Partie 1 - QUEL TEXTE REGLEMENTAIRE PROTEGE LA CONFIDENTIALITE DES DONNEES DES CITOYENS ?

Le **Règlement Général sur la Protection des Données (RGPD)** est une **directive européenne** qui a pour but de fixer les conditions dans lesquelles sont collectées, conservées et exploitées des données à caractère personnel au sein de l'Union européenne. Il a été adopté en 2016 et trouve son application en France depuis 2018.
Son but est de protéger la vie privée.

Il s'applique :

- au traitement des données à caractère personnel pour des activités d'un établissement de l'Union Européenne (que le traitement ait lieu ou non dans l'Union ;
- au traitement des données à caractère personnel de personnes se trouvant sur le territoire de l'Union même si l'établissement n'est pas dans l'Union ;
- au traitement des données à caractère personnel pour des activités d'un établissement régi par le droit RGPD.

Les droits du Règlement général sur la protection des données :

- **Droit à l'information :** Rester informé
- **Droit d'opposition :** Vous pouvez vous opposer à tout moment à ce qu'un organisme utilise vos données à des fins commerciales ou idéologiques
- **Droit d'accès :** Vous avez le **droit** de savoir quelles informations les administrations, les organismes publics ou privés et les sociétés commerciales détiennent sur vous dans leurs fichiers.
- **Droit de rectification ou modification :** Rectifier vos données personnelles
- **Droit au déréférencement** : vous avez le droit de déréférencer un contenu, c'est-à-dire ne plus associer votre nom/prénom à un contenu visible dans un moteur de recherche (photo, orientation sexuelle, …). Ce droit est valable sur tout le territoire de l'Union Européenne et partout où la norme RGPD est appliquée. Par exemple, on peut sortir de google.pt (Portugal) ou de google.be (Belgique)
- **Droit à la portabilité :** Possibilité de récupérer une partie de vos données dans un format lisible par une machine. Libre à vous de stocker ailleurs ces données portables ou les transmettre facilement d'un système à un autre, en vue d'une réutilisation à d'autres fins. (Par exemple une play-list)
- **Droit à l'effacement ou à l'oubli :** Effacer vos données si la conservation de celles-ci n'est plus justifiée.
- **Droit lié au profilage :** Le profilage est une technique de traitement automatisé des données personnelles. Elle permet notamment l'analyse et la prédiction de comportements, de performances, etc. Lorsque le profilage est lié à une prise de décision, les personnes physiques peuvent s'y opposer.
  L'article 22 du RGPD énumère **trois situations** dans lesquelles le profilage engendrant une décision automatisée peut être autorisé. En effet, cela est possible dans les cas où la décision est :
  - **nécessaire à l'exécution ou à la conclusion d'un contrat** entre la personne concernée et le responsable du traitement des données ;
  - **autorisée par le droit de l'Union Européenne ou le droit national ;**
  - fondée sur le consentement explicite de la personne.
- **Droit d'accès FICOBA :** Le FICOBA sert à recenser les comptes de toute nature (bancaires, postaux, d'épargne, etc.) et à fournir aux personnes habilitées des informations sur les comptes détenus par une personne ou une société. Selon votre situation, vous pouvez bénéficier d'un droit d'accès à ce fichier si :
  - Vous êtes titulaire du compte.
  - Vous êtes un héritier.
  - Vous êtes un professionnel agissant pour le compte d'un particulier.
  - Vous êtes un tiers autorisé.
- **Droit d'accès au fichier de la police/gendarmerie :**

Partie 2 - GUIDE DES AUTORISATIONS DES APPLICATIONS D'ANDROID

Les autorisations système peuvent être divisées en deux groupes : les normales et les autorisations à risque. Les groupes des autorisations normales sont autorisés par défaut, parce qu'ils ne posent pas de risque pour votre confidentialité. (Par exemple, Android permet aux applications d'accéder à Internet sans votre permission). Les groupes des autorisations à risque, cependant, peuvent donner aux applications l'accès à des éléments comme l'historique des appels, les messages privés, l'emplacement, l'appareil photo, le microphone, et plus encore. Par conséquent, Android vous demandera toujours d'approuver les autorisations à risque.

Autorisations potentiellement à risque à surveiller
Toute personne soucieuse de la protection de sa vie privée et de sa sécurité devrait surveiller les applications qui demandent l'accès aux neuf groupes d'autorisations suivants. Chaque groupe contient plusieurs autorisations et l'approbation d'une seule autorisation de n'importe quel groupe approuve automatiquement toutes les autres autorisations au sein de ce même groupe. (Par exemple, si vous autorisez une application à voir qui vous appelle, vous lui permettrez aussi de passer des appels téléphoniques.)

- **Capteurs corporels**
  Autorise l'accès à vos données de santé à partir des cardio fréquence mètres, de trackers de fitness et d'autres capteurs externes.
  Avantage : les applications de fitness ont besoin de cette autorisation pour surveiller votre fréquence cardiaque pendant que vous faites de l'exercice, fournir des conseils de santé, etc.
  Inconvénient : une application malveillante pourrait espionner votre santé.

- **Calendrier**
  Permet aux applications de lire, créer, modifier ou supprimer les événements de votre calendrier.
  Avantage : les applications de calendrier ont évidemment besoin de cette autorisation pour créer des événements de calendrier, mais il en va de même pour les applications de réseautage social qui vous permettent d'ajouter des événements et des invitations à votre calendrier.
  Inconvénient : une application malveillante peut espionner vos routines personnelles, l'heure des réunions, etc. et même les supprimer de votre calendrier.

- **Appareil photo**
  Permet aux applications d'utiliser votre appareil photo pour prendre des photos et enregistrer des vidéos.
  Avantage : les applications de photographie ont besoin de cette autorisation pour que vous puissiez prendre des photos.
  Inconvénient : une application malveillante peut secrètement allumer votre appareil photo et enregistrer ce qui se passe autour de vous.

- **Contacts**
  Permet aux applications de lire, créer ou modifier votre liste de contacts, ainsi que d'accéder à la liste de tous les comptes (Facebook, Instagram, Twitter, etc.) utilisés sur votre appareil.
  Avantage : une application de communication peut l'utiliser pour vous permettre d'envoyer des SMS ou d'appeler d'autres personnes de votre liste de contacts.
  Inconvénient : une application malveillante peut voler tout le contenu de votre carnet d'adresses, puis cibler vos amis et votre famille avec du spam, des arnaques par hameçonnage, etc.

- **Emplacement**
  Permet aux applications d'accéder à votre position approximative (à l'aide de stations de base cellulaires et de points d'accès Wi-Fi) et à votre position exacte (à l'aide du GPS).

Avantage : les applications de navigation peuvent vous aider à vous déplacer, les applications de photographie peuvent géolocaliser vos photos pour que vous sachiez où elles ont été prises et les applications de shopping peuvent estimer votre adresse de livraison.
Inconvénient : une application malveillante peut secrètement suivre votre position pour établir un profil sur vos habitudes quotidiennes ou même faire savoir aux voleurs quand vous n'êtes pas chez vous.

- **Microphone**
  Permet aux applications d'utiliser votre microphone pour enregistrer du son.
  Avantage : une application de reconnaissance musicale comme Shazam l'utilise pour écouter n'importe quelle musique que vous voulez identifier ; une application de communication peut l'utiliser pour vous permettre d'envoyer des messages vocaux à vos amis.
  Inconvénient : une application malveillante peut enregistrer secrètement ce qui se passe autour de vous, y compris les conversations privées avec votre famille, les conversations avec votre médecin et les réunions d'affaires confidentielles.

- **Téléphone**
  Permet aux applications de connaître votre numéro de téléphone, les informations actuelles sur le réseau cellulaire et l'état des appels en cours. Les applications peuvent également passer et terminer des appels, voir qui vous appelle, lire et modifier vos journaux d'appels, ajouter des messages vocaux, utiliser la VoIP et même rediriger les appels vers d'autres numéros.
  Avantage : les applications de communication peuvent l'utiliser pour vous permettre d'appeler vos amis.
  Inconvénient : une application malveillante peut espionner vos habitudes téléphoniques et passer des appels sans votre consentement (y compris des appels payants).

- **SMS**
  Permet aux applications de lire, recevoir et envoyer des messages SMS, ainsi que de recevoir des messages WAP push et MMS.
  Avantage : les applications de communication peuvent l'utiliser pour vous permettre d'envoyer des messages à vos amis.
  Inconvénient : une application malveillante peut espionner vos messages, utiliser votre téléphone pour spammer d'autres personnes et même vous abonner à des services payants non désirés.

- **Stockage**
  Permet aux applications de lire et d'écrire sur votre stockage interne ou externe.
  Avantage : une application musicale peut enregistrer les chansons téléchargées sur votre carte SD ou une application de réseautage social peut enregistrer les photos de vos amis sur votre téléphone.
  Inconvénient : une application malveillante peut secrètement lire, modifier et supprimer n'importe lequel de vos documents, musiques, photos et autres fichiers enregistrés.

Partie 3 - INTERNET ET DONNEES PERSONNELLES

Les sites Web auxquels vous vous connectez peuvent avoir accès à :

- Votre adresse IP
- Votre nom d'hôte (hostname) ainsi que le nom de votre fournisseur d'accès
- Votre système d'exploitation
- la page qui vous a conduit jusqu'à lui (c'est-à-dire le navigateur utilisé)
- la résolution de votre écran
- Ils peuvent avec votre autorisation déposer des cookies

Cnil protection des données dans le monde : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

1. Qu'est-ce qu'un cookie ?

Un cookie est un fichier qui est déposé par le navigateur sur votre ordinateur lorsque vous surfez sur internet.

- Il est stocké sur le disque dur de l'internaute.
- Il est déposé par un site Web lors de la consultation d'une de ses pages
- Il permet à un internaute de naviguer entre les différentes pages d'un site en restant identifié.
- Il permet aux sites de vente en ligne de pouvoir conserver le panier d'achat de l'internaute.
- Il retrace votre historique de navigation.
- Il permet aux annonceurs de proposer de la publicité ciblée.

Comment s'en prémunir ? La navigation privée ?

Les sites Web peuvent garder la trace de votre navigation en déposant des cookies. La navigation privée est un mode spécial de navigation proposé par son navigateur qui permet de naviguer sur le web avec plus de confidentialité. En effet, certaines données de navigation ne sont pas conservées comme :

- l'historique de navigation
- le cache navigateur
- les fichiers temporaires comme les cookies de votre navigateur
- les téléchargements
- le remplissage automatique des formulaires
- les mots de passe enregistrés dans votre navigateur (saviez-vous au passage qu'il était possible de récupérer un mot de passe enregistré dans votre navigateur ?)

2. Comment les emails sont-ils suivis ?

En théorie, le courrier électronique est un support de communication très simple. Mais en réalité, vous n'envoyez pas seulement un message texte à quelqu'un – les emails peuvent contenir du code HTML, comme sur les pages web. Ils peuvent également charger des images, c'est ainsi que fonctionne le suivi.
Lorsque vous ouvrez un email, votre client de messagerie charge les images présentes dans cet email depuis le serveur distant et les affiche, de la même manière que lorsque vous ouvrez une page web. Vous pouvez spécifier à votre client de messagerie de **ne jamais charger d'images** si vous le souhaitez, mais en général, il les charge par défaut.
Les entreprises qui envoient des newsletters par email ou d'autres emails automatisés incluent presque toujours une image de suivi spécifique. Il s'agit d'un minuscule fichier image invisible qui ne mesure qu'un seul pixel, aussi appelé **pixel invisible** ou **pixel espion**. Chaque destinataire de la newsletter se voit attribuer un code de suivi unique au sein de cette image. Ces images sont aussi connues sous le nom de " balises web ".
Lorsque vous ouvrez la newsletter, et qu'elle charge des images (même si vous ne pouvez pas les voir), elle charge donc également une balise web. Lorsque cette image spécifique est chargée à partir des serveurs de l'entreprise ou d'un service tiers, l'expéditeur peut dès lors savoir que l'email envoyé à votre adresse vient d'être ouvert.