

## Données à caractère personnel

La France est précurseur. **Loi du 6 janvier 1978 : loi informatique et liberté**, données qui sont issus d'un traitement informatique mais également de traitements papier des données. *Exemple* : un questionnaire papier dans la rue, demander le nom, le prénom ou l'adresse ; ces données rentrent dans la cadre de cette loi.

Cette loi s'applique toujours à l'heure d'aujourd'hui mais on rajoute à cela le **Règlement Général sur la Protection des Données (RGPD)**, 27 avril 2016 qui est entrée en vigueur le 25 mai 2018. Le RGPD est un texte de loi Européen. La France a « vendu » la loi de 1978 à l'Union Européenne pour créer le RGPD. Dès qu'un pays souhaite vendre ou proposer un service à la France le RGPD s'applique sur l'application, le service proposé par ce pays.

En France la loi de 1978 et le RGPD s'appliquent en même temps.

### Notion de données à caractère personnel

On retrouve cette notion à l'article 4 du RGPD. Toute information qui va permettre d'identifier une personne physique. Les personnes morales (les sociétés et les entreprises) ne sont pas protégées par le RGPD.

*Exemple de données à caractère personnel :*

- Numéro de téléphone
- Adresse électronique
- Géolocalisation
- Numéro de sécurité social
- Etat civile : prénom, nom...
- Adresse IP
- Un avatar
- Un pseudonyme
- Son image
- Biométrie, santé
- La voix
- ...

## Collecte

Différents principes :

### 1- Article 5 du RGPD :

- a. Collecte loyale : l'utilisateur doit être informé quand on collecte ses données.
- b. Transparente : l'utilisateur doit savoir lesquelles de ses données sont collectées.
- c. Finalité déterminée : l'utilisateur doit savoir pour quelle raison les données sont collectées et quel est l'usage qui en sera fait. Une fois que la finalité est atteinte les données doivent être anonymisées ou supprimées.

Les données sensibles par principe ne peuvent pas être collectées (génétique, origine ethnique, biométrie, croyance, orientation sexuelle).

### 2- Article 6 du RGPD : collecte des données, 6 piliers :

- a. Consentement : *exemple* : cocher une case.
- b. La donnée est nécessaire à l'exécution du contrat : le responsable du traitement collecte automatiquement la donnée donc il ne demande pas l'autorisation.

*Exemple* : collection de l'adresse IP de l'utilisateur lorsqu'il visionne une vidéo sur Netflix par exemple.

- c. La collecte est imposée par la loi : les fournisseurs d'accès à l'internet doivent garder les traces de connexions à leurs abonnés. L'ARCOM travaillent régulièrement avec les fournisseurs d'accès pour vérifier les téléchargements illégaux, etc.
- d. La collecte est nécessaire pour les intérêts vitaux de la personne.
- e. La collecte est nécessaire pour une mission d'intérêt public : *exemple* : vidéosurveillance.
- f. La collecte est justifiée par l'intérêt légitime du responsable du traitement : passoire du RGPD. L'intérêt légitime doit être loyale, l'intérêt de la collecte doit être donné à l'utilisateur. *Exemple* : une copropriété voulait mettre en place un système de vidéosurveillance. Pour imposer la vidéosurveillance ils l'ont imposé grâce à l'argument de l'intérêt légitime pour la sécurité des habitants.

## Droits

### Article 13 et suivant du RGPD

- 1- Droit à l'information : une information sur :
  - a. L'existence de la collecte
  - b. La nature des données collectées
  - c. La finalité
  - d. L'identité du responsable de la collecte
- 2- Droit de rectification : la personne dont les données sont collectées peut demander que les données soient corrigées ou mise à jour.
- 3- Droit d'effacement des données : retire le consentement ou quand la finalité est atteinte. Un des problèmes est la notion de mort numérique. En effet, quand une personne décède est ce que son compte de réseau social doit continuer à exister ? Grâce au principe de la mort numérique il est possible de désigner une personne qui aura les droits sur les comptes de l'utilisateur s'il advenait à décéder. Si l'utilisateur n'explicite pas de personnes le compte revient aux héritiers.  
(Droit à l'oubli : était présent avant le droit à l'effacement des données. Demande de déréférencer une page où son nom apparaît.)
- 4- Portabilité : la personne peut demander au responsable qu'il lui remette l'intégralité de ses données dans un format inter opérable.

Pour exercer l'ensemble de ces droits on s'adresse au **délégué à la protection des données DPO**. Tout responsable de traitement doit avoir désigné obligatoirement un DPO. Le DPO surveille en local.

## CNIL (Commission Nationale de l'Informatique et des Libertés)

La CNIL existe depuis la loi de 1978. La CNIL est une autorité administrative indépendante. Cela signifie que les membres sont désignés par l'état, que la CNIL est financée par l'état mais elle ne reçoit aucune directive de l'état officiellement. La CNIL surveille et sanctionne. Dans la passé la CNIL avait également la casquette de DPO, ce qui n'est plus le cas. La CNIL a différentes missions :

- 1- Mission d'information et de protection des citoyens
- 2- Mission de conseils et de conformité : s'adresse au responsable de traitement.
- 3- Mission d'anticipation : aspect recherche, l'ACNIL essaye d'identifier les nouveaux problèmes causés par les nouvelles technologies. *Exemple* : drones, voitures autonomes...
- 4- Missions de contrôle et de sanctions :

- a. **Sanctions de conformité** : *Exemple* : Pokémon GO quand les données étaient envoyées aux Etats Unis, ils ont dû arrêter les flux.
- b. **Amende** : le plafond est de 20 millions d'euros. Quand on est une entreprise, l'amende peut aller jusqu'à 4% du chiffre d'affaires annuel mondial.

Il existe un outil, CFVR, Ciblage de la Fraude et Valorisation des Requêtes, qui est en application depuis 2020 et en expérimentation jusqu'en 2023. La CNIL à la fin du test vérifiera l'efficacité du dispositif CFVR. Le CFVR est au service des services de Police, des imports et des douanes pour analyser toutes les informations publiques sur internet. Cela permet de vérifier la conformité des informations déclarées par les citoyens. *Exemple* : piscine non déclarée.

## Droits d'auteur

### Notion d'œuvre

L'œuvre est un effort intellectuel conscient et qui manifeste la personnalité de l'auteur. Ce qui fait une œuvre et qu'elle va être rattachable à la personne de qui elle émane. Le lien entre la personne et l'œuvre est très important. Il n'y a pas besoin de déclaration, il suffit d'être diffusé.

- **Droits patrimoniaux** : **protègent les intérêts économiques de l'auteur.**
  - o **Droit de représentation** : A chaque fois qu'il y a des représentations comme celles qui suivent il y a des droits d'auteur.
    - Représentation en direct de l'œuvre, *exemple* : théâtre, concert...
    - Représentation indirect, *exemple* cinéma, télévision...
  - o **Droit de reproduction** : il s'agit de toutes les fixations de l'œuvre sur un support physique ou dématérialisé. A chaque fois qu'un support est venu l'auteur perçoit des droits.

Les droits patrimoniaux sont :

- o **Cessibles** à un tiers.
- o **Dure toute la vie de l'auteur et jusqu'à 70 ans après son décès.**
- **Droits moraux** : **protègent le lien entre l'œuvre et son auteur.**
  - o **Droit de divulgation** : l'auteur choisi par quel moyen son œuvre va être diffusé. Action de **divulguer** au public une œuvre.
  - o **Droit de paternité** : seul l'auteur peut apposer son nom sur l'œuvre. Par mesure de précaution si un utilisateur souhaite protéger son œuvre Il faut qu'il adresse sa création à une personne de confiance sous pli cédé et daté, qu'il ne faut ouvrir. L'auteur peut rester anonyme ou utiliser un pseudo. *Exemple* : Alan Smithee quand les réalisateurs ne veulent pas être associé à leur œuvre.
  - o **Droit au respect de l'intégrité de l'œuvre** : seul le titulaire des droits à la possibilité de modifier son œuvre.
  - o **Droits de retraits de repentir** : permet à l'auteur de demander après la diffusion de l'œuvre sa modification ou son retrait de la diffusion. L'œuvre est dans ce cas **déjà en circulation** et l'auteur souhaite la **modifier** (repentir) ou la **retirer** (retrait).

Les droits moraux ont 4 caractères :

- o **Droit personnel** : le droit ne peut pas se détacher de la personne. Le droit ne peut pas être soustrait. *Exemple* : droit à l'image, droit à l'intégrité de son corps...
- o **Droit perpétuel** : droit qui n'a aucun terme (pas de date limite).
- o **Droit incessible** : on ne peut pas céder les droits moraux.
- o **Droit imprescriptible** : si une personne porte atteinte aux droits moraux l'auteur pourra toujours agir. Pas de délai d'extinction.

Les caricatures et les satires sont toujours autorisées sauf si l'objectif est de nuire à l'œuvre.

## Logiciel

Brevet ou droit d'auteur ? Les brevets nécessitent une déclaration d'une validité de 20 ans.

Il a été décidé que les logiciels étaient protégés par les droits d'auteur.

Il y a eu des contestations car il n'est pas forcément possible de retrouver le lien entre l'auteur et son œuvre, son logiciel. En effet, il n'y a pas d'émanation de sa personnalité.

Le logiciel va être protégé si son concepteur a produit un effort intellectuel pour **surpasser des contraintes techniques**.

Voici ce qui est protégé :

- Le logiciel en lui-même
- Son mode d'emploi
- Son code source
- Son code exécutable
- Les travaux de conception

Ce qui n'est pas protégé :

- Le langage de programmation
- Le cahier des charges
- Les fonctionnalités mais leur arrangement. *Exemple* : logiciel de traitement de texte, en fonction des logiciels les fonctionnalités sont les mêmes mais leur arrangement est différent.

## Titulaire des droits

Le titulaire est généralement son auteur mais il existe des exceptions :

- Le logiciel est conçu à plusieurs
  - **Collaboration** : partage équitable : co-auteurs.
  - **Collective** : une personne pilote : cette personne est alors l'autrice.
- Le logiciel peut être cédé
- Auteur salarié : les droits sur le logiciel appartiennent à l'employeur.

## Les différents droits

(Différences avec les droits d'auteur « normaux »)

- Droits patrimoniaux :
  - Droit de reproduction : mettre l'œuvre sur un support
    - Fixation définitive sur le support (CD, USB...)
    - **Fixation temporaire** (nombre d'installation)
  - **Droit de mise sur le marché** : le titulaire des droits décide de la distribution du logiciel. Cependant une fois que le logiciel est en circulation le titulaire perd toutes ses prérogatives patrimoniales sur le logiciel. **Théorie de l'épuisement des droits.** *Exemple* : dès que quelqu'un achète son logiciel l'auteur n'a plus les droits. Cela vise les logiciels sur support physique et les logiciels dématérialisés. *Exemple* : l'utilisateur peut revendre en légalité des clefs d'activation de logiciel, s'il ne l'utilise plus lui-même. L'épuisement des droits fonctionnent sur tout support physique. Cela est le cas puisque le support se dégrade. *Exemple* : livre...  
En ce qui concerne les œuvres dématérialisées on n'applique pas l'épuisement des droits. Il est interdit de revendre une œuvre dématérialisée.
- Droits moraux :
  - Divulgateion

- Paternité
- Droit de modification / droit au respect de l'œuvre qui continue à s'appliquer à l'exception de deux cas :
  - Les droits patrimoniaux ont été cédés à un tiers. Ce tiers peut alors modifier le logiciel sauf si cela porte atteinte à la réputation de l'auteur d'origine.
  - L'utilisateur du logiciel peut procéder à sa décompilation en vue d'en corriger les erreurs.
- Le droit de retrait et de repentir **ne s'applique pas en matière de logiciel**.

## Responsabilité des prestataires techniques

### Droit Européen

Directive 2000/31 du 8 juin 2000, droit européen. Il existe 3 types de prestataires techniques :

- **Simple transport** : fournisseur d'accès à internet et également les propriétaires des infrastructures de communication.
- **Prestataire de caching** : prestataires qui offrent un stockage temporaire des informations. Stockage en cache. *Exemple* : les moteurs de recherche comme Google.
- **Prestataire d'hébergement** : proposent un stockage permanent des données/des informations à la demande de leurs utilisateurs.

Ces différents prestataires :

- N'ont pas l'obligation de la surveillance des contenus
- Pas de responsabilité du fait des contenus

### Droit français

Loi LCEN, loi pour la confiance dans l'économie numérique, du 21 juin 2004.

Le caching n'est pas prévu en droit français, mais nouvelle catégorie : les éditeurs.

- **Les FAI** : les fournisseurs d'accès à internet. Ici on ne s'occupe pas des propriétaires des infrastructures. Les FAI ont deux grandes obligations :
  - **La mise en place de mesures de filtrage** : ces mesures peuvent être demandées par :
    - Le juge
    - L'autorité administrative, par les ministères : en cas de terrorisme ou de pédopornographie

Les premiers sites interdits sont les sites de jeux et paris. Aujourd'hui les juges doivent trouver une balance entre la liberté d'expression et la contrefaçon.

Les FAI sont dans l'obligation de mettre en place un filtrage fonctionnel, sinon le FAI sera responsable. Le FAI doit supporter le coût de cette mesure de filtrage mais il pourra se retourner contre le site internet bloqué. Mais régulièrement le propriétaire des sites ne sont généralement pas retrouvés.
  - Les FAI ont l'obligation de la **conservation des traces de connexion pendant 1 an** glissant. Ils sont obligés de remettre ces traces de connexion aux autorités compétentes qui les demandent. Le conseil constitutionnel affirme que la France n'est pas dans le respect des droits européens.
- **Les prestataires d'hébergement** : stockage permanent. L'hébergeur est passif envers le contenu.
  - Ils n'ont pas d'obligation de surveillance des contenus sauvegardés
  - Responsabilité à postériori. Pour qu'il soit responsable il y a deux conditions :
    - Notification d'un contenu illicite, *exemple* : contrefaçon

- Après notification le contenu doit être bloqué ou retiré dans un prompt délai.  
Le délai moyen est de 24h à 48h.
- Depuis le 1<sup>er</sup> janvier 2022, dans une situation de contrefaçon. On retrouve en plus des deux conditions précédentes :
  - L'auteur demande un filtrage de ses contenus. *Exemple* : un réalisateur peut demander avant la sortie de son film qu'aucun contenu en lien avec ce film soit disponible sur la plateforme de l'hébergeur en question.
  - L'hébergeur doit avoir obtenu les droits de tous les contenus hébergés.
- **Les éditeurs** : créateur de contenu. L'éditeur joue un rôle actif sur le contenu. *Exemple* : les blogs, un site web...
  - Obligation d'information : envers tout le monde
    - Sur leur identité
    - Sur leurs coordonnées (donner un moyen d'entrée en contact)
  - Droit de réponse : une personne qui est visé par un contenu a le droit de faire publier une réponse sur le site de l'éditeur. *Exemple* : si une personne est visée par une vidéo d'un créateur de contenu, cette personne peut demander à YouTube de répondre par une vidéo à la première vidéo. La réponse doit être proportionnée au propos qui visaient la personne.
  - Les éditeurs sont responsables de leur contenu

La loi DSA en février 2024 va mettre plus de responsabilité sur les hébergeurs.

*Exemples :*

<i>Hébergeur</i>	<i>Editeur</i>
<ul style="list-style-type: none"> <li>- Drop box</li> <li>- YouTube</li> <li>- Dailymotion</li> <li>- Site commerçant où les clients peuvent donner leur avis</li> </ul>	<ul style="list-style-type: none"> <li>- Ebay est considéré comme éditeur puisqu'il est actif dans la vente.</li> <li>- Le Bon Coin</li> <li>- Vinted</li> <li>- Site de streaming</li> <li>- Un journal qui héberge ses propres articles et demande l'application du droit Européen, puisqu'il n'y a pas le statu d'éditeur.</li> </ul>

## La cybercriminalité

La cybercriminalité prend place dans un monde numérique. Les outils numériques sont les moyens de commettre les infractions ou ils en sont la cible. La cybercriminalité laisse peut de trace puisque ces traces peuvent être modifiées ou effacées. Leur but est d'agir le plus rapidement possible.

Les technologies numériques sont un moyen d'appréhension des cybercriminels :

- Vidéosurveillance avec reconnaissance facile. Question sur la réglementation pour le respect de la vie privée. Ces caméras sont contrôlées par le service de cybercriminalité même si elles sont utilisées pour des agressions et délits non « cyber ».
- Identification par des paiements par carte bancaire
- Triangularisations GSM : beaucoup moins précis qu'un signal GPS.
- Analyse des matériels numériques, méthode de Forensic : il faut faire une copie du matériel pour démontrer des choses.

- La règle de collaboration des clefs de cryptages. *Exemple* : une personne était accusée d'action terroristes. Le FBI a fait un bras de fer avec Apple pour récupérer les clefs de cryptages. Un tier « aurait » trouvé la clef de cryptage. Aujourd'hui l'utilisateur est dans l'obligation de remettre les clefs de cryptages.
- Vente de produits illicites ou réglementés
- Utilisation des réseaux sociaux et messageries instantanées. *Exemple* : Télégramme qui était un réseau crypté utilisé pour les attentats.
- Pédopornographie : les méthodes sont :
  - o Se faire passer pour un enfant et de se rendre sur des sites. Ils ne peuvent pas inciter à l'infraction (sinon vice de procédure), la personne soupçonnée doit faire la demande de la rencontre.
  - o Générer la photo d'un enfant (non réel) avec un traceur pour récupérer les traces de connexions.

### Les technologies numériques pour de nouvelles infractions

- Cartes à puces contrefaites
- Skimmers : scanner de cartes et clavier superposé au vrai clavier, vrai scanner.
- Phishing
- Ransomware

### Les textes applicables

#### France

- Loi française de 1978, loi informatique et liberté
- Loi LCEN
- Loi LOPPSI 2, 14 mars 2011 : protection de l'identité numérique ainsi que des nouvelles infractions liées aux systèmes informatiques.

#### Europe

- Convention sur la cybercriminalité, 23 novembre 2001 : définit plusieurs infractions de cybercriminalité pour l'Union Européenne. Même définition partout en Europe. Permet la coopération.

#### International

- Convention de Budapest, 23 novembre 2011, qui définit les caractéristiques de la cybercriminalité. Très général.

### Autorités compétentes

#### France

- Services de police (répression)
- Services de gendarmerie (répression + recherches)

#### UE et international

- Interpol : permet à tous les services de police de rentrer en contact et de s'organiser. rapidement. 194 états membres, disponibilité des agents 24h/24, 7j/7.
- Europol : présente beaucoup de fonctions identiques à Interpol mais au niveau européen.
- Réseau G8, 24/7 : créé après les attentats de 2001. A un instant t peut geler toutes les données numériques d'un état membre. Les preuves ne peuvent donc pas disparaître.

### Que font ils

Ils récupèrent des preuves dans des réseaux fermés :

- Les FAI
- Les opérateurs de téléphonie
- Les hébergeurs de données

Ils utilisent les réseaux ouverts :

- Toutes les informations qui circulent sur internet

Face à ces informations :

- 1- Le site internet est-il l'hébergeur ou l'éditeur des informations ?
- 2- Quel est l'identité de l'auteur ? Vraie photo ? Vraie identité ?
- 3- Quelle est la nature de l'information ?
  - a. On vérifie et on regarde la date de l'information.
  - b. On vérifie la nature de site internet
  - c. Est-ce que l'information a été mise à jour ?