



## INFORMATIQUE ET LIBERTE DANS L'ENTREPRISE

La révélation dans les années 70, d'un projet du gouvernement d'identifier chaque citoyen par un numéro et d'interconnecter sur la base de cet identifiant tous les fichiers de l'administration créa une vive émotion dans l'opinion publique. Ce projet connu sous le nom de SAFARI, qui montrait les dangers de certaines utilisations de l'informatique et qui faisait craindre un fichage général de la population, a conduit le gouvernement à instituer une commission auprès du Garde des Sceaux afin qu'elle propose des mesures tendant à garantir que le développement de l'informatique se réalisera dans le respect de la vie privée des libertés individuelles et des libertés publiques.

Cette commission "informatique et libertés" proposa de créer une autorité indépendante.

A la fin de l'année 1977, un projet de loi fut examiné par le parlement avant de devenir la loi du 6/01/78 relative aux fichiers et aux libertés.

Elle a une mission d'information, de proposition, de conseil et de contrôle sur les traitements informatisés. Elle dispose pour ce faire d'un pouvoir réglementaire.

La CNIL est l'organisme auprès duquel les employeurs sont tenus de déclarer préalablement toute constitution de fichier informatique.

Depuis la loi du 6/08/04, les formalités de contrôle à priori de la CNIL sur les fichiers ou les traitements automatisés de données personnelles sont allégées et les possibilités d'intervention a posteriori sont élargies par l'attribution de nouveaux pouvoirs d'investigation et la possibilité de prononcer des sanctions graduées.

Les trois types d'intervention de la CNIL au niveau de l'entreprise se situent au niveau du respect des règles par l'employeur dans les domaines suivants :

- I – Recrutement du personnel
- II – Gestion du personnel
- III – Contrôle de l'activité des salariés

### I – RECRUTEMENT DU PERSONNEL

En matière de recrutement du personnel, la nature des informations demandées et les techniques de recrutement sont encadrées : aussi chaque candidat à un emploi devra être informé préalablement à leur mise en œuvre des méthodes et techniques d'aide au recrutement et d'évaluation utilisées à son égard.

### 1) Les questionnaires d'embauche

Selon l'article L 121-6 les informations demandées, sous quelque forme que ce soit au candidat à un emploi ou à un salarié ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles.

Ces informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles.

De même en application du principe posé par l'article L 120.2, 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 ou proportionnées au but recherché.

Ces principes s'appliquent à tous les supports de collecte d'information lors du recrutement (ils doivent être déclarés à la CNIL préalablement à leur mise en œuvre).

Toute personne a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement.

A titre d'exemple, un certain nombre d'infractions caractérisées ont été relevées par la CNIL :

- des questions particulièrement indiscrettes sur l'état de santé, la vie sexuelle ou la religion du candidat.
- d'autres ont trait au conjoint, aux parents,.....
- d'autres portent sur l'utilisation des revenus, les milieux fréquentés, les motifs d'éventuelles condamnations.

### 2) Information du candidat sur les méthodes de recrutement.

Aucune information concernant personnellement un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi (L 121.8).

Cette information nous semble devoir être faite par écrit par le recruteur qui sera soit l'employeur, l'organisme de formation ou de bilan de compétence.

### 3) Information préalable du CE.

L'employeur a l'obligation aussi d'informer le CE des méthodes d'aide au recrutement des candidats à l'emploi (L 432.2.1).

## II – LA GESTION DU PERSONNEL

L'utilisation de l'informatique pour la gestion du personnel comprend les traitements relatifs à la paie et aux cotisations sociales, aux absences, au déroulement de carrière (etc.....norme n° 46).

Les traitements de gestion du personnel bénéficient du régime de la déclaration simplifiée.

Ainsi le support d'entretien annuel des salariés constitue un traitement non encore automatisé de données propres à chaque salarié non appelé à figurer sur un fichier – en tant que support de données individuelles il doit faire l'objet d'une déclaration auprès de la CNIL.

Les personnes concernées sont informées de l'identité du responsable du traitement, du caractère obligatoire ou facultatif des réponses à apporter ainsi que de leur droit d'accès aux données les concernant et de rectification de ces données

Cette information doit être délivrée à tout employé par la remise d'un document écrit ou par voie électronique.

Conformément à l'article L 432.21 du code du travail, les instances représentatives du personnel doivent être informées et consultées avant la mise en œuvre du traitement concerné. Dans l'entreprise, seules certaines personnes peuvent avoir connaissance des données recensées : personnes chargées de la gestion du personnel, supérieurs hiérarchiques des employés concernés.

La CNIL a admis que l'utilisation automatisée d'informations issues de la liste électorale des salariés (nom, prénom, date de naissance et adresse des salariés) n'avait pas à faire l'objet d'une déclaration préalable (recommandation n° 96-105 du 3/12/96).

Pour la paie informatisée dont les seules mentions sont celles définies par le code du travail, la CNIL a par une délibération du 9 décembre 2004, dispensée de déclaration, ainsi que la tenue informatisée des registres obligatoires.

Mais la CNIL précise que ce premier pas vers la suppression de certaines formalités déclaratives ne remet pas en cause les garanties existantes pour les salariés. L'ensemble de leur droit (accès, rectification, opposition) reste applicable. Par ailleurs, la CNIL conserve entier son pouvoir de contrôle et de sanction et s'assure du respect de ces droits et obligations pour l'ensemble des traitements de paie mis en œuvre.

### III – Contrôle de l'activité des salariés

Quelles sont les obligations de l'employeur ?

Tout traitement automatisé d'informations nominatives doit faire l'objet d'une déclaration préalable auprès de la CNIL.

Dès lors si le système de contrôle de l'activité des salariés implique la création d'un traitement automatisé, l'employeur doit procéder à une déclaration. Il doit au préalable, informer les salariés concernés.

En effet, le contrôle à l'insu des salariés constitue une preuve illicite (soc. 15/05/01), de même un délégué du personnel peut demander le retrait d'éléments de preuve obtenus par des moyens frauduleux qui constituent une atteinte aux droits des personnes (soc.10/12/97).

Il existe à ce niveau une distinction importante entre la chambre sociale et la chambre criminelle de la Cour de Cassation " les juges répressifs ne peuvent pas écarter les moyens de produits par les parties au seul motif qu'ils auraient été obtenus de façon illicites ou déloyale (crim. 6 avril 1994) : ainsi un film provenant d'une caméra dissimulée constitue une preuve admissible pour le juge pénal, mais pas pour la chambre sociale de la Cour de Cassation.

Le CE est aussi obligatoirement informé et consulté préalablement à la décision de mise en œuvre dans l'entreprise de moyens et techniques permettant un contrôle de l'activité des salariés.

Rappelons que les salariés peuvent saisir les délégués du personnel qui disposent d'un droit d'alerte, en cas d'atteinte aux droits des personnes et aux libertés individuelles.

Les différents contrôles que l'employeur peut pratiquer sont les suivants :

- 1) Contrôle des accès à l'entreprise.
- 2) Contrôle de l'activité et de la productivité par les communications téléphoniques.
- 3) Contrôle de l'activité par la vidéosurveillance.

- 4) Contrôle de l'activité des salariés en déplacement.
- 5) Contrôle de l'activité des salariés par l'outil informatique.

### 1) Contrôle des accès à l'entreprise

- badgeage : doit être déclaré à la CNIL (norme 42) : à défaut de déclaration à la CNIL, le refus du salarié d'utiliser son badge n'est pas un motif valable de licenciement, il s'agit donc d'une formalité substantielle. (cass.6/04/04 Sté Allied signal Industrial Fibers cf Pacheo) ;
- système biométrique : doit faire l'objet d'une autorisation de la CNIL car selon la CNIL seul un impératif de sécurité incontestable peut justifier la constitution de base de donnée d'empreintes digitales.

Le TGI de Paris par un jugement du 19/04/05 a interdit un tel système car l'objectif poursuivi n'était pas de nature à justifier la constitution d'une base de données d'empreintes digitales du personnel, le traitement pris dans son ensemble n'apparaissant ni adapté ni proportionné au but recherché. Les différents dispositifs de reconnaissance biométriques sont les suivants : reconnaissance du contour de la main et reconnaissance de l'empreinte digitale.

### 2) Contrôle de l'activité et de la productivité par les communications téléphoniques

- Comptage des communications :  
avec autocommutateurs téléphoniques : la norme n° 47 précise que les finalités sont limitées à la gestion des moyens de communication ; sur les relevés les 4 derniers chiffres sont occultés ; la durée de conservation des données relatives aux services de téléphonie est fixée à un an.

Concernant les représentants du personnel, ils doivent pouvoir disposer d'un matériel excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants (CCass 6 avril 2004).

sans autocommutateur téléphonique : concernant la production de factures détaillées, la Cour de Cassation et la CNIL ne sont pas en accord : la première estime que la production par l'employeur des relevés de facturation téléphonique constitue un mode de preuve licite même en l'absence d'information du salarié ; quant à la CNIL elle estime que l'employeur doit informer les salariés concernés qui a demandé la facture détaillée.

- Ecoute ou enregistrement des conversations : doit faire l'objet d'une déclaration préalable auprès de la CNIL, les IRP doivent être informées et consultées, les salariés doivent être informés des objectifs poursuivis par la mise en place du dispositif d'écoute, des destinataires des enregistrements et de leur droit d'accès à ces enregistrements.

La Cour de Cassation a précisé que tous enregistrements, quels qu'en soient les motifs, d'images ou de parole à l'insu des salariés constituent un mode de preuve illicite (Soc. 20/11/91).

### 3) Contrôle de l'activité par la vidéosurveillance

- Contrôle des locaux de travail :

Le salarié doit être informé du procédé de surveillance même s'il est matériellement visible (Soc. 15 mai 2001).

Les IRP doivent être consultés, les salariés doivent être informés et une déclaration à la CNIL doit être déposée pour pouvoir mettre en place un tel système dans un lieu ouvert au public, particulièrement exposé au risque d'agression et de vol et dans l'unique but de sécurité des personnes et des biens.

La sanction de l'absence d'information préalable est l'illicéité de la preuve, sachant comme nous l'avons vu précédemment, que les positions divergent sur la question entre la Chambre criminelle et la Chambre Sociale de la Cour de Cassation.

Une Cour d'appel (Aix en Provence, 4 janvier 94) a considéré que compte tenu des possibilités de montage et de trucage qu'offre l'évolution des techniques, ce document (un enregistrement de vidéosurveillance) ne présente pas des garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu.

- Contrôle des locaux qui ne sont pas des lieux de travail. :

Selon la Cour de Cassation l'employeur est libre de mettre en place des procédés de surveillance des entrepôts de rangement dans lesquels les salariés ne travaillent pas et qui n'enregistre donc pas l'activité des salariés. Un salarié filmé qui détourne des marchandises a été licencié pour faute lourde, licenciement reconnu par la Cour de Cassation car il s'agissait de locaux ne constituant pas un lieu de travail.

#### 4) Contrôle de l'activité des salariés en déplacement

Dans une recommandation, la CNIL précise que les dispositifs de géolocalisation ne doivent pas porter atteinte à la liberté d'aller et venir anonymement et au droit à la vie privée des salariés concernés. Il faut distinguer le cas où l'utilisation d'un véhicule par des salariés n'est qu'un moyen d'accomplir leur mission du transfert de personnes et de marchandises.

Un tel contrôle doit faire l'objet d'une déclaration simplifiée auprès de la CNIL, d'une information préalable des salariés concernés ainsi que des IRP.

Ce système doit de surcroît remplir certaines conditions :

- finalité du traitement : (raison valable tel que le transport de fonds ou de valeurs) ; suivi d'une prestation de transport directement lié à l'utilisation du véhicule (ramassage scolaire...), sûreté ou sécurité de l'employé, meilleures allocations des moyens pour des prestations à accomplir en des lieux dispersés (taxi, dépannage...), suivi du temps de travail quand il ne peut être réalisé d'une autre façon.
- Nature des données traitées : elles doivent avoir trait à l'identification de l'employé, aux déplacements effectués et aux informations afférentes à l'utilisation du véhicule (vitesse, temps de conduite, nombre de kms...)
- Nombre limité de destinataires des données (RH, personnes en charge de la sécurité, personnes en charges de planifier et suivre les interventions).
- Durée de conservation = 2 mois ou 1 an si elle a pour objectif la réalisation d'un historique des déplacements en vue d'une optimisation des tournées ou si c'est le seul moyen de preuve de la réalisation d'une prestation. (si données relatives aux horaires : 5 ans).

#### 5) Contrôle de l'activité des salariés par l'informatique

Les administrateurs de réseaux doivent assurer le fonctionnement normal et la sécurité des réseaux et systèmes. Pour cela, ils sont conduits à avoir accès à l'ensemble des informations mais ils ne doivent ni les exploiter, ni les divulguer et ne peuvent être contraints de le faire (rapport CNIL février 2002) + CA Paris 11<sup>ème</sup> chbre 17/12/01.

#### Contrôle des connexions internet des salariés :

L'évolution des outils informatiques impose à chacun de prendre conscience des conséquences de l'utilisation et ces outils et plus particulièrement d'internet et de la messagerie électronique dans les relations entre employeur et salarié. Où trouver le juste équilibre entre le souci légitime de la valorisation optimale et de la préservation de l'outil de travail et le tout aussi légitime respect des libertés individuelles et de la vie privée ?

A l'entreprise de définir, dans le cadre de ses prérogatives, la marge de tolérance qu'elle entend adopter face aux utilisations choisies et aux utilisateurs désignés.

Au salarié de limiter et de prendre conscience du respect des règles légales et professionnelles. Les abus d'utilisation sont à proscrire et les abus de surveillance sont à éviter.

Lorsque l'entreprise met en place des logiciels permettant de surveiller les connexions des salariés (sites visités, temps passé....) ils doivent être déclarés à la CNIL et les salariés doivent en être informés.

On peut penser qu'un usage abusif d'internet sur le temps de travail pourrait être sanctionné, voire constituer une cause réelle et sérieuse de licenciement lorsque l'employeur apporte la preuve de la légitimité des griefs reprochés au salarié.

Mais pour éviter les litiges et difficultés de rapporter des preuves d'une utilisation abusive de l'internet ou de l'intranet, il est recommandé à l'employeur de fixer de façon claire et précise les droits et obligations du salarié dans le règlement intérieur, note de service voire charte d'utilisation.

Traçage informatique : selon la CNIL, les salariés doivent être informés du traçage informatique.

Pourtant la Cour de Cassation du 18/07/00 a admis le licenciement pour faute grave d'un salarié qui consultait par pure curiosité personnelle des comptes sans relation avec ses tâches professionnelles, alors même que le système de surveillance électronique n'avait pas été porté à la connaissance des salariés et des IRP.

C'est le 1<sup>er</sup> arrêt qui se prononce sur les problèmes de traçage informatique.

#### Contrôle des fichiers personnels stockés sur le disque dur de l'ordinateur du salarié :

L'employeur ne peut ouvrir des fichiers nommés personnels qu'à deux conditions : que le salarié soit présent ou informé + l'existence d'un risque ou d'un événement particulier pour l'entreprise.

Les fichiers stockés sur l'ordinateur du salarié sont présumés avoir un caractère professionnel et peuvent donc être ouverts par l'employeur hors de la présence du salarié, sauf lorsque le fichier est intitulé "personnel" arrêt 2 octobre 2001 Nikon " l'employeur ne peut pas ouvrir un

email d'un salarié marqué personnel même lorsque le règlement interdit d'utiliser le matériel à des fins personnelles".

#### Contrôle de l'usage de la messagerie électronique par les salariés :

L'employeur peut surveiller et contrôler l'activité des salariés mais pas sans limite : il doit en informer les salariés et veiller au respect de la vie privée de ces derniers.

L'employeur devra justifier le contrôle exercé par un intérêt légitime, tel que des problèmes de sécurité (préservation du secret des affaires) ou la nécessité d'éviter des usages abusifs ou préjudiciables à l'entreprise : les moyens mis en œuvre devront être proportionnés au but recherché.

Si l'entreprise met en œuvre un dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, le traitement automatisé d'informations nominatives doit être déclaré à la CNIL.

#### Emails personnels et correspondance privée :

Le tribunal correctionnel de Paris a jugé que le courrier électronique constitue de la correspondance privée protégée dès lors qu'il est envoyé de personne à personne (TGI Paris 17 chambre correctionnelle 2/11/00).

Cette décision a été confirmée par la CA de Paris (17/12/01) mais a estimé que ça n'interdit pas l'accès des administrateurs de réseaux aux messageries et à leur contenu.

C'est dans l'arrêt Nikon que la Cour de Cassation s'est prononcée pour la première fois (C Cass. 2/10/01).

Par cet arrêt, les juges affirment l'inviolabilité de la correspondance et des fichiers informatiques personnels des salariés.

Dans son rapport de 2002, la CNIL a proposé de considérer qu'un mail envoyé ou reçu depuis le poste de travail mis à disposition par l'entreprise revêt en principe un caractère professionnel sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire qui lui conférerait alors le caractère et la nature d'une correspondance privée protégée. Sans indication précise de leur contenu et à condition que les salariés aient été informés des éventuels contrôles les mails seront alors présumés professionnels et, à ce titre, susceptibles d'être lus par l'employeur.