LES LIMITES DE L'UTILISATION DES NOUVELLES TECHNOLOGIES DANS L'ENTREPRISE

AVERTISSEMENT :

- La réglementation sur les nouvelles technologies est dispersée, dans le code du travail, dans les lois, dans les délibérations de la Commission Nationale de l'Informatique et des libertés (CNIL)
- La CNIL, autorité administrative indépendante garantit la protection des libertés individuelles et veille à ce que les atteintes à la vie privée des salariés soient justifiées, proportionnées et que les salariés soient bien informés

1- LA MISE EN PLACE DES NOUVELLES TECHNOLOGIES

A- Protection de la vie des salariés

Les nouvelles technologies représente un risque d'atteinte à la vie privée

Le code du travail limite ce risque (Art 1121-1) :

« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

- ✓ Un système mis en place doit être justifié par des intérêts propres à l'entreprise et les atteintes à la vie privée doivent être proportionnées à l'objectif recherché par l'employeur

A- PROTECTION DE LA VIE DES SALARIÉS

Le CDT prévoit en outre (art L1222-4) : « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* »

Le salarié est informé individuellement que des informations le concernant sont récupérées et stockées par l'employeur.

Il en va de même pour les candidats à un emploi.

B- PRINCIPES GÉNÉRAUX S'APPLIQUANT AUX NOUVELLES TECHNOLOGIES

1) Principe de finalité :

Des données à caractère personnel ne peuvent être recueillies et traitées pour un usage propre à l'entreprise. Elles doivent être légitimes.

Par exemple, un employeur ne peut pas recueillir d'informations sur ses salariés et les revendre à des entreprises de prospection publicitaire

2) Principe de proportionnalité

Le traitement des données personnelles ne doit pas apporter aux droits et libertés des personnes des restrictions disproportionnées

Exemple : la mise en place d'une vidéo-surveillance possible seulement s'il y a de risques importants pour la sécurité des salariés ou un risque de vol de marchandises

B- PRINCIPES GÉNÉRAUX S'APPLIQUANT AUX NOUVELLES TECHNOLOGIES

3) Principe de pertinence des données

les données personnelles recueillies doivent être adéquates, pertinentes et non excessives au regard des objectifs poursuivis

Exemple : demander lors d'un recrutement des informations sur l'état de santé du candidat

4) Principe de conversion dans le temps des données recueillies

Variable suivant le type de données. Se renseigner auprès de la CNIL

5) Principe de sécurité et de confidentialité des données

L'employeur est le garant de la bonne conservation des données et de leur non-divulgation. Il prend les mesures nécessaires au maintien de cette confidentialité assure la protection de son système

B- PRINCIPES GÉNÉRAUX S'APPLIQUANT AUX NOUVELLES TECHNOLOGIES

6) Principe de transparence – information préalable :

les salariés sont informés préalablement et individuellement du traitement des données les concernant et des destinataires de ces données

7) Droit d'accès et d'opposition

Le salarié peut se faire communiquer toutes les informations le concernant, les faire rectifier si elles sont erronées.

8) Principe de discussion collective

Le CE (ou la DUP) est informé et consulté sur tout projet d'introduction de nouvelles technologies dans l'entreprise et de contrôle des salariés

C- L'INFORMATION PRÉALABLE DU COMITÉ D'ENTREPRISE

Le CE est informé et consulté préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail (Art 1223-13 CT).

Il est obligatoirement informé préalablement à l'introduction de méthodes de d'aide au recrutement et de techniques automatisées de gestion du personnel (Art 1223-23 CT).

Il es obligatoirement informé et consulté préalablement à la mise en place de moyens ou techniques permettant un contrôle de l'activité des salariés : badges, vidéo-surveillance... (Art 1223-23 CT).

D – LA DÉCLARATION À LA CNIL

A chaque fois que l'employeur met en place un système de traitement des données, il est censé le déclarer à la CNIL

Toute personne concernée peut vérifier auprès de la CNIL que la déclaration a bien été effectuée

Cette déclaration ne dispense de l'obligation d'informer et de consulter le CE et d'informer individuellement le salarié préalablement à la mise en place d'un tel système

II – LA CYBERSURVEILLANCE

A- L'accès aux dossiers stockés sur ordinateur

les dossiers et fichiers crées par un salarié grâce à l'outil informatique mis à disposition de l'employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors de sa présence (Cass soc. 18 oct. 2006 n° 04-48025)

Un salarié qui empêche son employeur d'accéder à son ordinateur encourt un licenciement pour faute grave

N'est pas considéré comme dossier personnel : un dossier intitulé par le prénom ou les initiales ou protégé par un mot de passe : il est nécessaire d'intituler le dossier « privé » ou « personnel »

L'employeur ne peut ouvrir un fichier personnel qu'en présence du salarié

L'employeur qui ouvre les fichiers personnels en dehors de la présence du salarié ne peut pas utiliser le contenu contre le salarié, sinon il commet une infraction pénale

B – INTERNET, OUTIL DE CONTRÔLE POUR L'EMPLOYEUR

Au même titre que pour le téléphone, un usage raisonnable d'internet est toléré notamment durant la pause déjeuner (Guide CNIL pour les employeurs et les salariés ed.2010)

Toutefois, l'employeur peut interdire, en amont, l'accès à certains sites ou le limiter à ceux qu'il prédétermine. Ces restrictions ne doivent pas pour effet d'entraver ou de discriminer certains syndicats ou même de de commettre une inégalité de traitement entre les salariés.

Les connexions Internet établies par le salarié sont présumées avoir un caractère professionnel, l'employeur peut les rechercher pour les identifier (Cass Soc. 9 juillet 2008, n° 06-45800).

Un usage personnel de l'ordinateur professionnel ne peut pas être interdit et un contrôle important de l'employeur alors que le salarié est en dehors de son temps de travail ne serait pas raisonnable (Appel Versailles 6è chambre sociale 18 mars 2008, n° 08/00046)

C – LA MESSAGERIE ÉLECTRONIQUE

L'employeur pour des raisons de sécurité, de prévention de l'encombrement, peut mettre en place des systèmes de contrôle de la messagerie.

L'employeur est responsable des dommages causés par le salarié en cas de propos injurieux, diffamatoires ou racistes envoyés par celui-ci par un courriel au nom de l'entreprise.

C'est pourquoi le régime des courriels est identique à celui des dossiers et fichiers contenus sur l'ordinateur : ils sont présumés être professionnels à moins d'être identifiés comme personnels (Cass. Soc. 18 oct. 2006, n°04-48025) et l'employeur ne peut lui-même ouvrir et consulter un courriel clairement identifié comme personnel : le salarié doit être présent.

L'employeur commet une infraction pénale s'il consulte un courriel sans avoir requis la présence du salarié

D – LES CHARTES ÉTHIQUES ET CODES DE CONDUITES

L'employeur peut définir unilatéralement ou par accord d'entreprise une charte d'utilisation d'Internet. Il dispose d'une certaine liberté dans son élaboration, à condition de ne pas porter atteinte :

- Au principe de non discrimination (art L.1132-1 CT)
- Aux droits et libertés individuelles des salariés (art L.1121-1 et L. 1321-3 CT)
- A l'expression collective des salariés (art 2281-1s CT)
- Aux règles posées par la CNIL ou les lois informatiques et libertés.

L'employeur doit informer et consulter le CE (ou les DP) préalablement à son entrée en vigueur car cet acte concerne « *l'organisation, la gestion, et la marche générale de l'entreprise* (art L.2323-6 CT).

D – LES CHARTES ÉTHIQUES ET CODES DE CONDUITES

Une charte informatique (mails, Internet, ordinateur...) peut définir ce qui correspond à une utilisation raisonnable (temps passé, taille des messages, nombre de connexions, pj...).

Un salarié peut être sanctionné s'il ne respecte pas cette charte (cass.soc. 22 oct 2008, n°07-42654).

Les dispositions et restrictions de la charte doivent être précises sinon elles constituent une atteinte disproportionnée aux libertés des salariés (cass. Soc. 8 déc.2009 n° 08-17191).

L'employeur peut y insérer des dispositions relevant en principe du règlement intérieur (comme des sanctions) mais en ce cas, il doit respecter les formalités prévues pour la mise en œuvre du R.I (communication à l'inspection du travail)

III – LES AUTRES TECHNOLOGIES

A – La collecte d'information et le recrutement

Le CE doit être informé de tout système automatisé en matière de recrutement.

Selon l'art L1221-6 du CT, les informations demandées à un candidat ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles. Elles doivent *« présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation de ses aptitudes »*

La collecte d'informations auprès de l'environnement professionnel du candidat est valable à condition de ne pas être faite à son insu.(art L.1221-9 CT)

B – LA TÉLÉPHONIE

Un salarié peut utiliser le téléphone mis à sa disposition pour un usage personnel à partir du moment où cette utilisation reste raisonnable et non préjudiciable pour l'entreprise.

Les salariés bénéficiant d'un mandat électif ou syndical « doivent pouvoir disposer d'un matériel ou procédé excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondances (Cass Soc 6 avril 2004, n°02-40498)

Aucune écoute permanente ni aucun enregistrement des conversation des salariés ne peut être mis en œuvre (Guide CNIL éd. 2010). Un enregistrement sur une brève période pour les besoins d'une formation peut être réalisé.

Les salariés doivent être informés sur ces enregistrements ou écoutes, notamment sur l'objectif poursuivi, sur la durée, sur les conséquences qui peuvent en découler...

C – LA VIDÉOSURVEILLANCE

La vidéosurveillance ne doit être utilisée qu'en dernier recours et de façon proportionnée, pertinente et strictement nécessaire à l'objectif poursuivi. Ainsi une caméra filmant en permanence des secrétaires ne peut être justifié par un objectif de sécurité.

Quand l'employeur a respecté les dispositions légales de mise en place de vidéosurveillance et l'information des salariés, il peut utiliser ce moyen pour prouver une faute d'un salarié.

Les salariés et le CE doivent être informés qu'ils sont susceptibles d'être filmés même si le procédé est matériellement visible.

Toute surveillance à l'insu des salariés est considérée comme illicite.

La durée de conservation des images ne doit pas excéder un mois et le système doit faire l'objet d'une déclaration à la CNIL.

D – LE BADGE ET LA BIOMÉTRIE

Le badge ne peut être utilisé que pour :

- La gestion des horaires et des temps de présence
- Le contrôle des accès et des sorties des locaux
- Le contrôle de l'accès au restaurant et son paiement
- Le contrôle de l'accès des visiteurs

Les systèmes de badge et de biométrie ne doivent pas entraver la liberté de circulation des salariés protégés, ni avoir pour effet de contrôler leurs déplacements.

.

E – LE DROIT D'ALERTE

Les délégué du personnel disposent d'un droit d'alerte leur permettant de saisir le conseil des prud'hommes. Selon l'article L2313-2 du code du travail, si un DP constate une atteinte à une liberté individuelle dans l'entreprise qui ne serait pas justifiée ni proportionnelle au but recherché, il en saisit immédiatement l'employeur.

En cas de carence de celui-ci, ou de divergence sur la réalité de l'atteinte, alors il peut saisir le bureau de jugement des prud'hommes en référé afin qu'il soit ordonné toutes mesures nécessaires à faire cesser cette atteinte.

En cas d'absence d'information préalable des IRP, ceux-ci peuvent saisir le T.G.I en demandant la suspension de l'application du dispositif dans l'attente de la régularisation de la procédure d'information et de consultation et ce sous-astreinte.

L'employeur peut également être condamné en correctionnel pour délit d'entrave.

.