Corantin GENTY
Morgane DENIS
Rafaël BRANGER

Séance ⅔ - Données personnelles

Question 1:

1. Le traitement de données dans le domaine de la santé connectée

- **Collecte des données:** Les montres connectées et les applications de suivi d'activité physique collectent un grand nombre de données personnelles : fréquence cardiaque, qualité du sommeil, nombre de pas, etc.
- **Traitement des données:** Ces données sont ensuite traitées par des algorithmes pour générer des rapports personnalisés sur la santé de l'utilisateur, des tendances et des recommandations.
- **Finalités:** Ces informations sont utilisées pour suivre l'évolution de la forme physique, détecter d'éventuels problèmes de santé et personnaliser les programmes d'entraînement.

2. Le traitement de données dans le secteur de la publicité en ligne

- **Collecte des données:** Les sites web et les applications mobiles collectent de nombreuses données sur nos comportements en ligne : sites visités, produits recherchés, publicités cliquées, etc.
- **Traitement des données:** Ces données sont analysées pour créer des profils d'utilisateurs très détaillés. Ces profils sont ensuite utilisés pour cibler les publicités de manière personnalisée.
- **Finalités:** L'objectif est de proposer des publicités pertinentes aux utilisateurs, en fonction de leurs centres d'intérêt et de leurs habitudes de consommation.

3. Le traitement de données dans le cadre de l'intelligence artificielle

- **Collecte des données:** Les assistants vocaux comme Siri ou Alexa collectent un grand nombre de données vocales pour améliorer leurs capacités de compréhension et de réponse.
- **Traitement des données:** Ces données vocales sont analysées pour entraîner les modèles d'apprentissage automatique. Ces modèles permettent aux assistants de mieux comprendre les requêtes des utilisateurs et de fournir des réponses plus pertinentes.
- **Finalités:** L'objectif est d'améliorer continuellement les performances des assistants vocaux et de rendre leur utilisation plus naturelle et intuitive.

Question 2 :

Les entreprises:

- **Grandes entreprises:** Les GAFA (Google, Apple, Facebook, Amazon) sont des exemples emblématiques de sociétés qui collectent et exploitent d'énormes quantités de données personnelles.
- **PME et TPE:** Même les plus petites entreprises sont concernées, qu'il s'agisse de gérer des données clients, des données de prospection ou des données de leurs employés.

Les administrations publiques:

- **Services fiscaux:** Ils collectent et traitent des données fiscales de chaque citoyen.
- **Services sociaux:** Ils gèrent des données personnelles dans le cadre de l'attribution de prestations sociales.
- **Hôpitaux et établissements de santé:** Ils traitent des données médicales de leurs patients.

Les associations:

- **Associations sportives:** Elles collectent des données sur leurs membres pour organiser des activités.
- **Associations caritatives:** Elles gèrent des données de donateurs.

Les prestataires de services:

- **Hébergeurs de sites web:** Ils stockent les données des utilisateurs de leurs clients.
- **Sociétés de conseil:** Elles peuvent traiter des données personnelles dans le cadre de leurs missions.

Les particuliers:

- **Créateurs de sites web:** Même un particulier qui crée un blog peut être considéré comme responsable de traitement.
- **Organisateurs d'événements:** Ils collectent des données des participants.

<u>Question 3 :</u>

Explication

1. **Consentement renforcé** :
    - **Nature explicite** : Le consentement doit être donné de manière claire et explicite, et ne peut pas être implicite ou sous-entendu. Cela signifie que les individus doivent être pleinement informés de ce à quoi ils consentent.
    - **Facilité de retrait** : Les personnes doivent avoir la possibilité de retirer leur consentement à tout moment, ce qui renforce leur contrôle sur leurs données personnelles.
2. **Transparence** :
    - **Information claire** : Les entreprises et organisations doivent fournir des informations claires et compréhensibles sur la manière dont les données personnelles sont collectées,

utilisées et stockées. Cela inclut des détails sur les finalités du traitement et les droits des personnes concernées.
    - **Accès à l'information** : Les individus ont le droit d'accéder à leurs données, de savoir comment elles sont traitées et d'être informés de tout incident de sécurité qui pourrait affecter leurs informations personnelles.

Question 4 :

- Droit à la portabilité des données :
  Le droit à la portabilité des données permet aux utilisateurs de récupérer et de transférer leurs données personnelles d'un service à un autre, de manière lisible et exploitable. Ce droit s'applique aux données fournies par la personne concernée, dans un format structuré, couramment utilisé et lisible par machine, lorsqu'elles ont été collectées avec son consentement ou dans le cadre d'un contrat.
  Exemple : Un utilisateur d'un réseau social comme Facebook peut demander à récupérer l'ensemble de ses photos, vidéos, et messages sous un format lisible (fichier ZIP ou CSV) et les transférer vers un autre service, comme une nouvelle plateforme de réseau social ou un site de stockage en ligne comme Google Drive.

- Droit à l'oubli :
  Le droit à l'oubli permet à un utilisateur de demander la suppression de ses données personnelles lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées, ou si la personne retire son consentement. Ce droit est limité par certaines obligations légales qui pourraient obliger l'organisme à conserver les données (par exemple, des raisons de sécurité ou des obligations légales).
  Exemple : Une personne peut demander à Google de retirer des liens contenant des informations personnelles la concernant (comme un vieux compte de blog ou un article d'actualité daté) si ces informations ne sont plus pertinentes ou peuvent lui causer un préjudice. Cependant, Google peut refuser cette demande si

l'information relève de l'intérêt public, comme une condamnation légale toujours en vigueur.

- Droit à notification :
  En cas de violation des données personnelles (par exemple, une fuite ou un piratage), le responsable du traitement des données a l'obligation de notifier la personne concernée. Cette notification doit inclure les détails de la violation, ses conséquences probables, et les mesures prises pour remédier à la situation. Cela permet à l'utilisateur d'agir rapidement pour protéger ses informations.
  Exemple : En 2017, la société Equifax, spécialisée dans les crédits, a subi un piratage massif de données personnelles (noms, numéros de sécurité sociale, etc.). Equifax avait l'obligation d'informer les utilisateurs concernés, ce qui leur a permis de surveiller leur crédit pour éviter des fraudes.

- Droit à réparation du dommage matériel ou moral :
  En cas de violation de la législation sur la protection des données personnelles, toute personne victime d'un dommage matériel (par exemple, une perte financière) ou moral (par exemple, un préjudice lié à une atteinte à la vie privée) a le droit de demander réparation. Cette réparation peut être accordée soit par le responsable du traitement, soit par un tribunal compétent.
  Exemple : Si une banque subit une violation de données compromettant des informations financières personnelles, et que cette violation entraîne des fraudes bancaires sur les comptes des clients, les utilisateurs concernés peuvent demander une compensation pour les pertes financières subies.

- Action de groupe :
  L'action de groupe permet à plusieurs personnes dont les droits ont été violés de se regrouper pour exercer une action collective contre un responsable de traitement. Cette mesure vise à simplifier et à renforcer la protection des droits des utilisateurs en leur permettant de se regrouper pour obtenir réparation.

Exemple : En 2020, un groupe d'utilisateurs européens a lancé une action de groupe contre Facebook, affirmant que l'entreprise avait abusé de leurs données personnelles à des fins publicitaires sans leur consentement. Cette action collective visait à obtenir une indemnisation pour les dommages causés à leurs droits à la vie privée.

Question 5 :

- Obligation générale de sécurité et de confidentialité
  Le responsable du traitement des données a l'obligation de garantir la sécurité et la confidentialité des données personnelles qu'il traite. Il doit mettre en place des mesures techniques et organisationnelles appropriées pour protéger les données contre tout accès non autorisé, perte, destruction ou altération. Ces mesures incluent le chiffrement, la pseudonymisation, et des protocoles de sécurité stricts.
  Exemple : Une entreprise de commerce en ligne, comme Amazon, utilise le chiffrement SSL pour sécuriser les informations de paiement des utilisateurs pendant leur transmission. De plus, elle pseudonymise certaines données clients pour garantir que même si des données sont interceptées, elles ne peuvent pas être associées directement à une personne sans informations supplémentaires.

- Obligation d'information :
  Le responsable du traitement doit informer les personnes concernées sur les modalités de traitement de leurs données (finalité du traitement, durée de conservation, destinataires, etc.). Cette information doit être claire, accessible et fournie au moment de la collecte des données. Il doit aussi informer les utilisateurs de leurs droits et des moyens pour les exercer (accès, rectification, suppression, etc.).
  Exemple : Lorsque vous créez un compte sur Spotify, l'entreprise vous informe dès le début des finalités pour lesquelles vos données seront utilisées, comme la personnalisation de vos playlists et recommandations. De plus, dans sa politique de confidentialité, elle explique clairement comment vous pouvez

accéder, rectifier ou supprimer vos données via votre compte utilisateur.

Question 6 :

- Désignation :
  Le DPO (Data Protection Officer) est désigné dans certaines organisations publiques ou privées qui traitent des données personnelles de manière significative ou sensible. La désignation du DPO est obligatoire pour les organismes publics et certaines entreprises privées qui traitent des données à grande échelle ou des données sensibles.
  Exemple : Une entreprise comme Uber, qui traite un grand nombre de données personnelles (localisation, informations de paiement, historique de trajets), est tenue de désigner un DPO pour garantir que toutes les pratiques de traitement des données sont conformes au RGPD.

- Rôles :
  Le DPO est responsable de la conformité au RGPD au sein de l'organisation. Il doit veiller à la protection des données personnelles, informer et conseiller le responsable du traitement ainsi que les employés sur leurs obligations, et coopérer avec les autorités de contrôle (comme la CNIL). Il joue également un rôle de médiateur avec les personnes concernées.
  Exemple : Dans une entreprise de télécommunications, le DPO est chargé de surveiller les traitements des données clients, tels que les historiques d'appels et de SMS. Il conseille également l'équipe de développement sur les mesures à mettre en place pour protéger ces données, par exemple en restreignant les accès à certaines catégories de données sensibles.

- Qualités et compétences requises :
  Le DPO doit avoir une expertise en matière de législation et de pratiques liées à la protection des données personnelles. Il doit

comprendre les processus de traitement des données, connaître les technologies de l'information et les pratiques de sécurité. Il doit également avoir une capacité de communication pour sensibiliser et former les employés aux bonnes pratiques en matière de protection des données.
Exemple : Un DPO travaillant pour une banque doit non seulement avoir une connaissance approfondie des réglementations comme le RGPD, mais également comprendre comment les systèmes d'information de la banque gèrent les données sensibles (comme les informations financières des clients). Il devra aussi organiser des formations pour les employés sur la sécurisation des données et la gestion des incidents de sécurité.

Question 7 :

Le registre des traitements est un document obligatoire pour toute organisation qui traite des données personnelles. Il permet de recenser et de documenter tous les traitements de données effectués par l'organisation. Ce registre est un outil essentiel pour prouver la conformité au RGPD.

- Intérêts :
  Le registre est crucial pour :
  1. Faciliter la gestion et le suivi des traitements de données.
  2. Fournir une preuve de conformité en cas de contrôle par une autorité de protection des données (comme la CNIL).
  3. Identifier les risques liés à certains traitements et ajuster les mesures de sécurité.

- Composition :
  Le registre doit inclure plusieurs informations, telles que :
  - Le nom et les coordonnées du responsable du traitement.
  - Les finalités du traitement.
  - La description des catégories de données collectées et des personnes concernées.
  - Les destinataires des données.
  - Les mesures de sécurité mises en place.

- La durée de conservation des données.
  Exemple : Un hôpital devra tenir un registre des traitements listant les données personnelles des patients, telles que les dossiers médicaux. Le registre contiendra des informations comme la finalité des traitements (soins médicaux), la durée de conservation des dossiers (10 ans après le dernier passage du patient, en France), et les mesures de sécurité (chiffrement des dossiers et accès restreint).

- Cas des entreprises de moins de 250 salariés :
  Les entreprises de moins de 250 salariés sont exemptées de tenir un registre des traitements, sauf si le traitement qu'elles effectuent présente un risque pour les droits et libertés des personnes concernées, s'il concerne des données sensibles ou s'il n'est pas occasionnel.
  Exemple : Une petite boutique en ligne avec moins de 10 employés n'a pas l'obligation de tenir un registre complet, sauf si elle traite des données sensibles (comme des informations médicales ou bancaires) ou des traitements de données récurrents, comme les abonnements à des newsletters ou des campagnes de publicité ciblées.

Question 8 :

Le RGPD prévoit une série de sanctions administratives pour non-conformité aux règles de protection des données :

1. Avertissement ou mise en demeure : L'autorité de contrôle (comme la CNIL) peut adresser un avertissement ou mettre en demeure une organisation si elle juge que des mesures correctives doivent être prises.
   Exemple : Une petite entreprise de vente en ligne, qui ne respecte pas certaines obligations d'information sur le traitement des données de ses clients, reçoit un avertissement de la CNIL. L'autorité de contrôle lui accorde un délai pour mettre à jour sa politique de confidentialité et informer correctement ses utilisateurs des finalités et durées de conservation des données.

2. Amendes administratives : Des amendes pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires pour les infractions mineures, et jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires pour les infractions graves.
Exemple : En 2021, Amazon a été condamné à une amende de 746 millions d'euros par la CNIL luxembourgeoise pour un traitement de données non conforme aux règles du consentement en matière de publicité ciblée. Ce traitement concernait des données collectées sans l'accord explicite des utilisateurs.

3. Restriction ou interdiction du traitement des données : Si un traitement présente un risque important pour les droits des personnes, une autorité peut ordonner la suspension ou l'interdiction de ce traitement.
Exemple : En 2018, une société de vidéosurveillance a reçu l'ordre de la CNIL de suspendre l'utilisation de caméras de surveillance à reconnaissance faciale dans un centre commercial. Le traitement des données était jugé trop intrusif et risquait de violer les droits des personnes, sans consentement clair et explicite.

4. Suspension ou retrait de la certification : Une certification obtenue en matière de protection des données peut être suspendue ou retirée en cas de non-conformité.
Exemple : Une entreprise de cloud computing certifiée pour la protection des données personnelles voit sa certification suspendue après qu'un audit révèle de graves failles de sécurité dans ses systèmes. L'entreprise est sommée de corriger ces failles avant que la certification puisse être rétablie.

5. Injonction de rectifier, de limiter ou de supprimer des données : L'autorité peut ordonner des corrections ou la suppression de données personnelles mal gérées.
Exemple : Un hôpital ayant conservé les dossiers médicaux de patients au-delà des délais légaux reçoit une injonction de la CNIL pour supprimer ces données. Il est obligé de mettre en place un

nouveau système de gestion des archives pour se conformer aux règles de conservation.

6. Publicité des sanctions : Certaines sanctions peuvent être rendues publiques, ce qui peut nuire à la réputation de l'organisation concernée.
Exemple : En 2020, la CNIL a publié une sanction contre une société immobilière qui conservait indûment des informations sur des clients potentiels, notamment des documents relatifs à leur situation financière. Cette publication a gravement terni la réputation de l'entreprise, entraînant une perte de confiance des clients.

7. Retrait du droit de transfert de données : Le transfert de données vers des pays tiers peut être suspendu en cas de non-respect des règles de protection.
Exemple : Une entreprise technologique effectuant des transferts de données vers des États-Unis sans respecter les standards européens en matière de protection des données (absence de garanties contractuelles adéquates) se voit interdire temporairement de poursuivre ces transferts jusqu'à ce qu'elle mette en place des mesures conformes au RGPD.

8. Sanctions spécifiques pour les sous-traitants : Les sous-traitants peuvent également être sanctionnés en cas de non-respect des obligations qui leur incombent.
Exemple : Une société de marketing digital, sous-traitant d'une grande entreprise, est condamnée pour avoir utilisé des données clients à des fins publicitaires sans l'accord des utilisateurs. La société sous-traitante reçoit une amende, même si elle agissait sous les ordres de l'entreprise principale, en raison de son non-respect des obligations de traitement de données.

Ces sanctions visent à garantir que les organisations respectent les obligations du RGPD et protègent les droits des personnes concernées.