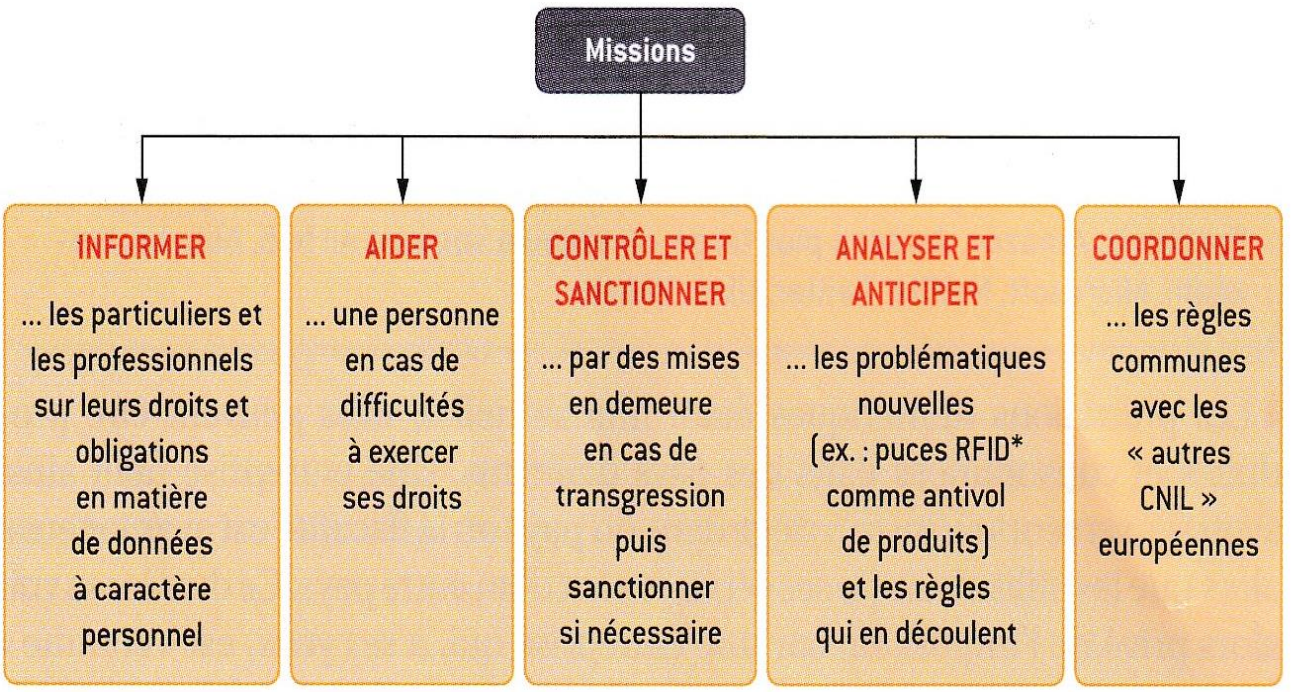
31 La protection de la personne dans l'univers numérique

La création et l'utilisation d'un fichier, l'usurpation d'identité, la surveillance des salariés, autant de pratiques intemporelles que le droit encadre déjà. Néanmoins, le numérique, s'il ne crée pas une nouvelle problématique, en change cependant la perception et les enjeux nécessitant des règles propres.

1 La Commission nationale de l'informatique et des libertés (CNIL)

Créée en 1978 par la loi Informatique et Libertés, la CNIL est une autorité administrative indépendante.



2 Les données à caractère personnel (DCP)

A Identifier un auteur et une œuvre de l'esprit

Dans son activité, l'entreprise ne cesse d'utiliser des DCP, c'est-à-dire des éléments propres à une personne, un salarié comme un client, et qui permettent de l'**identifier** comme un être unique :
- **directement** : nom et numéro de téléphone d'un prospect (démarchage téléphonique par exemple) ;
- **indirectement** : numéro de Sécurité sociale d'un salarié : sans la base de données du fichier du personnel, la seule connaissance du numéro ne permet pas de savoir de qui il s'agit.

À noter

Certaines DCP ont un statut particulier car elles concernent des éléments parfois délicats de la vie privée d'une personne : données médicales, ethniques, religieuses... Elles sont qualifiées de « sensibles » et sont interdites sauf autorisation de la CNIL pour les exceptions justifiées.

B Les obligations de l'entreprise en matière de DCP

Deux grands textes juridiques réglementent les DCP : la loi Informatique et Libertés de 1976 et le Règlement général sur la protection des données (RGPD) qui, en 2016, est le texte communautaire de référence en la matière. Au sein de l'entreprise, la personne responsable des DCP est le « **responsable du traitement** », c'est-à-dire la personne physique ou morale qui **détermine les finalités** (ce à quoi les DCP vont servir) et les **moyens employés** (selon quelles modalités s'effectuera le traitement). Ses grandes obligations sont :

Obtenir le consentement des personnes fichées : c'est l'étape de la collecte des données, la personne fichée doit être informée et avoir explicitement accepté que des DCP la concernant soit recueillies. Les informations données pour obtenir ce consentement doivent être loyales (pas de faux motif) et transparentes.

Définir les finalités du fichier : le responsable de traitement doit préciser ce à quoi les DCP collectées vont lui servir. Il ne pourra pas par la suite utiliser ces données pour un autre objectif que celui annoncé. Par ailleurs, une communication de ces données à des tiers sans le consentement préalable de la personne fichée est interdit.

Sécuriser les données : cette obligation comprend 3 grandes dimensions : la sécurité des locaux (serveurs dans une salle fermée), la sécurité informatique (anti-intrusion ou piratage) et le contrôle des personnes habilitées.

Limiter la collecte des données : la finalité permet de définir les informations à collecter et de s'y tenir : c'est le principe de minimalisation de la collecte. La durée de conservation est proportionnelle aux objectifs du fichier. À la fin de cette durée, les fichiers doivent être détruits.

Respecter les droits des personnes

- **Droit d'accès :** un individu peut demander directement au responsable d'un fichier s'il détient des informations sur lui, et préciser qu'il veut qu'elles lui soit communiquées intégralement et sous une forme compréhensible.
- **Droit de rectification :** l'article 40 de la loi du 6 janvier 1978 modifiée permet à toute personne de rectifier, compléter, actualiser, verrouiller ou effacer des informations qui la concernent lorsqu'elles sont erronées, inexactes, incomplètes, périmées ou s'il s'agit de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.
- **Droit d'opposition :** toute personne physique peut, si elle a un motif légitime, s'opposer à ce que des données la concernant fassent l'objet d'un traitement. Elle peut en outre refuser (sans frais) que ses données soient utilisées à des fins de prospection commerciale.
- **Droit de déréférencement :** une personne peut demander aux moteurs de recherche de ne plus indiquer une page web associée à son nom et à son prénom.

3 L'identité numérique

L'identité numérique d'une personne correspond au **lien technologique** entre une personne réelle et son entité virtuelle. Elle est un ensemble d'éléments provenant :

- des **données personnelles** saisies dans les comptes créés en ligne ;
- des **informations publiées** par (ou sur) une personne par des tiers ;
- les **traces numériques** laissées volontairement ou non par une personne (cookies, historique de navigation...).

L'usurpation d'identité numérique peut prendre des formes variées mais les cas les plus fréquents sont le piratage puis l'utilisation d'un compte sur un réseau social ou l'envoi de mails frauduleux et de l'usage d'un masque pour modifier le nom de l'émetteur d'un mail.

La protection de l'identité numérique est prévue par le **Code pénal** qui définit tout d'abord le délit d'usurpation d'identité numérique et en prévoit la sanction à l'**article 226-4-1** : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.* »

4 L'usage du numérique dans l'activité de travail

A Le droit au respect de la vie privée

Le premier principe à respecter ne découle pas du Code du travail mais de l'article 9 du Code civil « Chacun a droit au respect de sa vie privée » que la jurisprudence applique à la vie en entreprise (arrêt Nikon, 2001). On peut y ajouter 2 autres règles du Code du travail :

- tout **dispositif de surveillance d'un salarié** doit avoir été porté à sa connaissance (article L1222-4) ;
- les **atteintes aux libertés individuelles** (s'exprimer sur un réseau social par exemple) et **collectives** d'un salarié doivent être justifiées et proportionnées (article L1121-1).

B La surveillance du poste informatique du salarié

Ce que fait le salarié « *off line* » comme « *on line* »

- L'employeur **peut surveiller** l'activité du salarié sur le poste informatique par les fonctionnalités techniques permises par le réseau. Cette surveillance doit avoir été **portée à la connaissance** de l'employé (charte informatique).
- L'employeur **ne peut pas interdire totalement** que le salarié effectue une activité personnelle sur son poste informatique (« petit » jeu, consultation de la messagerie personnelle). Une sanction n'est possible que si la durée est excessive ou si la déconcentration provoquée porte préjudice aux tâches à réaliser. Il peut néanmoins : ne pas permettre l'installation de jeux ou d'un navigateur internet sur un poste ; interdire une utilisation spécifique (téléchargements importants) qui monopoliserait excessivement la bande passante, pénalisant le travail des salariés ; contrôler que le salarié n'utilise pas les ressources numériques de l'entreprise pour des activités illicites (téléchargements d'œuvres protégées par le droit d'auteur).

Ce qu'enregistre le salarié

Le contenu d'un disque dur	La messagerie @	Les périphériques de stockage personnels
• L'employeur peut le/la consulter. • L'employeur ne peut ouvrir un fichier identifié comme personnel par son nom ou par son classement dans un répertoire de type « perso ».		Ils sont présumés professionnels s'ils sont connectés au poste de travail professionnel du salarié.

C La surveillance du salarié en dehors du poste informatique

- Il est normal que l'employeur cherche à s'assurer de l'**effectivité du travail** pendant le **temps rémunéré**. Il peut donc installer des systèmes numériques de **contrôle des horaires** ou de **géolocalisation** des salariés. Ceux-ci doivent, en plus de la CNIL, en avoir été informés collectivement (institutions représentatives du personnel) et individuellement (contrat de travail, courriel...).

- La **vidéosurveillance** par l'employeur est licite et soumise aux mêmes règles d'informations qu'énoncées ci-dessus. L'employeur ne peut pas, sous peine de nullité de la preuve fournie, utiliser un enregistrement **non conforme à la finalité déclarée à la CNIL**.

Exemple

Un employeur ne peut pas licencier un salarié toujours en retard grâce à une caméra installée pour lutter contre les vols des clients.

- Enfin, un employeur peut surveiller l'**activité téléphonique** de ses salariés. Un simple relevé fourni automatiquement par l'opérateur ne nécessite pas d'information préalable mais l'installation d'un système de contrôle spécifique (notamment un **autocommutateur**) obéit aux mêmes règles que les autres systèmes.