Jacqueline PADEY
Avocat
Toque 605

LE CONTROLE DU SALARIE

L'arrivée en force des nouvelles technologies de l'information et de communication (NTIC) a modifié les modalités du contrôle et de la surveillance du salarié

Aux modes de surveillance connus (badge électronique ou vidéo surveillance) sont venus s'adjoindre de **nouveaux procédés de contrôle liés à l'informatisation des postes de travail , à la géo localisation des véhicules et des salariés, ou encore aux applications biométriques.**

L'employeur peut ainsi collecter de manière invisible de nombreuses informations personnelles sur le salarié, évaluer le respect des règles de discipline, le respect des obligations contractuelles (exécution loyale du contrat de travail, discrétion, respect des consignes..). Il peut établir un manquement entrainant éventuellement une sanction.

Enfin le salarié a généralement la possibilité de faire un usage personnel des NTIC que l'employeur met à sa disposition (internet, messagerie outils bureautiques) , dès lors il faut concilier le droit de contrôle et de surveillance reconnu à l'employeur et le droit à la vie privée du salarié y compris sur le lieu de son travail.

Plan de l'intervention :

- principes applicables au contrôle du salarié
- différents modes de contrôle
    - accès et circulation dans l'entreprise
    - matériel de l'entreprise
    - activité et comportement du salarié

55 rue de la République – 69002 LYON
Téléphone 04 37 23 62 60 –

I - CONDITIONS GENERALES DU CONTROLE

- la loi informatique et libertés 6 janvier 1978
- la CNIL COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

La Commission nationale de l'informatique et des libertés (CNIL) a pour mission de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni aux droits de l'homme, ni à l'identité humaine, ni à la vie privée, ni aux libertés individuelles ou publiques .

1- Respect des droits et libertés du salarié

L'article L 1121-1 du code du travail : référence principale s'agissant de la légitimité d'un dispositif de contrôle : **nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionné au but recherché**

Double conditions:
- Une justification (ex contrôle des entrées et sorties de l'entreprise, l'utilisation matériel)
- La proportionnalité de l'atteinte aux droits et libertés avec le but recherché

2- information préalable du salarié

L'article L1222-4 du code du travail prévoit qu'aucune information concernant personnellement le salarié ne peut être collectée par un dispositif qui n'a pas été porté à sa connaissance préalablement :

Pas de dispositif clandestin.
Information préalable précise et sans ambiguïté du salarié
Pas de stratagème :

3- information et consultation des représentants du personnel

Consultation du Comité d'Entreprise sur les moyens et techniques permettant un contrôle des salariés **(art L 2323-32 ali3** du code du travail)

Caractère **impératif de** cette obligation à défaut la preuve tiré d'un moyen de contrôle installé sans consultation du CE est illicite.

Consultation CHSCT : article L 4612-8 du code du tr avail en cas d'impact sur la santé ou la sécurité des salariés (ex stress accru des salariés opérateurs enregistrés automatiquement et dont l'autonomie est limitée de ce fait)

4- déclaration à la CNIL obligatoire de tout système de contrôle automatisé des données personnelles

La déclaration à la CNIL ne peut être utilisée à d'autres fins que celles, objet de la déclaration.
A titre d'exemple la déclaration faite dans le but de surveiller les clients ne peut servir de preuve des absences des salariés

5- sanctions

Irrecevabilité des preuves récoltées et inopposabilité du dispositif en cas de non déclaration à la CNIL

(Ex refus d'utiliser un badge électronique non déclaré à la CNIL n'est pas une faute justifiant une sanction.)

Un dispositif non déclaré ou non soumis à l'information consultation du CE peut être suspendu par :

- le juge des référés car trouble manifestement illicite constitué par le défaut de déclaration CNIL ou consultation CE
- Bureau de jugement du Conseil des Prud'hommes peut ordonner le retrait d'un dispositif de contrôle
- la CNIL : article 45 loi informatique et libertés 6/01/1978 peut suspendre un traitement de données à caractère personnel outre amende

Sanction pénale : article 226-15 CPénal réprime les atteintes à la vie privée, (images/paroles) ainsi que la violation des correspondances,
Un délit d'entrave peut être constitué en l'absence de consultation CE/CHSCT

II CERTAINS MODES DE CONTROLE

- circulation dans l'entreprise badge, dispositif biométrique
- utilisation par les salariés du matériel de l'entreprise : informatique , téléphone
- contrôle de l'activité et comportement du salarié par la vidéo surveillance, enregistrements, géolocalisation

A- CIRCULATION DANS L'ENTREPRISE

L'employeur ne peut entraver la liberté de circulation des Délégués du personnel.

1- badge

L'obligation faites au salarié de porter un badge nominatif permettant de s'identifier ou d'utiliser un badge électronique permettant de contrôler l'accès à l'entreprise et notamment leur temps de travail s'apprécie cas par cas.

- badge et horaire variable : :La mise en œuvre d'**horaires individualisés** doit s'accompagner d'un système de **décompte de la durée du travail** (**badge**, pointeuse, registre…) permettant de contrôler l'horaire effectué par le salarié

- BADGE ELECTRONIQUE ou puce électronique : ils comportent plus de risques d'atteintes à la vie personnelle et aux libertés des salariés car ils permettent l'enregistrement d'informations nominatives et peuvent suivre ses déplacements.

2- dispositif biométrique

C'est l'ensemble des dispositifs permettant d'identifier automatiquement une personne à partir de ses caractéristiques physique (main, rétine visage..) ou biologique (ADN) ou comportementaux (voix, signature, écriture)

Strictement encadré par la CNIL en raison du risque d'atteinte à la vie privée. (Communiqué CNIL 12/01/2006)

Le badge utilisant la technique des empreintes digitales ne se justifie que si elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés.

TGI PARIS 1ère chambre 29/04/2005 n°05-382 Ce système biométrique ne peut être mis en place pour contrôler le temps de travail.

B-CONTROLE DE L'UTILISATION DU MATERIEL DE L'ENTREPRISE

Ce contrôle peut avoir pour objet de vérifier:

- l'utilisation abusive de ce matériel à des fins privés (teléphone, fax, ordinateur, connexion internet, messagerie électronique)
- l'utilisation du matériel informatique dans des conditions de sécurité mettant en jeu la sécurité du réseau
- l'exécution par le salarié de son travail et de ses obligations professionnelles

L'utilisation abusive du matériel de l'entreprise peut entrainer une sanction voire un licenciement.

1- PRINCIPE :

L'employeur qui entend interdire ou fixer des limites à l'utilisation à des fins personnelles du matériel de l'entreprise le fait en général par un écrit soit :

- **Règlement intérieur** : rubrique « règles générales et permanentes de discipline »

- **note de service** : dans les entreprises non soumis à règlement intérieur (- de 20)

- **une charte informatique** qui encadre et sécurise l'usage du réseau informatique informe le salarié de ses droits et obligations

Nature juridique :

- annexe du Règlement Intérieur /contenu disciplinaire au sens de l'article L 1321-1 du code du travail puisqu'elle porte des prescriptions générales relatives à la discipline dans l'utilisation extra professionnelle du matériel informatique
En l'absence des formalités de dépôt et de publicité requises elle constitue un engagement unilatéral de l'employeur °

La charte fixe des règles concernant

- la sécurité du réseau : interdiction de télécharger certains logiciels par exemple
- Les attributions de l'administrateur réseau de l'entreprise et les contrôles que ce dernier peut être amené à effectuer
- l'usage abusif des NTIC : info sur les sites interdits (jeux sites porno ou négationnistes…)
- la prévention des comportements à risques (injures violences,..)
- l'utilisation de l'intranet et de la messagerie par les représentants du personnel ou les représentants syndicaux.

L'employeur peut limiter l'utilisation à des fins privées ce qui ne constitue pas une atteinte à la vie privée des salariés.

Etendue du contrôle :

Rapport CNIL 28/03/2001 :l'interdiction totale et absolue d'utilisation du matériel bureautique et informatique à des fins personnelles n'est pas raisonnable et selon la jurisprudence l'interdiction absolue porte atteinte aux libertés du salarié, est disproportionnée au sens de l'article L1221-1 du Code du Travail.

La Cour de Cassation a admis la protection des messages électroniques personnels du salarié même lorsque l'utilisation de l'ordinateur était interdite.

L'usage à des fins personnelles doit être raisonnable :
La jurisprudence sanctionne :

- le caractère répété ou systématique de l'utilisation du matériel à des fins personnelles
- le temps passé à titre personnel sur les NTIC au détriment de son activité professionnelle

2- MATERIEL INFORMATIQUE

L'ordinateur professionnel remis au salarié ne relève pas de sa vie privée et n'est pas en tant que tel protégé par la loi Informatique et Liberté

Il peut comporter subsidiairement des informations relevant de la vie privée du salarié , être protégé par un mot de passe et un login : ceci ne transforme pas l'ordinateur en un ordinateur privé.

Rôle de l'administrateur réseau : chargé de la gestion du réseau informatique

- obligation de confidentialité, (rappelée dans la charte d'utilisation du matériel informatique annexée au Règlement Intérieur.)
- accès aux données personnelles du salarié ne peut être justifié que s'il n'existe pas d'autres moyens d'assurer le bon fonctionnement des systèmes informatiques.
- aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité du réseau

Prise en main distance : aucune déclaration obligatoire à la CNIL de ce logiciel.

Preuve de l'usage abusif:

Pour justifier que le salarié a fait un usage abusif du matériel informatique il faut que l'employeur :

- ait recours à un mode de contrôle licite (information du salarié, consultation CE, etc..
- justifie que les faits établis sont imputables au salarié,
- la charge de la preuve pèse sur l'employeur.

Exemple Cass Soc 2/06/2004 n° 03-45269, l'employeur doit prouver que c'est bien le salarié qui est l'auteur d'un courriel incriminé/ problème en l'absence de mot de passe empêchant l'accès à d'autres salariés l.

Les horaires de connexion ne rapportent pas la preuve des absences ou retard d'un salarié pour la COUR D'APPEL de VERSAILLES 7-12-2004 n°05-5384

a/accès de l'employeur au disque dur aux fichiers et messages informatiques

FICHIERS INFORMATIQUES

- **fichiers non identifiés « personnel » dans un ordinateur mis à disposition :**

Principe :

Présomption de caractère professionnel sauf si le salarié identifie le fichier comme personnel.
La même solution est retenue pour les documents papiers détenus par le salarié à son bureau.

la notion de fichier ou dossier « personnel » selon la jurisprudence :

- fichier « mes documents » est insuffisant pour caractériser un document personnel (cass soc 10-05-2012)
- fichier avec les initiales du nom et prénom est insuffisant pour caractériser un document personnel (cass soc 21-10-2009)
- un fichier portant un code d'accès ou l'intitulé d'un répertoire ainsi que le prénom de l'utilisateur n'a pas été jugs personnel (cass soc 8-12-2009)
- idem le fichier dénommé « fichier divers B »

- la dénomination donnée par le salarié au disque dur de son ordinateur ne confère pas le caractère personnel à l'intégralité des données : ex un cadre SNCF, radié car 1500 fichiers pornographiques ont été découverts dans son disque dur, invoquait comme moyen de défense le caractère privé de l'intégralité du disque dur qu'il avait dénommé « D/DONNEES PERSONNELLES », or seule importe la dénomination des répertoires et fichiers figurant sur le disque dur . en l'état les fichiers nommés « rires » « Catherine » « socrif » n'ont pas été considérés comme personnels.
  (Cass soc 4-07-2012 n° 11-12502)

Le salarié a droit même sur son lieu de travail au respect de son intimité : si l'employeur peut consulter les fichiers non identifiés comme personnels, il ne peut les utiliser pour sanctionner une faute s'ils se révèlent comporter des éléments relevant de sa vie privée.
Distinction du droit de contrôle et du droit de s'en prévaloir
Cass Soc 5-07-2011 n°10-17284

- **fichier identifié comme personnel**

Principe ; sauf risque ou évènement particulier, la présence du salarié est obligatoire pour l'ouverture des fichiers ou celui-ci dument appelé.

A défaut de présence du salarié ou s'il n'a pas été régulièrement convoqué, les informations recueillies ne sont pas licites : ex faute grave invoquée par l'employeur qui a trouvé des photos compromettantes dans un fichier identifié personnel et ouvert sans la présence du salarié, le licenciement est jugé sans cause réelle ni sérieuse, la preuve écartée car illicite.
cass soc 17 mai 2005

L'employeur ne peut faire une copie du disque dur clandestinement, pour l'examiner à l'insu du salarié : manquement à l'article 8 de la Convention Européenne de Sauvegarde des droits de l'homme.

Risque ou évènement particulier justifiant l'ouverture de fichier personnel sans la présence du salarié :

Ex accès de l'employeur hors présence du salarié à un fichier dénommé personnel sur lequel était installé un logiciel permettant des téléchargements illégaux musicaux ; licenciement faute grave validé (CA VERSAILLES 31 mars 2011 n°09-742)

Si l'employeur obtient en justice la désignation d'un huissier (art 145 Code de Procédure Civile) afin de prendre connaissance de fichiers identifiés personnels vu le risque particulier justifié, un fichier personnel peut être ouvert hors la présence du salarié.
En revanche un huissier mandaté par l'employeur sans autorisation de justice ne peut prendre connaissance d'un fichier identifié personnel.

Salarié en congé : manquement à son obligation de loyauté s'il refuse de communiquer son mot de passe permettant l'accès à l'ordinateur nécessaire à l'activité de l'entreprise.

Une clé USB, dès lors qu'elle est connectée à l'outil informatique mis à disposition du salarié est présumée utilisée à des fins professionnelles : l'employeur peut donc avoir accès aux fichiers non identifiés comme personnels, qu'elle contient.
C'est une simple extension du stockage de l'ordinateur.
(cass soc 12-02-2013n°11-28649)

Posée sur le bureau, à moins d'être étiquetée « personnelle», la clé USB est présumée professionnelle.

MESSAGES ELECTRONIQUES

La CEDH estime justifiée le contrôle raisonnable de la messagerie professionnelle du salarié
CEDH 12-01-2016

- **L'accès de l'employeur aux messages dépend de leur caractère personnel ou non .**

- Des mesures de sécurité peuvent être prises dans des entreprises soumises à des contraintes particulières

  Des recherches sur la base de mots clés, de volume ou de taille des messages peuvent être mises en place pour notamment réguler le flux ou garder copie de sauvegarde des messages échangés. L'entreprise doit en informer les utilisateurs.

- contrôle des messages du salarie

  - Droit au secret des correspondances même en cas d'utilisation professionnelle de l'ordinateur sous réserve que le courriel soit identifié comme personnel. A défaut d'identification personnelle : présomption de caractère professionnel et l'employeur peut en prendre connaissance hors présence du salarié.

  - Le règlement intérieur peut restreindre le pouvoir de consultation de l'employeur toutefois une Clause prévoyant « les boites de messageries électroniques pourront être consultées par la direction en présence du salarié » est nulle car elle ne distingue pas les messages identifiés personnels et ceux non personnels ;

    En présence d'une telle clause dans le règlement intérieur, le contrôle de l'employeur sur des fichiers d'un salarié même non identifiés comme personnels est illicite.
    Cass soc 26-06-2011

- messages personnels reconnus : libellé (ex vacances) ou classement dans un fichier intitulé « PRIVE »

Exemple : les messages litigieux provenant de la messagerie personnelle du salarié distinct de la messagerie professionelle dont celui-ci disposait pour les besoins de son activité doivent être écartés des débats car leur production viole le secret des correspondances
Cass Soc 26-1-2016 n°14-15360

Un courriel échangé entre un salarié et un client dans un fichier personnel du salarié a un caractère personnel.

MAIS un salarié qui diffuse un message insultant depuis son domicile ne peut se prévaloir du secret des correspondances dès lors que ce message a été transmis sur la messagerie accessible à tout un service de l'entreprise
Idem en cas de transmission sur INTRANET.

- Delit de violation des correspondances

Article 226-5 du code pénal

L'employeur qui accède à la messagerie personnelle, identifiée comme telle et en prend connaissance viole le secret des correspondances
cass soc 7-04-2016 n°01427949

b//TRACAGE INFORMATIQUE

Le contrôle de l'employeur peut passer par un contrôle des logs de connexion (appelés également traces) ou par un contrôle des contenus (mails vus précédemment)

L'ordinateur peut enregistrer tout ce qui a été fait sur la machine, sa capacité de mémoire constitue un élément essentiel de ses performances : véritable boite noire de l'activité de son utilisateur.

- Obligations de l'employeur :

Informer les salariés : l'employeur qui conserve les logs de connexion de ses salariés se livre à un traitement de données à caractère personnel : il doit donc informer les salariés.

Informer le CE : la conservation des logs est un moyen de contrôle de l'activité du salarié , une information consultation du CE est obligatoire.

Déclarer à la CNIL : si les logs de connexion permettent de retracer l'activité de chaque salarié, la déclaration doit être « normale », dans le cas contraire , la déclaration est dite « simplifiée »
Si un correspondant Informatique et Libertés a été nommé dans l'entreprise : exonération de déclaration auprès de la CNIL

Limiter la durée de conservation des logs : les logs de connexion constituant des données personnelles, leur durée de conservation doit être limitée. La CNIL recommande 6 mois.

- Prérogatives de l'employeur :

Accéder aux logs de connexion des salariés présumés professionnels.
Sanctionner un usage abusif à des sites extra professionnels depuis son lieu de travail et pendant son temps de travail .

*c/- **CONNEXION INTERNET***

- La connexion internet de l'entreprise utilisée par le salarié est présumée professionnelle.

- l'inscription d'un site sur la liste des « favoris » ne démontre pas le caractère personnel

- l'autorisation de travailler à domicile vaut reconnaissance d'un usage privé : licenciement infondé d'un salarié connecté le dimanche à un site dont l'employeur estimait qu'il nuisait à l'image de l'entreprise.

- Accès aux réseaux sociaux :

Deux problèmes fréquents :
L'accès des salariés à des plateformes de communication en ligne
Le contrôle des propos tenus.

L'employeur peut mettre une place un filtrage ou interdire totalement ces connexions au travers du Règlement intérieur ou de la charte informatique ou par note de service le cas échéant et en l'absence de Règlement intérieur.

La question du contrôle des propos est complexe. Elle met en jeu la liberté d'expression, le respect de la vie privée et le secret de la correspondance sachant que ces correspondances peuvent être accessibles à un plus ou moins grand nombre d'internautes. Ne faut-il protéger que lorsque le salarié s'est lui-même protégé ?

À propos du réseau social FACEBOOK :
vu son organisation et sa finalité il peut être considéré comme un espace public.
L'internaute qui souhaite assurer la confidentialité de ses propos doit s'assurer qu'il a limité l'accès à son « mur » ou adopter des fonctionnalités adéquates

La CNIL recommande de créer des listes pour répartir ses contacts : famille, amis proches, moins proches…puis à adapter ses paramètres de confidentialité en fonction de la liste.

3-TELEPHONE

Un dispositif d'écoute et d'enregistrement des conversations du personnel ne peut être mis en place par l'employeur que s'il *est proportionné* et justifié soit :
Lorsque le téléphone est l'outil de travail et sert à l'évaluation du salarié
Lorsqu'il sert à la formation (banque, assurance)
Lorsque le travail est fait exclusivement par téléphone (exemple ordre commercial passé par ce biais)

CNIL : employeur doit prévoir la possibilité de téléphoner hors enregistrement.

Le salarié doit être averti, seul l'emploi d'un procédé de contrôle clandestin est interdit
Délit d'atteinte à la vie privée 226.1 du CODE PENAL : ex écoute des conversations dans un local lors des pauses alors que des sujets professionnels et privés étaient abordés.

Téléphone mobile de fonction

Présomption de caractère professionnel des SMS, l'employeur peut librement consulter les SMS non identifiés comme personnels. Il ne peut toutefois en invoquer le contenu à l'encontre du salarié si ce contenu s'avère relever de la vie privée de l'intéressé.

En revanche si l'enregistrement d'une conversation téléphonique privée à l'insu de l'auteur des propos est un procédé déloyale et irrecevable, l'utilisation des SMS par son destinataire , notamment pour prouver des faits de harcèlement sexuel, est recevable car l'expéditeur du SMS ne peut ignorer qu'il est enregistré.
Cass Soc 23/05/2007 n°06-43209

4/AUTRES MATERIELS/

Véhicule : disque chronotachygraphe est une obligation légale dans le transport, l'absence de déclaration à la CNIL ne prive pas l'employeur du droit de s'en prévaloir
Cass Soc 14-01-2014

C – CONTROLE DE L'ACTIVITE PENDANT LE TEMPS DE TRAVAIL

1-VIDEO SURVEILLANCE

a/ surveillance des lieux de travail

Dans les établissements ouverts au public, l'autorisation du préfet est requise après avis de la commission départementale.

Dans les entreprises / établissement non ouvert au public: déclaration à la CNIL et information des salariés

- obligation d'informer et consulter le CE
- obligation d'information des salariés
- principe de proportionnalité : la vidéo surveillance doit répondre à une préoccupation particulière dans un lieu exposé : risque de vol, poste dangereux, obligation de secret ou discrétion.

Conditions d'utilisation :

- Si la consultation / information du CE n'a pas été effectuée, les salariés ne sont pas considérés comme étant informés, la vidéo ne peut servir de preuve

CA PARIS 4.3.2016 n°12/10491

- La déclaration à la CNIL est déterminante :

Ainsi l'employeur ne peut contrôler l'heure d'arrivée des salariés alors que la déclaration CNIL ne concerne que la surveillance des clients

Une société de nettoyage ne peut se servir de l'enregistrement de la société cliente. comme preuve d'une faute d'un de ses salariés présent sur le site (abandon de poste) .

Si la vidéo surveillance est installée dans un local auquel le salarié n'a pas accès pour son activité, la preuve d'une faute enregistrée par vidéo surveillance sans information préalable, est licite puisque la présence du salarié en ce lien est indépendante de sa qualité de salarié

visionnage des images :

Art 36 loi Informatique et Libertés : seulement par les personnes habilitées, dans un délai imparti et déclaré.

b/ *surveillance des lieux non affectés au travail*

L'employeur n'est plus soumis à la loi Informatique et Libertés.
La Cour de Cassation a retenu la cause réelle et sérieuse du licenciement d'un salarié, licenciement fondé sur l'enregistrement du vol de marchandises dans un entrepôt de l'entreprise qui l'employait et auquel ce salarié n'avait pas accès pour son activité.
Cass Soc 31/01/2001 n° 98-44290

2/ ENREGISTREMENT SONORE

Information préalable du salarié à défaut l'enregistrement est illégal et constitue l' infraction pénale du délit d'atteinte à la vie privée.

L'employeur ne peut écouter les enregistrements réalisés par un salarié sur son dictaphone personnel qu'en sa présence ou celui-ci dument appelé.
cass soc 23-05-2012

le dictaphone posé sur le bureau est présumé professionnel si rien 'n'indique un enregistrement personnel
le dictaphone dans le sac personnel est un effet personnel ; l'employeur ne peut l'appréhender sans l'accord du salarié..

3/ GEOLOCALISATION

Procédé permettant de localiser en temps réel une personne, un véhicule (GPS, GSM), un objet.

Conformément à la loi Informatique et libertés le CE doit être consulté et les salariés informés du dispositif mis en place

La délibération de la CNIL du 4-06-2015 prévoit les cas de recours à la géolocalisation:
-sécurité ou sureté de l'employé, des marchandises ou du véhicule dans le cadre de la lutte contre les vols.
-meilleures allocations des moyens dispersés (ex :taxi. ambulances)
-suivi de la facturation d'une prestation de transport ou de personne
-suivi du temps de travail quand on ne peut faire autrement (c'est un procédé accessoire)

Principes mis en œuvre pour préserver les données à caractère personnel :
- interdiction de la collecte d'informations en dehors de temps de travail. Tout salarié doit pouvoir désactiver sa géolocalisation.
- Un système de géolocalisation ne peut être utilisé par l'employeur pour d'autres finalités que celles déclarées à la CNIL et portées à la connaissance des salariés

- La géolocalisation ne doit pas conduire à un contrôle permanent du salarié.
- la géolocalisation n'est pas licite quand le salarié dispose d'une grande liberté dans l'organisation de ses déplacements
- le recours à la géolocalisation pour le contrôle du temps de travail n'est pas justifié si le salarié concerné dispose d'une liberté dans l'organisation de ses déplacements.

Ainsi à titre d'exemple le suivi du temps de travail d'un cadre itinérant qui se connecte quotidiennement pour rédiger ses rapports d'activité, passer ses commandes ou préparer ses tournées etc.. ne justifie pas le recours à la géolocalisation.

4/ SURVEILLANCE VISUELLE

Dans l'entreprise :

- Aucune information préalable ni consultation du CE lorsque la surveillance est faite par un supérieur hiérarchique ou un service interne
  (cass soc 5-11-2014)

- Si la surveillance est faite par :

- un détective à l'insu du salarié concerné : la preuve est illicite.
  Cass civ 2ème 17/03/2016 n °15-11412

- un service de sécurité mandaté : preuve illicite si elle est recueillie à l'insu du salarié

- un audit occasionnel concernant l'organisation du service ou du travail du salarié :

« Ne constitue pas un moyen de contrôle illicite, la mission réalisée au siège d'une mutuelle par un cabinet d'expertise comptable et de commissariat aux comptes, pour vérifier qu'un salarié n'outrepassait pas ses fonctions de responsable administratif. »
Doit en conséquence être approuvée une cour d'appel qui a retenu que le rapport d'expertise n'était pas soumis aux dispositions de l'article L. 1222-4 du code du travail
Cass soc 26.1.2016 n°14-19002

Hors entreprise :

- l'employeur ne peut mettre en place un dispositif de surveillance clandestin
- Filature ; preuve illicite qu'elle soit faite par un détective ou par l'employeur lui-même en raison de l'atteinte à la vie privée
  Cass Soc 17-3-2016

5-CHARTE ETHIQUE

C'est un code de bonne conduite , ne pas confondre avec la charte informatique / NTIC. Elle est facultative
Elle peut être incluse dans le Règlement intérieur ou faire l'objet d'un accord collectif ou d'un engagement unilatéral de l'employeur.

alerte ethique : dénonciation anonyme par internet , ce dispositif a été mis en place par :

- Délibération CNIL du 14.10.2010 pour les domaines financiers, comptables, bancaires, lutte contre la corruption, pratiques anti concurrentielles.
- Délibération CNIL du 30.10.2014 étendue au traitement des alertes en matière de discrimination harcèlement au travail, santé hygiène sécurité, protection de l'environnement

Fonctionnement de l'alerte : L'auteur doit s'identifier, il est protégé et restera anonyme s'il est de bonne f

6/ FOUILLE

. a/ Armoires vestiaire coffre

Principe : la fouille n'est possible que si le Règlement intérieur l'autorise et dans les conditions prévues soit :

-en présence du salarié ou celui-ci dument prévenu
-en présence du représentant du personnel si le Règlement intérieur le prévoit

Coffre : En principe les coffres sur le lieu de travail sont à usage professionnel et peuvent donc être contrôlés.

b/ sacs et effets personnels

Cas de recours à la fouille:
-préventif en raison de la sécurité et/ou de circonstances exceptionnelles ou en cas de vol.
Conditions du recours :
- un motif légitime
- l'accord du salarié qui doit être avisé de la possibilité de refuser et le cas échéant avoir un témoin sauf circonstances exceptionnelles (ex terrorisme) mais dans ce cas le CE et CHSCT doivent être consultés.
-respecter la dignité du salarié

La fouille pour retrouver des objets volés est assimilée à une perquisition et doit ace titre respecter les dispositions du Code de Procédure Pénale à savoir être faite par un OPJ (art 56 Code de Procédure Pénale) si le salarié refuse de se laisser fouiller.

Si le salarié est pris en flagrant délit : selon l' article 73 du Code de Procédure Pénale, l'employeur peut retenir le salarié le temps nécessaire à l'arrivée des forces de l'ordre.

La fouille systématique quotidienne doit être justifiée par un impératif de sécurité

Ex une entreprise spécialisée dans les métaux précieux rencontre un risque particulier de vols, le Règlement intérieur peut prévoir un contrôle à l'aide d'appareils détectant les métaux : la fouille est proportionné au but recherché même en l'absence de consentement du salarié

Mais la fouille n'est pas possible si le salarié n'a pas eu connaissance du Règlement intérieur qui n'est pas affiché, il n'a pu être informé de son droit à s'opposer à la fouille.
L'information du salarié repose sur l'employeur
cass soc 8.03.2005