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 *Marie France Mazars*

Les dispositifs de surveillance dit TIC entrent dans le champ d'action de la CNIL.

Il faut constater tout d'abord qu'il y a un développement considérable de la nécessité de la prise en compte de la protection des données personnelles dans les relations professionnelles dans la mesure où les moyens de contrôle deviennent de plus en plus performants, à tel point qu'on s'est demandé s'il fallait légiférer ou s'en tenir à ce qu'on a fait jusqu'à présent, c'est-à-dire à s'attacher à l'application des principes généraux qui permettent de régler pas mal de problèmes (mais pas tous).

En 1992 (arrêt Nimietz du 16 décembre 1992) la CEDH a rendu un arrêt très important en disant que le cercle de la vie privée n'était pas seulement à la maison mais aussi au travail, en affirmant l'existence d'un droit au respect de la vie privée au travail. Et la chambre sociale de la Cour de Cassation a bien décliné les contours de ce droit depuis l'arrêt Nikon (2 octobre 2001.

La CNIL a été sollicitée pour se prononcer sur les nouveaux outils. Il y a une déclaration à faire à la CNIL lorsqu'on installe des nouveaux systèmes informatiques et en plus la commission reçoit les plaintes des salariés, donne des avis, et donc par son rôle qui peut être un contrôle a priori ou un contrôle a posteriori, elle a, durant ces dernières années, abordé tous ces problèmes. Exerçant son pouvoir de sanction (sanctions administratives), elle a aussi fixé des règles fortes.

Le Règlement UE (n°2016/679 du 27 avril 2016) modifiera peut être un peu la situation mais dans la mesure où le travail d'encadrement des NTIC est fait, ce sera moins difficile de s'adapter à ce règlement qui laisse la possibilité aux Etats d'adapter les normes même par conventions collectives, donc il n'y aura pas de bouleversement.

Les questions soulevées trouvent leur solution dans l'application conjuguée du Code du travail et de la loi Informatique et Libertés du 6 janvier 1978 modifiée.

Un employeur peut toujours décider de mettre en place des moyens de contrôle à distance. Cela a toujours été considéré comme un corollaire de son pouvoir de direction qui comprend les pouvoirs de surveillance, de contrôle et de sanction. Dans ce cadre, l'employeur peut poser des limites et conditions à l'accès à internet - il existe des chartes de l'utilisation du matériel informatique- et l'employeur pourra aussi mettre en place des procédés de filtrage et d'exigences de sécurité. Par exemple pour éviter l'intrusion de virus on peut avoir dans cette charte l'interdiction de consulter certains sites, ou pour faire obstacle à la commission d'infractions d'interdire l'accès aux sites pornographiques. Il y avait là deux problèmes : la responsabilité de l'entreprise pour avoir permis la circulation de ces images dans l'entreprise et aussi le fait que la

pornographie pendant le temps de travail mérite sanction (une CA a dit qu'il y avait à cette occasion une faute grave). Et la CEDH dans un arrêt très récent (CEDH, Bărbulescu c. Roumanie, 12 janvier 2016, 61496/08) est en phase avec la jurisprudence de la Cour de cassation. Elle estime que l'employeur peut accéder au compte internet professionnel du salarié et retenir la faute du salarié lorsque le relevé des communications prouvait que celui-ci utilisait l'ordinateur à des fins privées pendant les heures de travail tout en relevant que l'identité des personnes avec lesquelles il avait communiqué ne devait pas être divulguée.

Le principe, issu de la loi Informatique et Libertés de 1978, est proche de celui de l'article L.1121-1 du code du travail (« *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 proportionnées au but recherché* ». La loi de l'Informatique et des libertés ne dit pas autre chose. Son article 1er est ainsi rédigé : « *L'informatique doit être au service de chaque citoyen(…) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »*

S'agissant de certaines techniques de surveillance, l'employeur est obligé de soumettre le procédé à une déclaration préalable (par exemple la vidéosurveillance ou la géo localisation) ou à une autorisation spécifique de la CNIL préalable (par exemple pour tous les systèmes utilisant la biométrie) .

Les salariés peuvent porter plainte devant la CNIL si des traitements informatiques n'ont pas été déclarés ou /et ne sont pas conformes à la loi de 1978. C'est dans ce cadre que la CNIL a prononcé des mises en demeure ou des sanctions de certains magasins où il y avait des systèmes de vidéosurveillance avec des cameras qui filmaient en permanence les salariés, et en tous lieux y compris dans de lieux de pause. Dans ces dossiers on avait deux manquements à la loi de l'informatique et des libertés : tout d'abord le fait de placer les salariés sous un contrôle en permanence, mais aussi le fait de ne pas avoir informé préalablement les salariés de ce moyen de surveillance.

Il doit y avoir, pour la mise en place de chaque système de surveillance par traitement informatique (lequel collecte des données personnelles), une **information au Comité d'entreprise** (L.2323-32 du code du travail) et aussi une information destinée **aux employés** (L.1222-4 du même code et article 32 de la loi informatique et libertés « I&L ») (alors qu'en Italie cette information préalable ne doit être faite qu'aux salariés et pas aux syndicats et c'est une des raisons de ses critiques cf. Paolo Sordi).

Ce principe de **l'obligation d'information** et donc de transparence a été rappelé par la chambre sociale de la Cour de cassation dans de nombreux arrêts et notamment dans celui du 10 janvier 2012 .Dans cette affaire, les salariés d'une société de nettoyage sur le site d'une société cliente n'avaient pas été informés qu'il y avait un système de surveillance sur le site du client et l'employeur a toutefois utilisé ces enregistrements vidéo pour les sanctionner. Le Cour de Cassation a énoncé que *« l'employeur ne peut être autorisé à utiliser comme mode de preuve les enregistrements d'un système de vidéosurveillance dont les intéressés n'ont pas été préalablement informés de l'existence.* » La loi I&L prévoit que l'information des employés doit porter notamment sur la finalité du dispositif de surveillance, sur les destinataires des données personnelles collectées, la durée de conservation ainsi que les droits qui leur sont reconnus (droit d'opposition, d'accès et de rectification)

L'importance est dans **la finalité poursuivie**. L'employeur lorsqu'il déclare le système à la CNIL doit dire quelle est la finalité de son traitement (par exemple pour la vidéosurveillance, s'agit-il de la sécurité des biens ? ou des personnes?). Cette finalité doit être légitime, explicite et déterminée. Et cette obligation de préciser la finalité permettra de faire échec aux détournements de finalité (par exemple si on installe un système de vidéosurveillance pour la protection des biens l'employeur ne peut pas l'utiliser pour surveiller de manière permanente son salarié à son poste de travail). La finalité exige une certaine intégration restrictive et rigoureuse. Elle oblige l'employeur à se demander s'il a vraiment besoin de ce système pour l'administration de son entreprise. Cette analyse a été au cœur de la réflexion de la CNIL lorsque les

systèmes de surveillance utilisant la biométrie se sont développés. Par exemple, la CNIL avait d'abord autorisé le recours à la biométrie (lecture de l'empreinte digitale) pour le contrôle des horaires de travail, mais, à la suite de plaintes, elle est revenue sur sa position et a appliqué le raisonnement selon lequel la technologie utilisée ne doit pas être disproportionnée au regard de l'objectif poursuivi (comme elle avait refusé l'utilisation d'un dispositif reposant sur l'empreinte digitale pour l'accès à un établissement scolaire). La donnée biométrique (issue d'un élément du corps humain) est une donnée personnelle dont la collecte donne lieu à un encadrement rigoureux et sur ce point (que l'on ne peut développer plus avant ici) la doctrine de la CNIL a récemment été bien précisée (voir le site de la CNIL).

S'agissant des systèmes de géo localisation, il faut signaler qu'il y a eu une réflexion ayant donné lieu à des échanges entre la Chambre Sociale de la Cour de cassation et la CNIL pour parvenir à une solution qui est la suivante : il doit y avoir un intérêt légitime à connaitre la position géographique des salariés. C'est seulement s'il y a cet intérêt légitime que l'utilisation de la géo localisation est autorisée, à défaut elle ne l'est pas. Au surplus la finalité du dispositif doit être déclarée par l'employeur et il ne peut y avoir détournement de finalité. Et c'est ce même exemple qui nous a été donné par Paolo Sordi (distinction entre le technicien soumis au GPS pour des raisons antivol du véhicule ou pour lui permettre d'intervenir le plus tôt possible en étant le plus proche de l'intervention à effectuer). Au surplus, dans le souci du respect de la vie personnelle des employés, la CNIL estime que les salariés doivent pouvoir désactiver le GPS quand ils sont en heure de pause par exemple.

Certains outils sont particulièrement « à risques ». La cour d'appel de Paris a rendu un arrêt le 12 mai 2016 où elle a reproché à l'employeur de ne pas avoir déclaré préalablement à la CNIL son système de Data Leakage Protection (protection contre la fuite des données) et d'avoir sanctionné le salarié alors qu'elle ne l'avait pas préalablement informé de ce système existant sur son ordinateur. Ce traitement informatique, dit DLP, permet de lire, conserver et enregistrer chaque courriel envoyé depuis la messagerie professionnelle d'un employé. Il convient de rappeler que les messages identifiés comme « personnels » ne pourront pas être consultés par l'employeur.

Ces systèmes, qui permettent à l'entreprise d'éviter les fuites de données confidentielles se multiplient.

On peut également évoquer les key loggers, procédé qui permet avec « l'espionnage » de la frappe du clavier de l'ordinateur, à partir du repérage de mots-clés, de surveiller le contenu de ce que les salariés tapent. Saisie d'une plainte, la CNIL a dit qu'un tel procédé devait être interdit (Ce qui semble être le cas aussi en Italie) dans la mesure où ce type de logiciel permet à l'employeur d'exercer une surveillance constante et permanente sur l'activité professionnelle des salariés concernés mais aussi sur leur activité personnelle résiduelle effectuée à partir du poste informatique.

Ici, c'est **la règle de proportionnalité** qui conduit à bannir ce type de dispositifs. En effet, la CNIL exerce un contrôle de proportionnalité au regard de l'objectif poursuivi. Nous l'avons déjà examiné notamment en ce qui concerne la vidéosurveillance, la géo localisation et les traitements biométriques. D'ailleurs, dans certains cas, la disproportion est flagrante.

Enfin on rappellera brièvement que la CNIL exerce également un contrôle sur **la durée de conservation** des données collectées dans le système et **les mesures de sécurité** garantissant l'intégrité des données et du système

En conclusion, il faut aujourd'hui souligner que l'application du Règlement européen *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* entre en vigueur en mai 2018 et que nous devons nous préparer à l'application de ces nouvelles normes. On sait qu'il va y avoir un avis de la CNIL européenne sur le traitement des donnés personnelles des salariés et plus particulièrement sur les dispositifs permettant de contrôler directement ou indirectement les salariés. Notre loi interne va devoir être modifiée aussi en fonction du règlement

européen et il y a eu entretemps la loi pour une République numérique. Ce contexte va favoriser la coopération entre les différentes CNIL européennes. Il faudra nécessairement coopérer en cas de sanctions pour manquements au Règlement européen commis dans plusieurs Etats membres puisqu'est mis en place un système d'autorité de contrôle « chef de file » et de concertation et d'opérations conjointes des autorités de contrôle lorsque les poursuites pour manquement au Règlement concernent une entreprise établie dans plusieurs Etats membres.

Un dialogue, comme celui qui est initié aujourd'hui par ce colloque franco-italien, entre les juristes et les autorités judicaires ou administratives de nos différents pays européens, semble plus que jamais indispensable.

Annabel Boccara *:*

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 ets 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 ya 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 prononcé 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 ets alors possible au salarié de vérifier si l'employeur contourne cette interdiction.

En ce qui concerne les conséquences il ya une atteinte à la vie privée. Or, le salarié a droit au respect de la vie privée et ca ressort de l'article 9 cc et cela même sur le lieu de travail. On la vu avec l'arrêt Nikon 2001 l'employeur ne peut accéder librement à des donnés personnels 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 juge 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 le 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 Dun outil a priori personnel, et on a 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 ets 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 donnés professionnels.

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

Or, cette évolution jurisprudentielle ets 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.

Christiane Féral-Schuhl *:*

Dans la cadre de la commission parlementaire qu'elle a présidé pendant quatorze mois dans laquelle il a été travaillé aux droits et libertés à l'âge du numérique, intéressante puisque c'était la première fois qu'on se mettait ensemble dans une commission présidée par un député et une personne issue de la vie civile, doublement paritaire. Il a été découvert que la seule correspondante dans le cadre de l'Union Européenne c'était en Italie, et le souhait général était de permettre un développement de ce sujet partagé dans l'Union européenne. Or, même si ce but n'a pas été véritablement atteint, le rapport existe tout de même et il est toujours consultable sur internet.

La partie la plus importante sur laquelle s'est concentrée cette réflexion a été celle de la constitutionnalité de la protection des donnés personnels. Or cette constitutionnalité existe dans certains pays mais pas en France. Toutefois, aujourd'hui ils font partie des droits absolument fondamentaux et ne peuvent pas être attachés par ricochet à la vie privée. Et donc la protection des données personnelles doit faire l'objet d'une protection particulière en soi et cette commission y a travaillé avec le Parlement italien.

La raison qui l'a poussée à s'intéresser à ce sujet a été loi de l'Informatique et des libertés, laquelle loi va être modifiée cela l'attriste, car elle est plutôt partisane d'une loi de principe et la loi qui a mieux résisté au temps c'est notamment cette loi, puisqu'elle contient des principes généraux qui se déclinent. Et ce qui apparait avec la commission informatique et liberté c'est que à travers les recommandations de la CNIL on a vu une forme de jurisprudence se mettre en place et certains qui a permis de construire une réglementation.

Ainsi, le constat que souvent les lois sont souvent dépassées par l'évolution du numérique comme la loi sur la confiance e l'économie numérique qui a été très vite dépassée par le web 2.0 et qui a contribué à redistribuer les cartes.

Ce qui ressort ce sont ces principes, que ce soit en France en Italie ou ailleurs: il s'agit du principe de loyauté, de transparence, de proportionnalité. On va les trouver systématiquement et ils guident le juge dans son appréciation. La difficulté c'est que c'est toujours une appréciation au cas par cas, de circonstance. Si on a déjà cette difficulté en France, lors de l'appréciation différente menée par différentes chambres ou mêmes entre différentes sections au sein d'une même juridiction, il l'est encore plus imaginable à l'échelle européenne. Et lorsque on évoque les technologies, les défis, la vie privée, l'on constate déjà que l'éthique n'est pas appréhendée de la même manière par tous els pays. On a par exemple récent des salariés auxquels une entreprise belge décide de placer des puces électroniques sous-cutanées. Or, la CNIL a créé une commission d'éthique, ce qui témoigne de la place fondamentale de l'éthique. Ces puces électroniques sous-cutanées ont eu deux approches différentes en Belgique : elles ont été utilisées par l'employeur, alors que d'autres critiquent durement ce moyen de contrôle, surtout en ce qui concerne la difficulté de les enlever lors des temps de non travail. Il a été constaté qu'il s'agit de la personne, dès qu'on parle des donnés personnels c'est de l'identité d'une personne dont on parle. Comme il a été déjà expliqué pour la biométrie qui touche à des aspects de plus en plus intimes. La biométrie touche à des aspects des plus en plus intimes, et donc touchant à al vie privée. Or, il y a une entreprise en Suède qui a généralisé ce type de contrôle par des puces sous- cutanées, alors qu'en France en France on considère que c'est contraire à l'éthique.

En ce qui concerne la protection de la vie privée, laquelle n'est définie nulle part, pourtant elle fait partie d'un droit fondamental : elle est évoquée par les conventions internationales et seulement dans l'article 9 du code civil art 9 cc. Donc la notion de vie privée n'a rien à avoir à travers le temps et à travers les pays. Donc l'appréhension aujourd'hui de la vie privée en Angleterre et dans les autres pays n'a strictement rien à voir. L'appréciation des juges en effet va être différente, et ainsi on passe à l'intimité de la vie privée,

aussi appelée « extimité » de la vie privée. Si auparavant on avait des journaux intimes, aujourd'hui la même fille va partager son journal intime avec tout le monde et donc on parle désormais d'extimité.

En ce qui concerne le droit du travail, aujourd'hui les choses se mêlent encore plus car il y a utilisation des outils professionnels à des fins personnels et vice-versa. Et souvent le salariés sont soumis une Charte qui les soumet à une obligation de confidentialité, alors que parfois leur employeur leur demande des documents de travail hors du temps de travail et ils le font alors à travers leur adresse email personnel : ce qui pose un problème puisque ils se posent soit en fait vis-à-vis de l'employeur, soit vis-à-vis de la Charte. De même on peut avoir des cas d'utilisation de l'outil professionnel à des fins personnels, comme celui de réserver un billet d'avion à la dernière minute etc.

Le droit à la déconnexion : c'est difficile à le faire comprendre aux salariés, lesquels, dès qu'ils reçoivent une instruction, ne pensent qu'à y obéir, à n'importe quelle heure. Il fut donc effectuer un vrai travail de sensibilisation.

Qu'est-ce qu'il change avec le règlement européen ? Il a deux considérants qu'il faut garder en tête : ce sont les considérants 155 et 88 qui prévoient que les états membres peuvent mettre en place des règles spécifiques dans le cadre des relations de travail (avec le respect des différents conditions et droits comme celui à la dignité humaine etc.). Donc, ça veut dire qu'il y a une zone réservée dans chaque pays au droit du travail et que dans cette approche globale dans lequel le règlement européen s'inscrit, pour l'essentiel on va retrouver tous les principes de la loi de l'Informatique et des libertés. Donc, avec ce règlement on se retrouve dans une situation relativement analogue : il va d'être d'application immédiate en mai 2018 mais il ne va pas en effet changer les principes généraux, mais va donner ce marge de manœuvre aux états. Or, avec les sociétés internationales on a déjà eu des difficultés de coopération, en particulier avec l'Allemagne laquelle prévoit que les données des salariés doivent être hébergées dans le territoire national.

Pour une minorité, ca va concerner les sociétés internationales, car celles-ci il va y avoir des facteurs d'harmonisation et lorsqu'on va harmoniser on va avoir un dénominateur commun et lors comment gérer les différences au sein de l'UE. Il va y avoir aussi des difficultés hors de l'union européenne du fait de l'application extraterritoriale du règlement (lorsque donnés concernent des personnes extra européennes ils vont devoir décaler, c'est- à-dire qu'il s'applique dès lors que les données concernent les citoyens européens), laquelle fait en sorte que même si ces salariés résident en dehors de l'UE, ils vont devoir se baser sur ce règlement.

Donc il y a un sujet sur lequel il va devoir réfléchir et apporter des réponses. Mais sinon le règlement européen fait basculer d'un régime déclaratif avec des formalités qui sont souvent complexes pour les usagers à un système d' « accountability », c'est-à-dire de prise de conscience, de responsabilisation dans les outils à mettre en œuvre. Et la difficulté va être de concilier ce principe fondamental des droits et libertés des citoyens et donc des salariés avec toutes les spécificités nationales, culturelles, que l'on peut imaginer avec l'obligation de sécurité du chef d'entreprise, dont l'approche de loyauté, transparence proportionnalité également a le pouvoir de contrôle sur les outils qu'il met à la disposition des salariés . Donc le salarié lui-même a évolué. On n'est plus dans le cadre d'un salarié qui arrivait et quittait l'entreprise tout seul, puisqu'aujourd'hui le salarié arrive au bureau avec tous ces outils, ses adresses email et il s'installe et puis il repart. C'est cette évolution là qu'il faut arriver à intégrer. On y ajoute qu'il travaille dans un espace collaboratif de manière générale par exemple, en matière de recherche, les chercheurs travaillent forcement dans un approche collaboratif et donc travaillent dans des réseaux qui sont ouvertes, et à un moment donné soit ils quittent l'entreprise et les recherche qu'ils ont fiat disparaissent , soit ils terminent leurs recherches et ces recherches peuvent être revendiqués par des tiers, en termes de brevets etc. Donc on va bien des situations qui forcent l'employeur à contrôler les outils. Il y a ainsi des droits des salariés, mais aussi des devoirs, comme la délicatesse des propos, le devoir au moins de ne pas insulter son employeur, de consacrer son temps de travail effectivement à son employeur. Na donc ces obligations qui

vont se conjuguer à celle du chef d'entreprise qui sont celles d'assurer la sécurité, à tel point que aujourd'hui il ya à la charge du chef d'entreprise toute une série d'obligations dans le règlement européen. Et plus on avance on va protéger ces outils pour sécuriser.

En fait, pour résumer, c'est comme un bateau, dans lequel le capitan a l'obligation de s'assurer qu'il n'y aura aps d'ouvrages, mais qu'il est quand même obligé régulièrement de faire décharger son bateau et donc à la déconnexion. C'est une image parlante puisque représente bien cet océan numérique dans lequel on navigue tous les jours.

Questions du public :

- Est-ce le raisonnement effectué pour la messagerie professionnelle pourrait s'appliquer aussi aux téléphones professionnels ? est-ce qu'il est possible d'utiliser les relevés des appels téléphoniques qui révèlent une utilisation pour ¾ à des fins personnels pendant le temps de travail ?

Mme Boccara : Oui, s'il démontrer que les horaires professionnels ont été utilisés à des fins personnels et il n'y a pas donc des problèmes concernant le contenu de la vie privée puisqu'il n'y pas du tout d contenu, il s'agit juste des appels.

Mme Mazars : sur le site de la CNIL il y a la possibilité de demander des conseils concernant l'enregistrement des appels téléphoniques, puisque la mission de la CNIL est d'accompagner dans le respect de ces règles. Il faut plus préciser que la modification de la loi de l'Informatique et des libertés ne concerne que la mise en conformité de cette loi au règlement UE, et qu'il n'est aps question de toucher à l'article 1 qui est magnifique, et surtout « au service du citoyen ». L'esprit reste le même. Il faut encore préciser que la CNIL demandait à que le droit à la protection des données personnels ait été inscrit dans la Constitution, ce qui n'a pas été fait.

- Il n' ya pas de jurisprudence permettant de faire rentrer le droit à la protection des données personnels dans le bloc de constitutionnalité, sans modifier pour autant la Constitution, ou est-ce qu'il y a-t- il d'autres moyens ?

Mme Féral-Schuhl : Non, cela n'a pas encore été fait.

Mme Mazars : peut-être, lors de la révision de la directive, le Conseil Constitutionnel sera amené à se prononcer sur ce sujet, mais rien n'est sur. La seule chose qui est sure c'est que tout est e mouvemente en en évolution.

- Quel est le délai légal de conservation des empreintes digitales ?

Mme Mazars : ca dépend du contexte dans lequel elles sont prises, si elles sont prises pour les intégrer dans un fichier régalien (par exemple pour un passeport) c'est un délai très long. Mais si leur finalité est celle de permettre l'accès à des locaux, le délai de conservation sont ceux pendant lesquels le salarié va être employé dans l'entreprise. Ce qu'on peut empêcher c'est que ces empreintes digitales ne soient aps conservées dans un serveur informatique et qu'elles restent à al main de la personne, et comme ca il y pas de risques de vol des empreintes digitales.