'employeur n'est pas soumis aux formalités d'information individuelle des salariés et de consultation du comité social et économique si le dispositif de vidéosurveillance est installé dans des locaux dans lesquels les salariés n'ont pas le droit d'aller (*Cass. soc., 11 décembre 2019, n° 17-24.179* : sous-sol du bâtiment réservé au stationnement des deux-roues ; *Cass. soc., 19 janvier 2010, n° 08-45.092* : toit d'un bâtiment dont l'accès était interdit au personnel pour des raisons de sécurité ; *Cass. soc., 19 avril 2005, n° 02-46.295* : porte d'accès d'un

local dans lequel les salariés ne devaient avoir aucune activité ; *Cass. soc., 31 janvier 2001, n° 98-44.290* : entrepôts et locaux de rangement) ou si le dispositif n'est utilisé que pour se prémunir des vols de la clientèle et pas pour contrôler les salariés dans l'exercice de leurs fonctions *(Cass. soc., 26 juin 2013, n° 12-16.564)*.

Déclaration spécifique pour les lieux ouverts au public

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

La **Cnil recommande** par ailleurs d'**aviser** les **personnes concernées** (salariés et visiteurs) au moyen d'un panneau affiché de façon visible dans les locaux sous vidéosurveillance, de l'existence du dispositif, des finalités du traitement installé, de la durée de conservation des images, du nom et du numéro de téléphone du responsable ou du délégué à la protection des données, de l'existence des droits « Informatiques et libertés » et du droit d'introduire une réclamation auprès de la Cnil. Un simple panneau « établissement sous surveillance vidéo » ne suffit pas.

Quelles sont les modalités de consultation et de conservation des images enregistrées ?

Seules les **personnes habilitées** peuvent visionner les images enregistrées (par exemple le responsable de la sécurité de l'entreprise). Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéosurveillance.

Les images captées et enregistrées au moyen du dispositif de vidéosurveillance doivent être suffisamment protégées contre des accès par des tiers non autorisés *(Délib. Cnil n° 2010-112, 22 avril 2010)*.

La **conservation des images** ne doit **pas excéder un mois**. 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. Si de telles procédures sont engagées, les images sont alors extraites du dispositif (après consignation de cette opération dans un document spécifique) et conservées pour la durée de la procédure. Lorsque c'est techniquement possible, une **durée maximale de conservation** des images doit être **paramétrée** dans le système, mais elle ne doit pas être fixée en fonction de la seule capacité technique de stockage de l'enregistreur.

LA GÉOLOCALISATION

Les salariés peuvent être géolocalisés notamment par leurs téléphones portables (GSM, Wi-Fi, etc.) et par les GPS de leurs véhicules.

À quelles conditions ?

Des finalités limitées

Selon la Cnil *(Délib. n° 2006-066, 16 mars 2006, reprise dans la fiche pratique « La géolocalisation des véhicules », accessible sur www.cnil.fr)*, l'**usage** de la géolocalisation comme moyen de contrôle de l'activité des employés peut donner lieu à des **dérives** qu'il convient de **prévenir**. Compte tenu de leur caractère intrusif, leur **mise en œuvre** n'est **justifiée** que pour un **nombre limité de finalités** :

– le **suivi** et la **facturation** de l'exécution d'une **prestation de transport** de personnes, de marchandises ou de services directement liés à l'utilisation du véhicule ;

– la **sûreté** ou la **sécurité** du **salarié** lui-même ou des **marchandises** ou **véhicules** dont il a la charge (travailleurs isolés, transports de fonds et de valeurs, etc.) ;

– l'**amélioration** du **processus de production**, soit directement par une meilleure allocation des moyens disponibles (par exemple, l'envoi du véhicule le plus proche pour exercer une activité : interventions d'urgence (ambulances, ascenseurs, etc.), chauffeurs de taxi, flottes de dépannage, etc.), soit indirectement en analysant *a posteriori* les déplacements effectués (par exemple, l'analyse des temps nécessaires à des déplacements ou à la réalisation d'une tâche) ;

– le **respect** d'une **obligation légale ou réglementaire** imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés ;

– le **contrôle** du respect des règles d'**utilisation** du **véhicule** définies par l'employeur ;

– **accessoirement**, le **suivi** du **temps de travail**, lorsque cela **ne peut être réalisé par d'autres moyens**, étant précisé que le recours à la géolocalisation n'est **pas** justifié lorsqu'un employé dispose d'une **liberté** dans l'**organisation** de son **travail** *(Cass. soc., 17 décembre 2014, n° 13-23.645)*. Appliquant à la lettre cette dernière précision, la Cour de cassation a jugé que l'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen et n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail *(Cass. soc., 3 novembre 2011, n° 10-18.036 ; CE, 15 décembre 2017, n° 403776 ; Cass. soc., 19 décembre 2018, n° 17-14.631)*.

La Cnil précise également que la géolocalisation ne doit pas servir à collecter des données relatives aux éventuels dépassements de limitation de vitesse : les infractions éventuelles ne doivent pas être identifiées, l'employeur n'étant pas habilité à les constater. Seul le traitement de la vitesse moyenne peut être réalisé.

À NOTER **L'utilisation illicite d'un système de géolocalisation peut constituer un manquement suffisamment grave pour justifier la prise d'acte de la rupture du contrat de travail aux torts de l'employeur** *(Cass. soc., 3 novembre 2011, n° 10-18.036)*.

Pas de contrôle permanent

Autre restriction au recours à la géolocalisation, celui-ci ne doit pas conduire à un contrôle permanent des salariés. Ainsi, il ne doit **pas être collecté de données** relatives à la **localisation en dehors des horaires de travail**. Les salariés doivent avoir la possibilité de désactiver la fonction de géolocalisation à l'issue de leur temps de travail, lorsque leurs véhicules (ou leurs appareils connectés) peuvent être utilisés à des fins privées.

Cette possibilité n'est pas assurée lorsque le GPS d'un véhicule de fonction permet certes de « griser » les données de localisation en dehors du temps de travail, mais que l'employeur peut lever ce « grisage » *(CA Bordeaux, 27 novembre 2012, n° 11/06565)*.

Cas des IRP

Enfin, la géolocalisation ne doit **pas être utilisée** dans le cadre de **déplacements de représentants du person-**

nel lorsqu'ils agissent dans le cadre de l'**exercice** de leur **mandat**. En effet, cela heurterait le principe de liberté de déplacement *(CA Bordeaux, 27 novembre 2012, nº 11/06565)*.
Il en irait autrement si l'employeur réussissait à prouver que ce dispositif est indispensable à la sécurité du salarié, mais à notre connaissance, aucune affaire n'a été jugée en ce sens.

Quelles modalités d'accès et de conservation des données de géolocalisation ?

L'employeur doit mettre en place des **mesures de sécurité** afin que l'**accès aux données** de géolocalisation soit limité aux seules personnes qui, dans le cadre de leur fonction, peuvent légitimement en avoir connaissance (les personnes en charge de coordonner, de planifier ou de suivre les interventions, les personnes en charge de la sécurité des biens transportés ou encore les personnes ou le responsable des ressources humaines).
Les accès individuels aux données de géolocalisation doivent s'effectuer par un **identifiant** et un **mot de passe individuels**, régulièrement renouvelés, ou par tout autre moyen d'authentification.

À NOTER Au titre du droit d'accès aux données, toute personne peut interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir la communication, sous une forme accessible, des données à caractère personnel qui la concernent. Une entreprise qui refusait à un salarié la communication de données de géolocalisation au motif que ces données ne pouvaient quitter l'entreprise a ainsi été condamnée à une sanction pécuniaire de 10 000 € *(Délib. Cnil nº 2012-213, 22 juin 2012)*. Cette position reste d'actualité dans le cadre des règles issues du RGPD.

Pour la Cnil, les **données** peuvent être **conservées au maximum deux mois**, sauf si un délai plus long est nécessaire, soit dans un objectif d'historique des déplacements à des fins d'optimisation des tournées, soit à des fins de preuve des interventions effectuées lorsqu'il n'est pas possible de rapporter la preuve de cette intervention par un autre moyen. Dans ces cas, une durée de conservation d'un an est recommandée.
Dans le cadre du **suivi du temps de travail**, les données relatives aux horaires effectués peuvent être conservées pour une durée de **cinq ans.**

LA SURVEILLANCE DE L'UTILISATION DES TÉLÉPHONES

À quelles conditions ?

Il faut distinguer le simple contrôle des relevés et l'enregistrement des conversations téléphoniques.

Contrôle des relevés téléphoniques

Dès lors que l'usage personnel par les salariés du téléphone professionnel est admis sous réserve d'une utilisation raisonnable et non préjudiciable à l'entreprise, il est légitime que l'employeur contrôle le caractère non abusif de cette utilisation, en vérifiant la **durée**, le **coût** et les **numéros des appels** téléphoniques passés à partir de chaque poste.
Une telle **vérification** ne relève pas du contrôle de l'activité des salariés et n'a **pas à être préalablement portée** à la **connaissance** du **salarié** *(Cass. soc., 29 janvier 2008, nº 06-45.279 ; Cass. soc., 15 mai 2001, nº 99-42.937)*.

QUID DE LA FILATURE ?

Une filature organisée par l'employeur pour contrôler et surveiller l'activité d'un salarié constitue un moyen de preuve illicite dès lors qu'elle implique nécessairement une atteinte à la vie privée, insusceptible d'être justifiée, eu égard à son caractère disproportionné, par les intérêts légitimes de l'entreprise *(Cass. soc., 26 novembre 2002, nº 00-42.401 ; Cass. soc., 26 septembre 2018, nº 17-16.020)*.

Toutefois, ce contrôle doit s'opérer dans des conditions propres à **garantir** le respect de la **vie privée** et des libertés des personnels sur leur lieu de travail. Pour cela, la Cnil préconise que, sur les **facturations** détaillées des **opérateurs** de téléphone, les **quatre derniers chiffres** des numéros de téléphone soient **occultés**, les supérieurs hiérarchiques ne pouvant accéder aux numéros complets des relevés individuels que de façon exceptionnelle, notamment en cas d'utilisation manifestement anormale du téléphone par un salarié *(Délib. Cnil nº 20005-019, 3 février 2005)*.

Enregistrement et écoute des conversations téléphoniques

L'écoute des conversations téléphoniques des salariés obéit à des règles beaucoup plus strictes. Selon la Cnil *(Cnil, Fiche pratique « L'écoute et l'enregistrement des appels », accessible sur www.cnil.fr)*, l'**enregistrement** des conversations téléphoniques ne peut être réalisé qu'en cas de **nécessité reconnue** et doit être **proportionné** aux objectifs poursuivis. Un employeur est ainsi en droit d'installer un dispositif d'écoute ou d'enregistrement ponctuel pour :
– **former** ses **salariés** ;
– les **évaluer** ;
– **améliorer** la **qualité du service**.
Dans ce cadre, l'employeur ne peut collecter que les données nécessaires à l'objectif poursuivi.
L'écoute ou l'enregistrement ne peut **pas** présenter un **caractère permanent ou systématique**, sauf exigence légale. La Cour de cassation interdisant un enregistrement à l'insu du salarié *(Cass. soc., 16 mars 2011, nº 09-43.204)*, le salarié doit être informé des plages d'activité pendant lesquelles il est susceptible d'être enregistré.
La Cnil exige par ailleurs que la fonction enregistrement puisse être **neutralisée** pour les **appels privés** : les salariés doivent disposer de lignes téléphoniques non reliées au système d'enregistrement ou d'un dispositif technique leur permettant, en cas de conversation privée, de se mettre hors du champ du dispositif d'enregistrement. Ce principe s'applique *a fortiori* pour les représentants du personnel dans le cadre de l'exercice de leur mandat.
Appliquant à la lettre cette préconisation, la Cour de cassation a jugé que pour l'accomplissement de leur mission légale et la préservation de la confidentialité qui s'y attache, les salariés protégés investis d'un mandat électif ou syndical doivent pouvoir disposer sur leur lieu de travail d'un matériel ou procédé excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants *(Cass. soc., 4 avril 2012, nº 10-20.845 ; Cass. soc., 6 avril 2004, nº 02-40.498)*.

À NOTER Les SMS envoyés aux temps et lieu de travail à l'aide d'un téléphone professionnel sont présumés professionnels, de sorte que l'employeur peut les consulter

librement et les invoquer à l'appui d'une sanction disciplinaire dès lors que leur contenu est en rapport avec l'activité professionnelle et ne relève pas uniquement de la sphère privée *(Cass. soc., 28 septembre 2011, n° 10-16.995)*.

Quelles formalités ?

Comme tout dispositif de surveillance des salariés, l'employeur doit **informer** les **salariés** et **consulter** le **comité social et économique** préalablement à la mise en place de dispositifs d'écoute ou d'enregistrement des communications.

L'**enregistrement** d'une conversation à l'insu de l'intéressé est prohibé et constitue un procédé déloyal rendant irrecevable en justice la preuve ainsi obtenue *(Cass. soc., 16 mars 2011, n° 09-43.204 ; Cass. soc., 29 janvier 2008, n° 06-45.814)*. En revanche, si les salariés sont dûment avertis que leurs conversations téléphoniques sont écoutées, ces écoutes réalisées constituent un mode de preuve valable *(Cass. soc., 16 décembre 2008, n° 07-43.993 ; Cass. soc., 14 mars 2000, n° 98-42.090)*.

À NOTER Les interlocuteurs doivent pour leur part être informés sur l'enregistrement possible des conversations téléphoniques, la finalité poursuivie et sur leur droit de s'y opposer. Afin d'être en mesure d'exercer ce droit, l'information doit leur être faite avant la fin de la conversation téléphonique.

Quid de l'accès et de la durée de conservation ?

Selon la Cnil, seules peuvent écouter ou accéder aux données les **personnes habilitées** des **services concernés** par l'objectif poursuivi : formateur, supérieur hiérarchique, etc.

La **durée maximale de conservation** des **enregistrements** est en principe de **six mois**. Les **comptes-rendus** des conversations téléphoniques et grilles d'analyse sont quant à eux conservés pour une durée d'**un an** maximum.

À NOTER La Cnil recommande la pratique des « enregistrements tampons » : celle-ci consiste à ce que les enregistrements soient écoutés dans les jours suivant leur réalisation et donne lieu à la rédaction des documents d'analyse nécessaire. De la sorte, les enregistrements peuvent être rapidement supprimés et n'ont pas à être conservés pendant six mois.

Lorsque les enregistrements sont réalisés à des fins de preuve en matière bancaire, la durée de conservation doit être conforme aux articles 321-78 et 321-79 du Règlement général de l'Autorité des marchés financiers (cinq ans maximum).

LA SURVEILLANCE DE LA MESSAGERIE PROFESSIONNELLE

À quelles conditions ?

Mails privés/mails professionnels

De manière générale, les entreprises peuvent, selon la Cnil, mettre en place des outils de **contrôle** de la **messagerie** au nom d'**exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau** *(Cnil, Fiche pratique « Les outils informatiques au travail »)*. Il peut s'agir d'outils de mesure de la fréquence et/ou de la taille des messages électroniques ou d'outils d'analyse des pièces jointes (détection des virus, filtres « antispam » destinés à réduire les messages non sollicités, etc.).

L'arrêt Nikon a **toutefois** consacré le **droit au secret** des **messages personnels** émis et reçus par les salariés grâce à un outil informatique mis à sa disposition pour leur travail, et ce, même si, l'employeur a interdit une utilisation non professionnelle de l'ordinateur *(Cass. soc., 2 octobre 2001, n° 99-42.942)*.

À NOTER Les messageries des instances représentatives du personnel doivent rester parfaitement confidentielles, comme d'ailleurs toute leur activité informatique dans le cadre de leur mandat.

Comment les distinguer ?

Les **courriels** adressés ou reçus par le salarié à l'aide de l'**outil informatique mis à** sa **disposition par l'employeur** pour les besoins de son travail sont **présumés** avoir un caractère **professionnel** : l'employeur est en droit de les ouvrir en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels *(Cass. soc., 15 décembre 2010, n° 08-42.486 ; Cass. soc., 16 mai 2013, n° 12-11.866)*.

La **mention du caractère personnel** des messages doit avoir été **portée textuellement** par le salarié *(Cass. soc., 30 mai 2007, n° 05-43.102)*. À défaut d'une telle mention, les messages sont présumés être professionnels *(Cass. soc., 9 septembre 2020, n° 18-20.489)*.

La Cnil recommande aux salariés de faire figurer la mention « **personnel** » **ou** « **privé** » dans l'**objet du message** ou dans le nom du **répertoire** dans lequel il est stocké *(Cnil, Fiche pratique « Les outils informatiques au travail »)*.

En revanche, l'employeur ne peut **pas accéder**, en dehors de la présence et sans l'accord du salarié, à la **messagerie personnelle** que celui-ci a **installée** sur son **ordinateur professionnel** : cette messagerie est en effet protégée par le secret des correspondances *(Cass. soc., 26 janvier 2012, n° 11-10.189 ; Cass. soc., 26 janvier 2016, n° 14-15.360 ; Cass. soc., 7 avril 2016, n° 14-27.949 ; Cass. soc., 23 octobre 2019, n° 17-28.448)*. Mais les messages et pièces jointes enregistrés sur le disque dur de l'ordinateur professionnel mis à disposition du salarié sont présumés avoir un caractère professionnel : le seul fait qu'ils émanent de la messagerie personnelle du salarié ne les identifie pas comme personnels *(Cass. soc., 19 juin 2013, n° 12-12.138)*.

À NOTER Même si le message n'est pas identifié comme personnel, si son contenu se rattache uniquement à la vie privée du salarié, il bénéficie de la protection attachée à la vie privée. La conversation perd toutefois son caractère privé si elle a un rapport avec l'activité professionnelle :

– deux salariés échangeant en des termes désobligeants sur un supérieur hiérarchique ou un collègue *(Cass. soc., 2 février 2011, n° 09-72.449 ; Cass. soc., 11 février 2011, n° 09-72.313)* ;

– échanges de messages entre une employée et son supérieur hiérarchique dans lesquels transparaît une confusion entretenue entre les sphères privée et professionnelle *(Cass. soc., 1er décembre 2015, n° 14-17.701)*.

Limites au droit de contrôler les mails professionnels

Le **règlement intérieur peut restreindre** le **pouvoir de consultation** des documents présumés professionnels en imposant par exemple la présence du **salarié** lors de la consultation *(Cass. soc., 26 juin 2012, n° 11-15.310)*.

Par ailleurs, la Cnil considère excessif le fait, pour la hiérarchie, de paramétrer le système de manière à recevoir en copie automatique tous les messages écrits ou reçus *(Cnil, Fiche pratique « Les outils informatiques au*

travail »). Elle condamne également les « keyloggers », dispositifs qui permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur, sauf fort impératif de sécurité (lutte contre la divulgation de secrets industriels, par exemple).

Limites au droit au secret des mails privés

Le fait qu'un courriel soit clairement identifié comme personnel n'empêche pas toute **consultation** par l'employeur. En effet, l'employeur pourra ouvrir le message, mais en **présence** de l'**intéressé**, ou, *a minima*, en l'ayant fait dûment appeler *(Cass. soc., 17 mai 2005, nº 03-40.017).*

Il ressort de ce même arrêt que les courriels peuvent être consultés sans la **présence du salarié si** l'employeur justifie d'un **risque ou** d'un **événement particulier** justifiant l'atteinte portée à la vie privée *(Cass. soc., 10 mai 2012, nº 11-13.884),* la réalité de ces « risques ou événements particuliers » dépendant de l'appréciation des juges et étant donc à manier avec précaution.

Mais, dans ce cas, ou si le salarié, présent, refuse l'ouverture de ses messages, l'appel à un **huissier** est recommandé.

Par ailleurs, l'article 145 du Code de procédure civile permet à l'employeur d'**accéder** aux messages privés **sur décision de justice** *(Cass. soc., 23 mai 2007, nº 05-17.818; Cass. soc., 10 juin 2008, nº 06-19.229),* à condition qu'il justifie d'un **motif légitime de** conserver ou établir avant tout procès la **preuve** des faits dont pourrait dépendre la solution d'un litige.

Quelles formalités ?

Un **système de messagerie professionnelle qui ne s'accompagne pas d'un dispositif de contrôle individuel** de l'activité de salarié n'a **pas à répondre** aux **exigences** propres aux dispositions de surveillance des salariés, qu'il s'agisse de l'**information préalable** du salarié et de la **consultation** du **comité social et économique**, ou du respect des règles issues du RGPD : l'employeur peut ainsi librement produire en justice les messages adressés par l'employeur ou par le salarié *(Cass. soc., 1er juin 2017, nº 15-23.522).*

À l'inverse, les dispositifs de contrôle de la messagerie, comme par exemple un dispositif de contrôle de l'importance et du flux des messages *(Cass. soc., 8 octobre 2014, nº 13-14.991)* doivent donner lieu à une consultation du comité social et économique, à une information individuelle des salariés, et au respect des règles relatives à la protection des données.

LA SURVEILLANCE DE L'UTILISATION DE L'ORDINATEUR PROFESSIONNEL

À quelles conditions ?

Les fichiers informatiques

Comme pour les mails transitant par la messagerie professionnelle, l'**employeur peut accéder relativement librement** aux fichiers informatiques **stockés** sur l'**ordinateur professionnel** du salarié. Sauf si le salarié les identifie comme étant personnels, les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés avoir un caractère professionnel, de sorte que l'employeur peut y avoir accès, même hors la présence du salarié *(Cass. soc., 10 mai 2012, nº 11-13.884).*

En revanche, l'employeur ne peut **consulter** les **fichiers clairement identifiés comme personnels** que si l'**intéressé** est **présent** ou a été dûment appelé, **ou** en cas de **risque ou d'événement particulier** justifiant l'atteinte portée à la vie privée *(Cass. soc., 17 juin 2009, nº 08-40.274).*

Là encore, comment distinguer un fichier personnel d'un fichier professionnel ? La jurisprudence n'admet guère d'autre signe d'identification que la mention « personnel » ou à la limite « perso » *(Cass. soc., 17 mai 2005, nº 03-40.017).*

Ainsi, n'ont pas été considérés comme personnels :

– un répertoire identifié par les initiales du salarié *(Cass. soc., 21 octobre 2009, nº 07-43.877)* ;

– un répertoire dont l'intitulé était le prénom du salarié *(Cass. soc., 8 décembre 2009, nº 08-44.840)* ;

– un fichier dénommé « Mes documents » *(Cass. soc., 10 mai 2012, nº 11-13.884).*

Selon la même logique, le fait de mettre un code d'accès sur son ordinateur professionnel ne lui donne pas nécessaire un caractère privé *(Cass. soc., 8 décembre 2009, précité).* Idem pour la tactique consistant à renommer son disque dur « D:/données personnelles » : cela ne confère pas un caractère personnel à l'intégralité des données qu'il contient et ne le protège pas de toute consultation par l'employeur *(Cass. soc., 4 juillet 2012, nº 11-12.502 D).* La Cour de cassation a, sur cette position, été suivie par la Cour européenne des droits de l'Homme *(CEDH, 22 février 2018, req. nº 588/13).*

À NOTER **Dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, la clé USB appartenant au salarié est présumée utilisée des fins professionnelles, de sorte que l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié** *(Cass. soc., 12 février 2013, nº 11-28.649 FS-PB).*

Les connexions internet

Selon la Cnil, l'**employeur** est **libre de fixer les conditions et limites** de l'utilisation d'internet par les salariés *(Cnil, Fiche pratique « Les outils informatiques au travail »).* Ainsi, il peut mettre en place des dispositifs de filtrage de sites non autorisés (sites à caractère pornographique, pédophile, d'incitation à la haine raciale, etc.). Il peut également fixer des limites dictées par des exigences de sécurité, telles que l'interdiction de télécharger des logiciels, de se connecter à des forums ou d'utiliser les « chats », l'interdiction d'accéder à une boîte aux lettres personnelle compte tenu des risques de virus qu'un tel accès est susceptible de présenter, etc.

La jurisprudence considère que l'employeur a par conséquent le droit de surveiller les connexions internet de ses salariés grâce à l'**historique des sites visités** durant le **temps de travail** à l'aide de l'**ordinateur professionnel**, étant précisé que pour contrôler les connexions internet, la présence du salarié n'est pas requise *(Cass. soc., 9 février 2010, nº 08-45.253, Cass. soc., 9 juillet 2008, nº 06-45.800).*

À NOTER **En cas d'utilisation abusive d'internet, les salariés encourent des sanctions pouvant aller jusqu'au licenciement disciplinaire. C'est notamment le cas lorsqu'ils consultent des sites à connotation sexuelle** *(Cass. soc., 10 mai 2012, nº 10-28.585),* **mais également lorsqu'ils consacrent une part excessive de leur temps de travail à la consultation de sites privés parfaitement légaux** *(Cass. soc., 26 février 2013, nº 11-27.372* **: faute grave d'une salariée en raison de 10 000 connexions à des sites extraprofession-**

nels en moins de trois semaines de travail ; *Cass. soc., 18 décembre 2013, n° 12-17.832* : licenciement pour faute d'un salarié ayant téléchargé et envoyé à ses collègues des vidéos « consistant en dessins animés, scènes de sexe, d'humour, de politique, de football féminin », dont 178 envoyées sur l'adresse professionnelle d'une seule de ses collègues). L'employeur doit toutefois être en mesure de prouver que le salarié est bien l'auteur des connexions *(Cass. soc., 3 octobre 2018, n° 16-23.968)*.

Quelles formalités ?

Comme pour tout moyen de surveillance des salariés, le comité social et économique doit avoir été **consulté** et les **salariés informés au préalable** des dispositifs mis en place et des modalités de contrôle de l'utilisation de l'outil informatique, notamment quant à la finalité du dispositif de contrôle, à l'identité des destinataires des données et à la durée pendant laquelle les données de connexion sont conservées.

Lorsque l'entreprise met en place un dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste, le traitement ainsi mis en œuvre doit respecter les règles relatives à la protection des données personnelles. Tel est par exemple le cas d'un logiciel de contrôle permettant d'analyser les données de connexion de chaque salarié ou de calculer le temps passé sur Internet par un salarié déterminé.