# CHAP. III : LA PROTECTION DES PERSONNES DANS L'UNIVERS NUMERIQUE

Dans un environnement de plus en plus numérique, **les individus laissent des traces en utilisant les nouvelles technologies** d'information et de communication : **ils livrent ainsi des données à caractère personnel** (DCP), c'est-à-dire des informations relatives à leur vie personnelle, professionnelle, amicale, sentimentale, **qui nécessitent d'être protégées par des règles juridiques** (I). La protection mise en place par le droit doit être prise en compte et **respectée par toutes les entreprises** qui exploitent ce type de données (II).

## I. Repérer les enjeux de la protection des données à caractère personnel

### A. Le besoin de protection des données à caractère personnel

**La navigation sur Internet, les applications pour smartphone et les outils digitaux** utilisés par les entreprises conduisent **les personnes à livrer** de plus en plus d'**informations qui permettent, directement ou indirectement, de les identifier**. Ces données, dites « à caractère personnel » (**adresse IP, prénom, nom, coordonnées, localisation, goûts, habitudes…**) **révèlent une part importante de la vie privée** des individus et doivent, à ce titre, être protégées. En effet, le traitement de ces données par d'autres personnes comporte **plusieurs risques** :

– le **risque d'une exploitation commerciale par des E**, (**profilage publicitaire**) ;

– le **risque d'une exploitation politique par des pouvoirs publics**, afin d'**influencer l'opinion publique à l'occasion d'élections** ;

– le **risque d'une exploitation frauduleuse par des pirates**, qui pourraient **usurper l'identité numérique** dans un but malveillant.

**Le droit a donc dû intervenir pour protéger ces DCP** (**la vie privée des individus**).

### B. Les règles juridiques protégeant les données à caractère personnel

Actuellement, la protection des DCP est assurée par le règlement général sur la protection des données (**RGPD**). Ce règlement, pris dans le cadre de l'Union européenne et applicable **depuis** le 25 mai **2018**, **renforce les droits des résidents européens et s'impose à toute organisation, établie dans ou hors de l'UE, qui exploite leurs DCP.**

**- il a amélioré les moyens d'information des personnes sur la collecte et l'utilisation de leurs DCP (information sur les données collectées, durée de conservation, utilisation faite, et information en cas de piratage).**

**- il permet aux individus de maîtriser davantage leurs DCP : ils doivent autoriser les entreprises à les utiliser (recueillir leur consentement), ils peuvent demander une copie des données détenues, leur rectification, leur suppression, leur transfert vers un autre service (« droit à la portabilité ») et s'opposer à leur utilisation.**

En cas de manquement par une entreprise à des règles du RGPD, **les personnes victimes d'un préjudice similaire peuvent agir en justice ensemble pour obtenir réparation au moyen d'une action de groupe**.

### C. L'organe de protection des données à caractère personnel

En France, c'est la **Commission nationale de l'informatique et des libertés (CNIL) qui garantit le respect du RGPD** par les entreprises et les administrations. La CNIL dispose de missions lui permettant d'assurer l'effectivité du RGPD :

**- de manière préventive** (**information des individus sur leurs droits, accompagnement des entreprises pour se mettre en conformité avec les règles**) et

**- de manière curative** (**réception des plaintes** émises par les personnes, **sanctions** des organisations ne respectant pas le RGPD).

La CNIL a vu ses pouvoirs de sanction renforcés :
– elle peut prononcer une **mise en demeure**, visant à inciter une entreprise à adopter les mesures correctives nécessaires pour se mettre en conformité avec le RGPD ;
– elle peut prononcer une **amende pécuniaire** d'un montant dissuasif (de **10 à 20 millions d'euros ou de 2 à 4 % du chiffre d'affaires annuel mondial**).

### D. La protection contre l'usurpation de l'identité numérique

**Usurpation d'identité numérique : fait pour une personne, de collecter toutes les données à caractère personnel d'une autre personne afin de se faire passer pour cette dernière dans un but malveillant** (contracter une dette, tenir des propos infamants ou dégradants…).
Elle est **sanctionnée pénalement** (peine d'**emprisonnement et amendes**). La victime de l'usurpation peut **également** obtenir condamnation **civile** des **dommages-intérêts** en réparation du préjudice subi.

## II. Caractériser les conséquences juridiques de la protection des données personnelles pour l'entreprise

### A. Les obligations issues du RGPD pour l'entreprise

Toute entreprise qui exploite des DCP pour son activité de production de biens ou de services doit respecter les règles européennes de protection de ces données.
**Le RGPD a introduit une logique de responsabilisation (« *accountability* ») : les entreprises doivent anticiper, par des outils adéquats, les risques d'exploitation malveillante des DCP** qu'elles collectent et analysent. Elles doivent pouvoir prouver, à tout moment, qu'elles respectent la réglementation en la matière.
**Pour assurer leur mise en conformité avec le RGPD, les entreprises sont guidées par 2 principes** :
– le **principe du « *privacy by default* »**, qui les enjoint d'**assurer**, **dès le départ**, **le plus haut degré de protection des données** ;
– le **principe du « *privacy by design* »**, qui impose aux entreprises de **prévoir**, **dès la conception d'un nouveau produit ou d'une nouvelle procédure** qui nécessitera l'exploitation de données personnelles, **des mesures préventives de sécurisation des DCP** (mise en place d'un **registre de traitement** des données pour récapituler les données collectées et les mesures mises en place, réalisation d'une **analyse d'impact** permettant de prévenir les risques d'atteinte à la vie privée, rédaction d'une **charte de protection des DCP**…).
Les entreprises sont incitées à **désigner un délégué à la protection des données (*Data Protection Officer* – DPO), chargé de veiller à la fois au respect du RGPD** dans l'E **et à l'adaptation permanente des processus avec l'évolution technologique** (**démarche d'amélioration continue**).

### B. La protection des données personnelles des salariés

Traitant des DCP de ses salariés dans le cadre de leur activité professionnelle pour gérer leurs carrières et leurs missions, **l'employeur** est tenu de respecter les règles du RGPD :
– il **ne peut collecter que les données personnelles nécessaires à la gestion de ses salariés** ;
– il doit **sécuriser les données personnelles collectées** ;
– il doit **permettre aux salariés de pouvoir exercer les droits** que leur reconnaît le RGPD (information, droit d'obtenir une copie, droit de rectification, droit de suppression…).
**L'employeur peut encadrer l'utilisation des outils numériques** par les salariés dans le cadre de leur activité professionnelle, **afin de garantir la sécurité du réseau et de s'assurer que les salariés remplissent la mission pour laquelle ils ont été employés** (Ex: il peut en principe **lire tous les mails envoyés et sanctionner les connexions abusives à Internet pour des usages strictement personnels**).
**Cependant, les prérogatives de l'employeur sont limitées** par l'obligation qui lui incombe de **respecter la vie privée de ses salariés et le secret de leurs correspondances (**interdiction de lire un **mail explicitement déclaré privé,** de collecter des informations issues d'un **compte bloqué sur un réseau social**).