**Le cadre juridique des données à caractère personnel**

1. Une donnée personnelle est une information qui permet d’identifier ou de reconnaître une personne, directement ou indirectement. Il peut en effet s’agir d’un nom, d’un prénom, d’une photo, d’une date de naissance, d’un statut matrimonial, d’une adresse postale, d’une adresse électronique, d’un e-mail, de l’adresse IP d’un ordinateur, d’un numéro de Sécurité sociale, d’un numéro de téléphone, d’un numéro de carte bancaire, de la plaque d’immatriculation d’un véhicule, d’une empreinte génétique, d’un élément d’identification biométrique, etc.
2. Comme l’illustre l’annexe 2, l’internaute est confronté à la « volatilité » et à la vulnérabilité des données stockées sur son ordinateur.
3. Les questions de protection des données personnelles sont aujourd’hui au centre de la vie quotidienne : au travail, dans les relations avec les autorités publiques, dans le domaine médical, lorsque l’on surfe sur Internet, que l’on consomme, etc. Tous ces actes impliquent la collecte d’informations personnelles pour alimenter des fichiers toujours plus nombreux.

Il y a donc développement de multiples dangers que les réseaux sociaux, et plus généralement toutes les technologies de l’information et de la communication, peuvent présenter pour leurs utilisateurs, compte tenu du mélange possible entre les données touchant à la vie privée et les éventuelles répercussions sur la vie professionnelle des intéressés

Ainsi, l’exemple de l’ « e-réputation », image numérique d’une personne sur Internet, permet de mesurer les dangers à voir un recruteur, un employeur, un client, un ami ou membre de la famille, etc., être avisé d’informations que l’on n’aurait pas souhaité divulguer.

1. Les données personnelles sont les noms et les coordonnées des personnes listées dans les fichiers.

Il s’agit d’utilisations abusives de fichiers pouvant nuire aux personnes qui y figurent. La CNIL peut même trouver des commentaires péjoratifs et subjectifs pouvant nuire aux personnes concernées.

1. Des bases de données peuvent se révéler dangereuses dès lors qu’elles ne se cantonnent pas à l’enregistrement de données objectives mais contiennent des données subjectives, avec les risques liés à des commentaires à caractère raciste, politique, etc.
2. En droit communautaire, la collecte de données à caractère personnel n’est légale que dans des conditions strictes de : proportionnalité, transparence et finalité légitime du traitement des données. Ainsi, les personnes ou organisations qui collectent et gèrent vos informations personnelles sont tenues d’empêcher leur utilisation à mauvais escient et de respecter certains droits conférés aux propriétaires de ces données par le droit communautaire.
3. La directive européenne pose des limites relatives à la collecte et à l’utilisation des données à caractère personnel, sachant qu’il est nécessaire de créer, dans chaque État membre, un organisme national indépendant chargé de la protection de ces données.

**Le rôle des autorités de régulation**

1. La CNIL (Commission nationale de l’informatique et des libertés) a pour interlocuteurs les particuliers et les entreprises qui traitent des données personnelles.
2. La CNIL veille à ce que l’informatique soit au service de chaque citoyen, sans porter atteinte à l’identité humaine, aux droits de l’homme, à la vie privée ou aux libertés individuelles ou publiques. Cette autorité administrative indépendante est chargée d’organiser la protection des personnes physiques à l’égard des traitements des données à caractère personnel et exerce, dans ce but, de nombreuses missions.
3. Les faits :

La société Fnac Direct, conservais dans une même base de données plusieurs informations, le nom du titulaire de la carte, la date de validité de la carte, et parfois le cryptogramme visuel, et même le numéro de la carte dans un format insuffisamment sécurisé. La base comprenait plusieurs millions de carte en cours de validité ou la validité était expiré sans qu'elles soit supprimé de la base.

Sanction :

Un avertissement pour que la Fnac procède à un changement sur les informations

1. Les données bancaires doivent avoir des mesures de sécurités élevé, ce sont des données sensibles qui touchent au patrimoine des personnes
2. La CNIL joue son rôle dans la protection des données personnels, elle rappelle que les données ainsi collectés ne devraient être conservé que sur une durée limitée et dans des conditions de sécurité renforcé.
3. Le CIL est une personne qui gère les données détenues au sein de son entreprise, il est se titre le garde-fou de l'application de la loi informatique et liberté.
4. A – droit à l'information préalable

B – droit d'acces

C – droit de curiosité

D – droit de communication

E – droit de rectification

F – droit d'opposition

G – droit d'oublie