

**MOYENS DE CONTRÔLE À DISTANCE DES SALARIÉS EN ITALIE ET EN FRANCE : LES DÉFIS DES NOUVELLES TECHNOLOGIES ET LE RESPECT À LA VIE PRIVÉ**

**(« I sistemi di controllo a distanza degli impiegati in Italia e in Francia : le sfide delle nuove tecnologie e il rispetto del diritto alla riservatezza »)**

**Vendredi 12 mai 2017,**

**Maison du Barreau, Salle Monnerville**

**Paris**

**PRESENTATION DE ANNABEL BOCCARA,**

**Ancien membre du conseil de l'Ordre du Barreau de Paris et avocat associé du cabinet Studio Airieau Meyrieux**

**La jurisprudence de droit social en France**

La difficulté dans le contexte général c'est que le salarié a la plupart du temps la disposition des matériaux fournis par l'employeur sur lesquels il va pouvoir utiliser à des fins personnels et pareil le salarié peut utiliser lui-même ses matériels personnel à des fins professionnels et donc cette interaction va poser de difficulté pour distinguer vie privée et vie professionnel et l'évolution de jurisprudence le confirme.

Pour les conditions x contrôler soit les déplacements soit le travail des salariés :

- il faut que l'entreprise ait un intérêt légitime (et donc tant le juge et CNIL contrôlent le respect de cette exigence). Et ça en fonction de l'article L.1121-1 du code du travail, lequel exige que ne soit pas apporté une atteinte disproportionné et illégitimes aux droits et libertés des salariés.
- Ensuite l'employeur devra consulter les instances représentatives du personnel. Il s'agit d'une obligation légale de consultation, et donc il n'ets pas lié par l'avis ainsi rendu.
- L'employeur devra également informer tous les salariés même s'ils ne sont pas tous concernés, que ce soit un moyen de contrôle informatique, vidéosurveillance, etc. Et cela à titre personnel.
- Enfin, il a une obligation de déclaration préalable à la CNIL Et la déclaration préalable à la CNIL.

La sanction du non respect de l'ensemble de ces condition c'est tout simplement que l'employeur ne pourra pas utiliser ces infirmations recueillies dans le cadre de ces mesures de surveillance obtenues de manière ainsi illégale.

Il ya la possibilité pour la CNIL de prononcer des sanctions administratives voire des sanctions prononcées par la chambre Sociale (peines d'amende) mais en tout état de cause il s'agit d l'impossibilité pour l'employeur de sanctionner les salariés sur la base des moyens de surveillance s'il n'a pas satisfait à l'ensemble de ses obligations .Par exemple si on s'aperçoit qu'un vidéo de surveillance n'est pas légal ou justifié, l'employeur ne pourra rien faire à l'égard d'un salarié ayant volé et dont la preuve se trouve dans ce vidéo ; la seule chose qu'il pourra faire ce sera de le surveiller un peu plus (sauf au pénal mais avec les difficultés de la longueur de la procédure pénale, alors que ne lui sera jamais possible de prendre de mesures disciplinaires).

Les différents outils qui servent à contrôler le temps de travail : biométrie, le badge, la géolocalisation des véhicules, la messagerie d'entreprise, la boite à lettre, les fichiers informatiques, tout ce qui est connexion internet, les sms. Si l'employeur a rempli ces différentes obligations de proportionnalité, il pourra donc utiliser les informations ainsi obtenues.

Par exemple, un on a un cas particulier d'un employeur ayant installé un camera mais pour surveiller le clients contre les vols, et l'employeur en regardant ces vidéos s'est aperçu que un salarié a volé au sein de son magasin et ainsi il s'en sert pour licencier le salarié pour faute lourde, mais la finalité de cette caméra n'était pas la surveillance des salariés, le salarié n'en avait aps été informé, et ainsi la Chambre sociale , rappelle que pour l'essentiel que l'employeur ne peut pas se prévaloir de ce mode de preuve pour licencier le salarié.

Le système de géolocalisation, comme il a déjà été dit a fait l'objet de plusieurs prononciations de la CNIL et on aussi certains cas en jurisprudence, comme un arrêt de la CA de Provence qui constate que le véhicule géolocalisé pour contrôler les horaires d'un salarié qui travaillait sur un chantier n'était aps le moyen le plus approprié pour contrôler les horaires de ces salariés et il aurait été mieux par exemple un contrôle effectué par des fiches de chantier. Ainsi, cette Cour d'appel a jugé que le système était disproportionné par rapport à la finalité.

Il y a une autre jurisprudence de la CA de Paris qui demande que ce type de contrôle puisse être retiré lors des pauses (la géolocalisation), ce qui est logique, puisque l'employeur ne peut pas savoir ce que le salarié ferait dans le weekend.

Il y a un autre moyen de contrôle qui est très pratiqué et admise de façon générale aux conditions dites et parfois est même imposé par la loi dans certains cas : il s'agit des écoutes téléphoniques.

Pour les messageries du bureau l'employeur a la possibilité de la pouvoir consulter hors la présence du salarié si l'outil est un outil fourni par l'employeur, puisque présumé être une messagerie professionnelle et donc il serait justifié par la nécessité de contrôler le suivi des dossiers du salarié et pour contrôler son activité. Il y a toutefois une exception : sauf si le salarié distingue sur cet ordinateur professionnel ce qui est personnel, et donc il est tout à fait admis que l'ordinateur professionnel puisse être utilisé à des fins personnels mais c'est alors au salarié lui-même de l'indiquer pour distinguer ce qui relève de sa vie professionnelle et personnelle (par exemple si l'employeur prend connaissance d'une email personnelle alors qu'il n'avait aucun moyen de savoir qui s'agissait d'une email personnelle , effectivement là le salarié ne pourra pas se plaindre d'une atteinte à la sa vie privée.

En ce qui concerne le déjà cité cas de la CEDH, il s'agit d'un ingénieur roumain qui avait conversé avec sa famille avec un outil fourni par l'employeur pendant son temps de travail. Or, l'employeur avait bien précisé dans son règlement intérieur qu'il n'était pas possible d'utiliser des matériels professionnels pour des fins personnels. Ainsi, même si cela peut paraitre étonnant puisqu'incohérent, ici la CEDH a dit que à partir du moment le règlement intérieur prévoit une tolérance zéro alors l'employeur pourra sanctionner. C'est une solution assez sévère et le salarié a été licencié pour une faute simple.

Par contre si le salarié a une messagerie personnelle dans son ordinateur professionnel, a priori il ya une présomption qu'il s'agit de correspondances personnelles et l'employeur ne pourra pas les consulter hors la présence du salarié en son absence parce que il y a bien une distinction entre l'adresse email professionnel et celui personnel.

Sur les disques dur, c'est la même chose : le salarié peut avoir une rubrique personnelle mais il doit l'avoir indiqué si l'outil ets professionnel.

Et pareil pour les SMS, l'employeur peut très bien consulter les SMS si l'outil ets professionnel, sauf si il est évident qu'il s'agit d'une correspondance personnelle, sinon il pourra être poursuivi pour atteinte au secret des correspondances.

Sur les connexions internet : l'employer peut restreindre du fait des virus les connexions internet et cela pour certains sites ou pour l'accès à certaines réseaux sociaux, ou interdire d'implanter une messagerie

personnelle par exemple par la crainte de virus, et pourra le faire soit par le règlement intérieur, soit, pourquoi pas, dans le contrat de travail.

L'employeur peut effectivement contrôler que les salariés respectent ces interdictions.

Il y a un cas en jurisprudence de 2008 dans lequel l'outil mis à la disposition par l'employeur au salarié est présumé être à usage strictement professionnel, et donc il pose une présomption à caractère professionnel.

Il y a une exception sur tout ce qui est la prise en main à distance d'un ordinateur pour une opération de maintenance par un ordinateur, il est nécessaire que le salarié en soit averti au préalable par tout moyen.

Les logiciels espions sont interdits en principe, sauf forme impérative de sécurité (comme les keys logger lesquelles sont utilisés pour voir ce que le salarié tape). Il y a un cas tranché par la Cour d'appel de Nancy où il y avait un salarié qui avait implémenté une key logger pour savoir si l'employeur lui avait implémenté une key logger et il a été licencié, mais la CA de Nancy s'est prononcée en retenant qu'il s'agissait d'un licenciement sans cause réelle et sérieuse puisque si l'employeur le fait sans en avoir le droit, il est alors possible au salarié de vérifier si l'employeur contourne cette interdiction.

En ce qui concerne les conséquences il y a une atteinte à la vie privée. Or, le salarié a droit au respect de la vie privée et ça ressort de l'article 9 cc et cela même sur le lieu de travail. On l'a vu avec l'arrêt Nikon 2001 l'employeur ne peut accéder librement à des données personnelles en absence du S. mais il faut que ces documents personnels soient identifiables comme tels.

La difficulté des réseaux sociaux relève du fait que l'employeur peut y avoir accès très facilement et obtenir ainsi certaines informations personnelles puisque elles comptent 31 million d'utilisateurs environs et très rarement le salarié n'utilise pas ses données personnelles pour s'identifier, et cela même dans l'optique dans l'embauche.

Et parfois il est même en cause la liberté de parole, d'expression du salarié. On a eu différents cas dans lesquels les juges ont été saisis pour savoir si cette liberté était absolue ou susceptible de restrictions : tout dépend du profil du salarié (par exemple s'il est cadre ou pas) mais en tous les cas le juge a tranché en disant que les salariés n'ont pas une liberté totale d'expression à l'égard de l'entreprise et de l'employeur et de ses conditions de travail. Il y a par exemple un cas où une militante syndicale qui à la suite d'un suicide du aux conditions de travail avait indiqué sur Facebook « journée de merde, boulot de merde etc. » et elle a été ainsi à la fois sanctionnée pour injurie au correctionnel et licenciée pour faute. Donc les salariés n'ont pas toute liberté de parole.

Le cas particulier aujourd'hui qui n'est pas véritablement réglé ce sont les BYOD (bring your own devices) : c'est-à-dire l'utilisation par le salarié de ses propres outils à des fins professionnels et donc il s'agira d'un outil a priori personnel, et on aura une présomption à caractère personnelle mais il faut quand même que l'employeur puisse contrôler son travail, ses horaires de récupérer ce qui a été enregistré par le salarié concernant son travail. Donc il est demandé à l'employeur (et c'est la CNIL qui le recommande dans une recommandation) de pouvoir distinguer ce qui est professionnel et ce qui est personnel. Mais là-dessus il n'y a pas en tant que elle de législation et donc ça crée des difficultés. On a eu par exemple un cas en 2013 d'une utilisation d'une clé USB personnelle sur un ordinateur professionnel et là on a jugé que l'employeur pouvait en contrôler le contenu à partir du moment où il s'agit des données professionnelles.

Donc, il faut être bien attentif lorsqu'on donne des autorisations aux contrôles, pour savoir ce qui va être contrôlé, surveillé et aussi pour combiner de temps.

Or, cette évolution jurisprudentielle est très similaire avec celle italienne, surtout au regard des informations recueillies à travers les réseaux sociaux, même à travers des « likes » qui témoignent une

certaine approbation au regard de certains sujets et qui font donc ainsi comprendre aux autres, comme à l'employeur certaines informations concernant la vie privée des salariés.