Chapitre 3 : la protection des personnes dans l'univers du numérique.

1. Les données à caractère personnel et leur protection.

Une donnée personnelle correspond à toute information permettant d'identifier une personne physique.

1) Le besoin de protection des données à caractère personnel.

- L'utilisation des données personnelles à des fins commerciales, dans les entreprises les base de données constitue un marché apparent tiers, en effet les données des clients présente une valeurs marchandes considérable est les entreprises multiplies les outils pour les collecter. Cela leur permet notamment de cataloguer les personnes et ainsi de cibler leurs messages publicitaires.

- L'utilisation de l'identité numérique a des fins malveillante, l'identité numérique, c'est l'ensemble des traces laissées par un individu sur Internet. Notre identité numérique peut faire l'objet d'une usurpation par une personne qui souhaite commettre des actes répréhensibles ou illégaux sous une fausse identité, cela peut être aussi de bénéficier des avantages à la place d'une autre personne ou encore de porter atteinte à la réputation d'une personne dont l'identité est usurpée. L'usurpation de l'identité numérique est considérée comme un délit inscrit au code pénal, ce délit et généralement commis de deux manières : par la technique du phishing (technique frauduleuse destinée à tromper l'internaute pour l'inciter à communiquer ces données personnelles en se faisant passer par un tiers de confiance), la deuxième technique consiste en la création d'un faux site web ou d'un faux profil sur un réseau social, le délit d'usurpation d'identité numérique est punis d'un an d'emprisonnement est de 15 000 euros d'amendes

2) Les règles juridiques qui protègent les données à caractère personnel.

C’est le RGPD (Règlement Général sur la Protection des Données) qui constitue le texte de référence européen en matière de protection des données.

Le RGPD renforce et unifie la protection des données des individus au sein de l’Union européenne, le RGPD à énumérer les droits des individus sur leurs données personnelles.

- **Le droit à l’information** signifie que toute personnels doit être informé du traitement que seras fait de leurs données s’il en fait la demande.
- **Le droit d’accès et de rectification** signifie que toute personnel qui justifie que son identité détient le droit d’accèdes à ses données qui font l’objet d’un traitement par un organisme, est à demander à le modifier si nécessaire.
- **Le consentement** signifie qu’il doit être donné de façon claire est libre est peut-être retirer à tout moment par les personnes qui le demande.
- **Le droit à la portabilité** signifie que tout individu peut récupérer les données qui a fourni est les transférer ensuite à un autre organisme gratuitement.
- **Le droit à l’effacement ou l’oublie** signifie qu’une personne a le droit de demander l’effacement de ces données est au droit au déréférencement.
- **Le droit d’apposition** signifie qu’une personne a le droit pour des raisons légitime à ce que des informations la concernant face à l’objet d’un traitement.

3) La CNIL.

En France, c’est la CNIL qui garantit le respect du RGPD par les entreprises est les administrations. La CNIL dispose d’une mission qui consiste au respect du RGPD de manière préventive en informant les individus de leurs droits, et en accompagnant les entreprises dans leurs mises en conformité avec le RGPD. La CNIL agit aussi de manière curative, elle réceptionne les plaintes des personnes et sanctionne les entreprises qui ne respectent pas le RGPD.

Les pouvoirs de sanction de la CNIL sont les suivants :

- Elle peut prononcer une mise en demeure visant à inciter une entreprise à adopter les mesures nécessaires pour se mettre en conformité avec le RGPD.
- Elle peut prononcer une amande pécuniaire d’un montant important. (10 à 20 millions d’euros ou de 2 à 4 % du chiffre annuels)

2. Les conséquences juridiques de la protection des données personnelles pour l'entreprise.

1) Les obligations issues du RGPD pour les entreprises.

⇨ Le principe de responsabilisation (« accountability ») c'est l'obligation pour les entreprises de prendre des mesures qui permettent de démontrer le respect des règles relatives à la protection des données.

La CNIL incite les entreprises a désigné un délégué à la protection des données qui aura pour mission de prouver que les mesures nécessaires, on était prise. Dans certaines organisations, le déléguer à la protection des données est obligatoire.

⇨ Assurer des mesures préventives :

- « Privacy by design » C'est le principe du respect de la vie privée dès la conception. Ce principe oblige les entreprises à trouver des solutions en amont, et de ne pas attendre l'existence d'une faille.
- « Privacy by default » C'est le principe de la protection des données par défaut, ce principe impose aux entreprises de paramètre par default avec un haut niveau de protection

2) La protection des données personnelles des salariés.

Les prérogatives (avantage de l'employeur) sont limitées, par son obligation de respecter la vie privée de ces salariés.

L'employeur est tenu de respecter les règles du RGPD :

- Il ne peut collecter que les données personnelles nécessaire à la gestion des salariés.
- Il doit sécuriser les données personnelles collectées.
- Il doit permettre au salarié de pouvoir exercer leur droit que leur reconnaît le RGPD.

L'employeur peut encadrer l'utilisation des outils numérique par les salariés afin de garantir la sécurité du réseau de l'entreprise, est de s'assurer que les salariés remplissent bien leur mission.

S'il existe une tolérance pour permettre l'utilisation des outils numérique à titre privé, il faut que ce temps d'utilisation soit raisonnable.
L'employeur est donc en droit de s'assurer du caractère non-abusif.
L'employeur a le droit de surveiller, c'est salarié et peut librement inspecter l'ordinateur qu'il utilise dans le cadre professionnel même sans sa présence pour rechercher la nature

des sites visités, si un salarié veut protéger un dossier (un message personnel, un fichier) il doit l'identifier dans son objet comme « personnel ou privé. »

Le code du travail prévoit qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté à sa connaissance au préalable. Les salariés doivent donc être informés de la mise en place d'un système de vidéo-surveillance sur leurs lieux de travail.