Thème 4 : L'impact du numérique sur la vie de l'entreprise

Chapitre V – La protection des personnes et des données

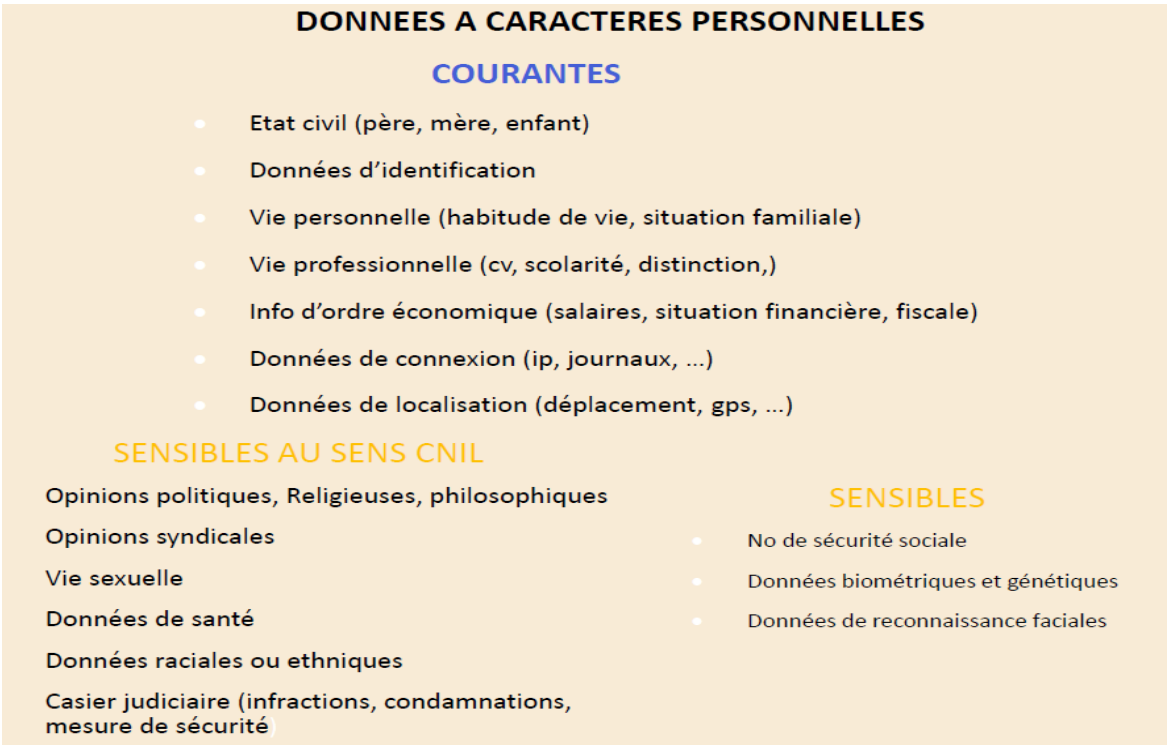
COMPETENCES	SAVOIRS ASSOCIES
- Caractériser les conséquences juridiques des choix opérés par l'entreprise sur la protection des personnes, des données	- La protection de la personne : les données à caractère personnel, l'identité numérique, l'usage du numérique dans l'activité de travail

SYNTHESE ENRICHIE

Avec la digitalisation des échanges, les données à caractère personnel (DCP) sont un enjeu marketing et stratégique pour les entreprises. Mais la collecte et le traitement de ces données entraînent des risques et nécessitent un cadre réglementaire afin de protéger les personnes. La CNIL a un rôle important, notamment depuis la mise en place du RGPD.

I. La protection des données à caractère personnel

L'article 4 du RGPD définit une donnée à caractère personnel comme « **toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement ».**



Une personne peut être identifiée par son nom, son numéro de client, des données sur sa localisation ou son adresse IP, mais aussi par un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale comme la voix (enregistrement téléphonique) ou l'image (photos, vidéos).

Utiliser une application, créer un compte client, commander sur Internet, génèrent des données à caractère personnel. Ces données sont un atout concurrentiel pour les entreprises. Connaissant mieux ses clients, elles développent des offres commerciales adaptées aux profils de ces clients et de plus en plus personnalisées.

II. Le cadre réglementaire relatif à la protection des personnes et des données

A. La Commission Nationale de l'Informatique et des libertés (CNIL)

La CNIL est une AAI (Autorités administratives indépendantes) chargée de veiller au respect de la vie privée et des libertés dans le monde numérique.
Ses principales missions sont :
– d'informer et conseiller les citoyens, les professionnels et les autorités publiques ;
– de contrôler le respect de la loi par les professionnels et les administrations ;
– de sanctionner les abus et les pratiques irrégulières :
- avertissement,
- une mise en demeure visant à contraindre les entreprises à mettre en place des actions correctives,
- une sanction financière de 10 à 20 millions d'euros ou de 2 à 4 % du chiffre d'affaires annuel mondial.

Son rôle de contrôle a été renforcé par le RGPD.

B. Le Règlement général sur la protection des données (RGPD)

Le RGPD fixe la nouvelle réglementation au niveau européen (depuis 2018) sur la protection des DCP des personnes physiques lors de leur traitement et de leur circulation.
Ses trois objectifs principaux sont :
- renforcer les droits des personnes ;
- responsabiliser les acteurs intervenant dans le traitement des données ;
-assurer une protection efficace des données.

1 – Renforcer les droits des personnes :

Le RGPD a renforcé les droits des personnes en reprenant les dispositions de la loi Informatique et Libertés de 1978 :
- **Droit d'accès** : une personne peut demander directement au responsable d'un fichier s'il détient des informations sur elle et se les voir communiquer ;
- **Droit de rectification** : s'il y a des erreurs sur les données enregistrées ;
- **Droit d'opposition** : toute personne physique peut, si elle a un motif légitime, s'opposer à ce que ses données fassent l'objet d'un traitement ;
- **Droit à l'effacement = droit à l'oubli**.

De nouveaux droits ont été ajoutés avec le RGPD :
- **Droit à la portabilité des données** : une personne peut récupérer et transférer ses données sans subir de problèmes d'interopérabilité qui pourraient la dissuader de changer de prestataire
- **Droit à la notification** en cas de piratage de ses données personnelles
- **Droit d'intenter une action de groupe** : des personnes victimes d'une infraction relative à leurs DCP peuvent agir collectivement en justice via une association
- **Droit à la réparation du dommage matériel ou moral** pour les conséquences issues d'un préjudice lié à un mauvais traitement de leurs DCP (en général une faille de sécurité).

2 – Responsabiliser les acteurs intervenant dans le traitement des données :

Le RGPD a introduit une **logique de responsabilisation (principe d'accountability)** : les entreprises doivent s'assurer en permanence de la conformité du traitement des données personnelles et doivent à tout moment être en mesure de savoir quelles sont les données collectées et dans quel but. Elles doivent justifier cette conformité, en tenant à jour **un registre des traitements.**

3 – Assurer une protection efficace des données :

Pour respecter ce principe d'accountability, différentes mesures doivent être prises :

– **le traitement des données repose sur des bases légales** : l'exécution d'un contrat, une obligation légale, l'exécution d'une mission d'intérêt public, l'intérêt vital, intérêt légitime ;
Dans tous les cas, le consentement de l'internaute doit être demandé.
– **le respect des droits des utilisateurs** : minimisation des données, droit de rectification, d'opposition, information des utilisateurs, etc. ;
– **mise en place des mesures de sécurité pour la conservation des données** : principe de confidentialité, d'intégrité, de disponibilité.
– **nomination d'un délégué à la protection des données (DPO)** : Il a une mission d'information, de conseils, de contrôle et d'interface. Il va impulser, piloter, coordonner les actions de mise et de maintien en conformité de l'organisme.
– **sensibilisation et formation du personnel aux enjeux de la protection des données personnelles**.

De plus, le traitement de données personnelles doit respecter 2 principes :
– **le principe du « privacy by default »**, c'est-à-dire assurer, dès le départ, le plus haut degré de protection des données, sans action spécifique de la part des utilisateurs ;
– **le principe du « privacy by design »** : il s'agit d'intégrer des mesures de protection de la vie privée dès la conception d'un produit ou d'un service.

En cas de violation de données, les entreprises doivent **notifier** l'incident à la CNIL s'il existe un risque au regard de la vie privée des personnes concernées. En cas de risque élevé, les personnes concernées doivent en être informées. En cas de manquement par une entreprise à des règles du RGPD, toute personne peut introduire une réclamation auprès de la CNIL ou une action de groupe.

III – L'identité numérique de l'entreprise et de ses salariés

A – Les composantes de l'identité numérique.

L'identité numérique est constituée de l'ensemble des contenus publiés sur Internet permettant de définir un individu : éléments d'authentification, données, signes de reconnaissance, traces numériques.
L'identité numérique peut être décomposée en 3 parties :
- **L'identité déclarative** : qui correspond aux données saisies par l'utilisateur (email, nom, prénom, date de naissance, identifiants..) .
- **L'identité agissante** : liée directement aux activités de l'internaute (habitudes, préférences de navigation, photos, vidéos…). Les traces laissées sont volontaires.
- **L'identité calculée** : le nombre de réseaux sociaux où l'utilisateur évolue et l'engagement que ses posts recoivent (nombre d'amis, nombre de groupes..). Ce sont ici des traces héritées ou involontaires.

B – Les enjeux de le-réputation et de l'usurpation d'identité.

L'e-réputation désigne les éléments de la notoriété d'une entreprise véhiculés sur des supports en ligne.
L'usurpation de l'identité numérique est le risque majeur pour les particuliers ou les entreprises, qui peuvent être victimes d'escroqueries ou voir leur **e-réputation** se dégrader. Elle est sanctionnée pénalement (peine d'emprisonnement et amendes- article 226-4-1 du code pénal)).
La victime de l'usurpation peut obtenir des dommages et intérêts en réparation du préjudice subi.

Il faut faire une **distinction entre l'identité numérique et l'e réputation**. Cette dernière ne dépendant pas de ce que l'entreprise choisit de publier, mais bien de ce que les internautes publient à son propos (avis sur Google, commentaires sur les réseaux sociaux, articles de blog, etc.) sur internet.

En d'autres termes, l'identité numérique est la partie gérable de **l'image de son entreprise**, quand **l'e-réputation est la partie « subie »**, qu'elle soit positive ou négative. L'information communiquée par l'entreprise doit donc être méticuleusement préparée pour éviter toutes retombées négatives.

C – L'obligation de respect de la vie privée des salariés.

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.
On peut y ajouter 2 autres règles du code du travail :
- tout dispositif de surveillance des salariés doit avoir été porté à sa connaissance (article L222-4)
- Les atteintes aux libertés individuelles (ex : s'exprimer sur un réseau social) et collectives d'un salarié doivent être justifiées et proportionnées (article L 1121-1)

IV – L'usage du numérique dans l'activité de travail

A – L'usage personnel de l'informatique par les salariés

Un employeur peut surveiller l'activité informatique de ses salariés en les ayant informés au préalable, idéalement au moyen **d'une charte informatique**.

Il peut aussi veiller à ce que les utilisations personnelles de l'outil informatique :
- demeurent raisonnables (notamment en termes de volume horaire)
- Ne remettent pas en cause la sécurité du système informatique (pas de téléchargement potentiellement infecté)
- Ne limitent pas la disponibilité du système informatique pour les besoins professionnels (pas de stockage trop volumineux ou de captation excessive de la bande passante)
- Ne diminuent pas la productivité du travail (diminution de ses rendements en raison de ses occupations personnelles).

La consultation du poste informatique du salarié est licite, à l'exception des documents identifiés comme personnels. Dans ce cas, l'employeur ne peut les consulter qu'en présence du salarié.

B – La surveillance de l'activité des salariés

L'employeur peut utiliser les outils numériques pour surveiller les locaux, le matériel, mais aussi l'activité des salariés (vidéosurveillance, géolocalisation…). L'objectif est la sécurisation des données de l'entreprise et la sécurisation de l'accès au réseau de l'entreprise.

Dans tous les cas, l'employeur doit respecter les règles suivantes :
- Consultation des représentants du personnel
- Licéité de la finalité déclarée puis suivie par la mise en place de cet outil
- Proportionnalité de l'outil et de son utilisation au but poursuivi (ex : lutter contre les vols ne justifie pas une caméra filmant des employés administratifs à leurs bureaux)
- Information préalable des salariés de la mise en place et utilisation de ces dispositifs

En cas de manquement à ces obligations, outre les éventuelles infractions commises, l'entreprise se verrait priver des informations collectées comme preuve lors d'une action en justice.