Machine Learning et IA pour marketing et commerciaux

Éthique et responsabilité

Jeff Abrahamson

juillet / août 2024

Introduction à l'éthique et la responsabilité en IA

- Définition de la responsabilité dans le contexte du ML.
- Importance de l'éthique, de l'accessibilité, de l'inclusivité, et de l'éco-conception dans les projets ML.
- Introduction aux normes RGPD et leur importance pour la protection des données.

RGPD (en révision. . .)

- Consentement
- Intérêt légitime (contrat, obligations légales, . . .)

RGPD

- Informations Claires : informer sur la manière dont leurs données sont collectées, utilisées, stockées et partagées.
- Accès et Rectification : droit d'accès, de correction ou de suppression.

RGPD

Minimisation des Données

- Données pertinentes et nécessaires
- Anonymisation et pseudonymisation

RGPD

Droits des Utilisateurs

- Droit à l'oubli
- Portabilité des données
- Opposition

RGPD

Sécurité des Données

- Protection des données
- Data breach

RGPD

Responsabilité et documentation

- DPO
- Documentation

RGPD et l'IA/ML

- Biais et discrimination
- Explicabilité *(droit à une explication ?)*
- Impact sur la vie privée

RGPD

- Transfert en dehors de l'UE

RGPD

- DPIA pour les Systèmes ML/IA
- Identification et atténuation des risques pour la vie privée.

RGPD

- Techniques de protection des données
- Protection contre la ré-identification des individus.

RGPD

- Précautions pour les Données Sensibles
- Conformité avec les exigences strictes du RGPD.

RGPD

Décisions automatisées et profilage

- Limites des décisions automatisées *(droit de ne pas être soumis à des décisions basées uniquement sur un traitement automatisé ?)*
- Intervention humaine nécessaire pour certaines décisions importantes.

RGPD

Minimisation des données pour l'entraînement des modèles

- Minimisation et pertinence

Sécurité des Données

- Sécurité des modèles et des données
- Protection contre les accès non autorisés et les cyberattaques.

Éco-conception et optimisation des ressources

- Explication de l'impact environnemental des technologies ML (énergie, matériel, etc.).
- Techniques pour réduire la consommation d'énergie (par exemple, optimisation des modèles, utilisation d'infrastructures plus vertes).
- Importance de l'éco-conception dans le cycle de vie du développement ML.
  - Choix du modèle
  - Quantité de données

Accessibilité et inclusivité

- Le ML peut aider à améliorer l'accessibilité (reconnaissance vocale, traduction automatique, etc.).
- Enjeux de l'inclusivité dans les jeux de données et les biais potentiels (Uber, sèche-mains, reconnaissance faciale, . . .).

Sécurité et protection des données

- Principes de base de la sécurisation des données dans les projets ML.
- Impact du RGPD sur la collecte et l'utilisation des données.
- Stratégies pour sécuriser les données, y compris le chiffrement (au repos et en transit) et l'anonymisation.

Définition et contexte

- Introduction à la deanonymisation (surtout avant entraînement)
- Exemple : taxis (mais pas que)

Techniques utilisées pour la deanonymisation

- Inférence de données : des informations apparemment anonymes peuvent être croisées avec d'autres sources de données pour réidentifier des individus.
- Limites de l'anonymisation : Certaines méthodes d'anonymisation échouent — par exemple, insuffisance de l'agrégation, réversibilité des hachages avec puissance de calcul élevée, ...

Stratégies de protection contre la deanonymisation

- **Renforcement des techniques d'anonymisation** : Approfondir des méthodes avancées comme le "differential privacy", où l'ajout de bruit dans les données empêche la réidentification.
- **Contrôles d'accès et surveillance** : Mettre en place des politiques strictes de contrôle d'accès aux données et des audits réguliers pour détecter et prévenir les tentatives de deanonymisation.
- **Formation et sensibilisation** : Souligner l'importance de former le personnel impliqué dans les projets du ML à comprendre et à mettre en œuvre des pratiques de gestion des données sécurisées.

Exercice

Exercice

Choisir un projet et analyser comment le rendre plus sécure, plus respectueux de la vie privée et moins energivore.

Étapes de l'exercice

- Choisir un projet
- Identifier les enjeux spécifiques en matière d'éthique, d'accessibilité, d'éco-conception, et de protection des données.
- Élaborer une solution
  - Proposer un modèle de machine learning adapté.
  - Planifier des méthodes pour minimiser l'impact écologique (serveurs verts, optimisation du modèle).
  - Développer des stratégies pour garantir l'accessibilité et l'inclusivité.