Vie privée et protection des données: comment protéger la vie privée des individus dans un contexte d’utilisation croissante des données personnelles par les systèmes d’Intelligence Artificielle?

Présentateur ?

- Docteur en droit public : expert du droit du numérique Directeur des Affaires Juridiques, de la Conformité et du Contentieux à l'Autorité de Protection des Données à caractère Personnel (APDP)
- Auteur du livre:
  - Protection des données à caractère personnel en droit malien: entre affirmation et effectivité contrariée;
  - Articles et communications scientifiques.

Problématique de la présentation

L’Intelligence Artificielle (IA) est grande consommatrice **surtout** de données à caractère personnel.

Comment les Systèmes d’IA peuvent-ils se développer tout en respectant le droit au respect de la vie privée et les données à caractère personnel?

Plan de la presentation

Contexte général sur l'Intelligence Artificielle

I. Risques de l'Intelligence sur la vie privée et les données à caractère personnel

II. Mesures de protection de la vie privée et des données personnelles face à l'Intelligence Artificielle

Contexte général:
Intelligence Artificielle: de quoi parle-t-on?

- **Absence de définition consensuelle;**

- L'IA peut désigner des concepts différents, ayant différents niveaux de sophistication et employant divers procédés techniques (Option consommateurs).

- L'Intelligence Artificielle est tout système mettant en œuvre des mécanismes proches de celui d'un raisonnement humain (Commission Nationale de l'Informatique et Libertés CNIL);

- Il suffit de se pencher sur l'étymologie du terme **IA** pour s'en a percevoir:

- « **Intelligence »,** du latin « intelligere » qui signifie la faculté de comprendre;
- « **Artificielle »,** du latin « artificialis, pour désigner ce qui est dû à l'art, ce qui est fabriqué, fait de toutes pièces; ce qui imite la nature.

(Jean-Philippe Desbiolles et Grégoire Colombet (Humain ou IA qui décidera le futur?),

Ainsi, une **IA** représenterait une faculté de comprendre, fabriquée de toutes pièces.

L'IA est égale imitation des fonctions cognitives de l'humain telles que:

- **la perception;**
- **l'apprentissage;**
- **la résolution de problèmes ou la compréhension du langage.**

Contrairement aux logiciels traditionnels qui suivent des instructions explicites, les systèmes d'IA apprennent à partir de données et affinent leurs opérations au fil du temps.

Aussi, les procédés techniques utilisés pour supporter l'IA peuvent varier : **Machine learning-deep learning;**

- **Machine learning** est un procédé par lequel des algorithmes traitent **d'immenses quantités de données** et sont capables **d'apprendre de leurs propres** erreurs ou succès pour **améliorer continuellement leur efficacité**

1. **Collecte des données;**
2. **Minimisation d'erreurs;**
3. **Algorithme d'optimisation;**
4. **Construction d'un modèle.**

Deep learning ou l'apprentissage profond: Cette technologie permet d'identifier des corrélations dans les données qu'il serait difficilement possible de découvrir avec des fonctions statistiques traditionnelles.

1. **Réseau neuronal;**
2. **Puissance de calcul;**
3. **Masse exponentielle de données;**
4. **Minimisation de l'erreur entre valeur de sortie et modèle**

Deep learning ou l’apprentissage profond:

Réseau neuronal;

1. **Puissance de calcul;**
2. **Masse exponentielle de données;**
3. **Minimisation de l’erreur entre valeur de sortie et modèle**

I. Risques de l'IA pour la vie privée et les données à caractère personnel

Livre: La guerre des Intelligences Artificielles à l'heure de ChatGPT: Nous sommes les idiots utiles de l'IA « nous alimentons la machine numérique de demain, sans en avoir conscience ».

« La matière première de l'IA, c'est l'information. D'où vient-elle? De nous-mêmes, qui faisons des milliards de requêtes Google ou déposons des milliards d'images par jour sur Facebook ».

- Pour le *deep learning*, l'avalanche d'images et de données qui déferle sur le web constitue une matière première *quasi infinie* et qui se renouvelle chaque jour.

Les données abonnées par les milliards d'internautes aux grands opérateurs du numériques constituent ‘’un véritable trésor’’, leur patrimoine social, économique, émotionnel.

Que font donc, ces géants de cette fortune numérique? **Ils créent un nouveau monde, celui que nous connaissons aujourd'hui: Intelligence Artificielle avec ses risques pour la vie privée et les données à caractère personnel**

Quelques exemples de risques poses par l'IA

Les Systèmes d'Intelligence Artificielle (SIA) peuvent amplifier certains risques relatifs aux données à caractère personnel. Il s'agit :

- **de l'identité de l'interlocuteur (présence ou non de l'IA);**
- **de l'erreur (variabilité des données ou analyse erronée);**
- **de la discrimination (exclusion sur la base de traitement automatisé, profilage);**
- **de la surveillance (restriction de libertés individuelles et collectives);**
- **Cybercriminalité (usurpation d'identité, discours haineux, désinformation, vol de données);**
- **Violation de la vie privée (segmentation, personnalisation);**

Cette personnalisation est obtenue par l'analyse de grandes quantités de données personnelles afin de proposer le contenu le plus pertinent.

L'algorithme de recommandation de YouTube étonne par sa capacité à suggérer des vidéos correspondant aux centres d'intérêt de l'utilisateur (mécanismes d'IA sophistiqués)

Autres:

- **les compagnies d'assurance utilisent l'IA pour générer des devis d'assurance précis;**
- **les agences de recrutement utilisent des outils d'IA pour passer au crible les CV et les candidatures;**
- **les institutions financières traitent les données personnelles pour décider qui peut prétendre à un prêt.**

- **Même les applications de fitness sont désormais dotées de fonctions d'IA qui fournissent des informations sur:**
  - **les paramètres de santé d'un individu, et**
  - **proposent des recommandations personnalisées en matière d'entraînement et de régime.**

Ces avancées technologiques s'accompagnent d'un certain nombre de défis d’où l’intervention des lois sur la protection des données entrent en jeu.

- **Selon Ray Kurzweil-vice président de Google « une authentique d'IA dotée d'une conscience qui devrait écraser l'intelligence humaine émergera dès 2045 et sera un milliard de fois plus puissante que la réunion de réunion de tous les cerveaux humains ».**
- **Il ajoute que d'ici 2035, environ dans 15 ans, Google fournira des réponses à nos questions avant même que nous les posions.**
- **Marc Zuckerberg, le fondateur de Facebook a expliqué, le 16 juin 2016, que dans le futur les utilisateurs de Facebook échangeraient directement leurs pensées et sentiments grace aux technologies célébrales.**

II. Mesures de protection de la vie privée et des données personnelles des individus dans un contexte d'utilisation croissante des données personnelles par les systèmes d'Intelligence Artificielle?

Elon Must (celui qui a financé la recherche sur Chatbot ChatGPT) a averti que l'IA est plus dangereuse qu'une ‘'arme nucléaire'' et a donc appelé les autorités à règlementer le secteur.

Il dit « si rien n'est fait pour réguler le secteur, les choses échapperont au contrôle humain ».

II. Mesures de protection de la vie privée et des données personnelles des individus dans un contexte d'utilisation croissante des données personnelles par les systèmes d'Intelligence Artificielle?

Pour établir un équilibre entre la sécurité et le respect des droits et libertés fondamentaux dans le cadre d'une politique de protection des données personnelles, la mise en place d'un cadre juridique clair et de mécanismes de contrôle efficaces est cruciale .

Il existe plusieurs textes internationaux et nationaux qui consacrent la protection de la vie privée et des données à caractère personnel contre les dangers de l'IA.

Les normes supra nationales régissant la protection des données à caractère personnel

- Normes des organisations supranationales “à caractère international” régissant la protection des données à caractère personnel : les textes de l’ONU;
- Normes des Organisations supranationales ‘’à caractère régional’’ encadrant la protection des données à caractère personnel;
- Normes nationales

Normes nationales

- Constitution du 22 juillet 2023 notamment son article 12;
- Code pénal;
- Loi n°2013-015 du 21 mai 2013 portant protection des données à caractère personnel au Mali;
- Loi n°2016-012 du 6 mai 2016 relative aux transactions, échanges et services électroniques
- Loi n°2019-056 du 05 décembre 2019 portant répression de la cybercriminalité au Mali, entre autres.

IA et les principes de protection des données à caractère personnel

Les technologies d'IA et notamment celles qui reposent sur l'apprentissage automatique étant, par nature intrusives, il faudrait veiller à ne pas porter atteinte aux droits et libertés des individus lors de la conception et l'utilisation de ces outils.

- Les données utilisées dans le cadre du développement doivent être collectées dans le respect des exigences sur la protection des données et leur utilisation ne doit se faire que pour des finalités légitimes.
- Il faut dès lors que le responsable du traitement s’assure au préalable de la conformité de ces données et identifie les finalités pour lesquelles elles peuvent être traitées.

Agir dans la transparence

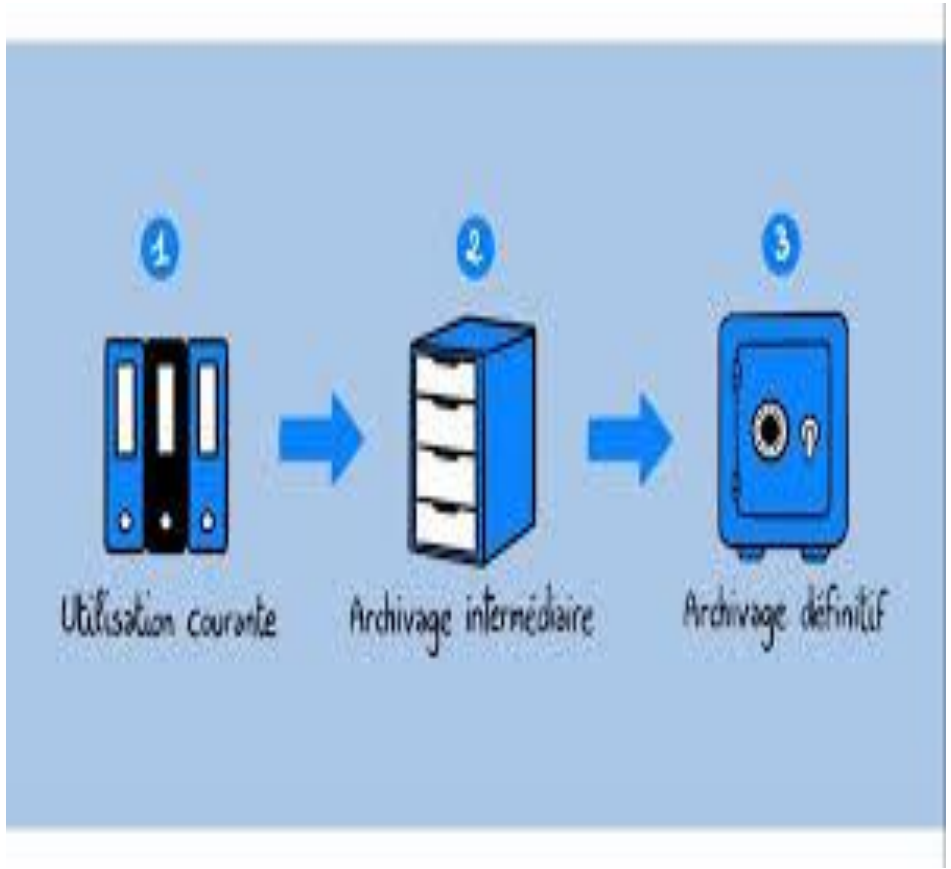
- Les responsables de traitement doivent élaborer des procédures pour rendre les systèmes d'IA transparents et compréhensibles.
- Ceci nécessite d'informer les personnes concernées des données personnelles collectées et utilisées et des modalités de prise des décisions par les systèmes d'IA, en particulier en ce qui concerne les décisions ayant un impact significatif sur eux

Recueil du consentement

- Le consentement des personnes doit être collecté dans le cas où cette base légale s’applique.

Fixée une durée de conservation

- On doit également veiller à ne conserver les données que le temps nécessaire pour atteindre les objectifs prédéfinis



Minimisation des données

- Les données personnelles collectées pour l'IA doivent être limitées à ce qui est nécessaire pour atteindre l'objectif visé.
- Ainsi, une évaluation de la quantité des données doit se faire de manière régulière afin de réduire le nombre de données utilisées durant la phase d'apprentissage et celle utilisées lors de l'usage des systèmes.

Sécurité des données

- Des mesures suffisantes et adaptées doivent permettre de sécuriser les données personnelles contre les cyberattaques ou autre violation de données et doivent renforcer la confiance dans l'utilisation des systèmes.
- Cette responsabilité d'assurer la conformité des systèmes pèse non seulement sur les fournisseurs, mais également sur les développeurs, importateurs, distributeurs, sous-traitants et fabricants, dont notamment les concepteurs des algorithmes qui doivent garantir cette conformité durant toute la durée de vie des applications.

Sécurité des données

- Des mesures suffisantes et adaptées doivent permettre de sécuriser les données personnelles contre les cyberattaques ou autre violation de données et doivent renforcer la confiance dans l'utilisation des systèmes.

Autres principes à respecter

- Les responsables du traitement doivent aussi observer les principes institués par le RGPD à savoir, le privacy by design et privacy by default.
- Le privacy by design et le privacy by default peuvent constituer la balance entre innovation et protection des données à caractère personnel (en amont et en aval du traitement).

Autres principes à respecter

- Les responsables du traitement doivent aussi observer les principes institués par le RGPD à savoir, le privacy by design et privacy by default.
- Le privacy by design et le privacy by default peuvent constituer la balance entre innovation et protection des données à caractère personnel (en amont et en aval du traitement).
- Dans cette perspective, le privacy by design s'incarne comme principe de prévention et le privacy by default comme principe de protection.

Je vous remercie de votre aimable attention!