Audit R. G. P. D. d'une IA

Le dépôt est : https://github.com/MiKL5/GDPR-audit-of-AI.

Le fichier zip contient tout le projet complet dont le modèle « rfr_model.pkl ».

Les auteurs sont :
Mickael GAILLARD → Créer et entraîner du modèle, les principes éthiques
Quentin HECQUET → Identifier les données, A. I. P. D. et P. S. S. I.
Amadou BOUBACAR → Droits des personnes, sécurité et registre de traitement.

Il s'agit d'une Intelligence artificielle qui prédit le prix des maisons en Californie via une caractéristique démographique et géographiques. Ces données sont anonymisées.

Elle est développée avec « Streamlit ». Le programme est fonctionnel avec le clavier en plus de la souris. Nonobstant, il est parfaitement compatible avec les screens-readers. Le test a été fait avec VoiceOver sur macOS 15.7.1. Les contrastes peuvent être renforcés pour une meilleure accessibilité. Les descriptions alternatives peuvent être ajoutés aux éléments alternatifs

Toutes les données utilisées pour l'estimation du prix ont pour objectif d'affiner notre modèle qui permettra une estimation du prix plus précise et plus adaptée en fonction du besoin de l'utilisateur :

- La latitude, longitude : permet de déterminer la zone géographique. Ces paramètres peu utiles sont préremplis et masqués pour simplifier la navigation.
- La proximité de l'océan : réel avantage pour un bien immobilier si proche de celui-ci.
- Le nombre moyen de chambres/pièces : critères de base pour décrire un bien immobilier ou pour en rechercher un.
- L'âge moyen de la maison permet de chercher un style de maison particulier. Et aussi en fonction de l'âge. Il peut potentiellement y avoir des rénovations à prévoir si le bien est ancien.
- La population du quartier : connaitre la tranquillité potentielle du quartier est un critère important.
- Le revenu médian : pouvoir voir si avec les critères précédents, le revenu sera suffisant et donc réalisable.
- L'occupation en moyenne : s'il est faible, cela peut indiquer un appartement/maison avec des problèmes cachés.

Droits des personnes

Conformément au RGPD, chaque personne dont les données sont susceptibles d'être traitées dispose des droits suivants :

Droit	Description	Mise en œuvre
Droit d'accès	Les individus peuvent obtenir savoir comment sont traitées leurs données et accéder aux informations les concernant.	Bien que le projet utilise des données agrégées et non personnelles, un point de contact est prévu pour toute demande d'accès.
Droit de rectification	Les personnes peuvent demander la correction de données inexactes.	Non applicable directement (les données sont statistiques), mais les sources seront mises à jour régulièrement pour garantir leur exactitude.
Droit à l'effacement ('droit à l'oubli')	Permet de demander la suppression de données personnelles.	Non concerné ici, car aucune donnée personnelle n'est récupérée.
Droit à la limitation du traitement	Permet de restreindre temporairement le traitement.	Applicable uniquement en cas de nouvelle collecte individuelle.
Droit d'opposition	L'utilisateur peut s'opposer à certains traitements.	Si une donnée personnelle devait être ajoutée (ex. retours utilisateurs), une option de refus serait intégrée.
Droit à la portabilité	Permet d'obtenir les données dans un format lisible.	Non applicable ici.

Une procédure interne devra être documentée pour répondre aux demandes sous un délai d'un mois.

Sécurité des données

Des mesures techniques et organisationnelles assurent la protection des données et des modèles utilisés :

- Chiffrement des fichiers contenant des coordonnées géographiques précises.
- Contrôle des accès via authentification forte et rôles limités.
- Pseudonymisation / agrégation systématique avant toute exploitation.
- Journalisation des accès pour détecter toute utilisation anormale.
- Sauvegardes chiffrées et tests réguliers de restauration.
- Formation et sensibilisation des membres de l'équipe à la sécurité et à la protection des données.

L'objectif est de garantir la confidentialité, l'intégrité et la disponibilité des données conformément à la PSSI.

Registre des traitements

Un registre de traitement est tenu afin de documenter toutes les activités impliquant des données, même agrégées.

Élément	Contenu
Responsable du traitement	Équipe projet (coach data / encadrant pédagogique)
Finalité	Analyse et prédiction de prix immobiliers à partir de données publiques
Catégories de données	Données géographiques, statistiques, socio-économiques agrégées
Base légale	Intérêt légitime de recherche et d'analyse de marché
Durée de conservation	Aucune conservation directe, données utilisées à la volée
Mesures de sécurité	Agrégation, chiffrement, restriction d'accès, journalisation
Transferts hors Union Européenne	Aucun transfert prévu
Évaluation d'impact (AIPD)	Réalisée sous forme simplifiée (faible risque)

Ce registre permet d'assurer la traçabilité et la responsabilité du traitement.

L’A. I. P. D. (Analyse d’Impact relative à la Protection des Données)

Elle consiste à analyser, avant la mise en place du traitement, la manière dont les données seront collectées, utilisées, stockées et sécurisées. L’objectif est d’identifier clairement les risques potentiels (perte de données, accès non autorisés, détournement d’usage, etc.) et de définir des mesures techniques et organisationnelles pour les réduire (chiffrement, limitation des accès, anonymisation, sensibilisation du personnel …). L’AIPD permet donc de garantir que le traitement est conforme au RGPD et respecte la vie privée des personnes concernées.

L’objectif de notre traitement de données est d’obtenir une estimation de prix en fonction de critères géographiques et de critères techniques. Par contre, il n’utilise absolument pas de données personnelles pour faire fonctionner la prévision ce qui nous permet d’effectuer une AIPD simplifiée.

Description du flux de données :

- Le flux de données provient de **https://moncoachdata.com/**.
- Les données traitées sont des données géographiques, agrégées, statistiques et socio-économiques.
- Grâce aux données entrées dans le formulaire, nous avons en sortie une estimation du prix.

Description du modèle ML :

- Type : modèle de régression / classification / clustering, etc.
- Données d’entrée : uniquement agrégées ou pseudonymisées.
- Données de sortie : variables statistiques sans identifiants.

Acteurs impliqués :

- Le responsable de traitement est Mickael Gaillard
- Il n’y a pas de sous-traitants.
- Les utilisateurs finaux sont des particuliers.

P. S. S. I. (Politique de Sécurité des Systèmes d'Information)

La PSSI définit les mesures techniques et organisationnelles pour sécuriser le projet. La mise en œuvre du PSSI repose sur l'adoption de bonnes pratiques au quotidien. Cela implique tout d'abord de sensibiliser l'ensemble des utilisateurs aux risques liés à la sécurité de l'information et de veiller au respect des règles définies (gestion des mots de passe, verrouillage des postes, vigilance face aux e-mails suspects). Il est également essentiel de maintenir les systèmes à jour, de sauvegarder régulièrement les données et de contrôler les accès aux ressources sensibles. Enfin, une communication claire et continue permet d'assurer l'adhésion de tous et de faire du PSSI un véritable outil de protection et d'amélioration de la sécurité. L'avantage, que nous avons dans notre cas, est qu'il n'y a ni données enregistrées ni de demande de connexion pour y accéder. Mais, sinon pour les bonnes pratiques, il faut que les identifiants de connexion soient enregistrés dans une base de données dont le mot de passe qui doit être haché. Pour le stockage de données, il faut donner une justification pour toutes données enregistrées et ne les conserver qu'un certain temps en fonction de celles-ci. Il faut que ces données soient enregistrées sur plusieurs plateformes parce que si l'on met uniquement sur un datacenter si le datacenter rencontre un problème, les données pourraient être perdues. Il faut aussi un journal de log, permettant de rencontrer s'il y a un problème tel qu'une attaque DDOS. Pour la sensibilisation, il faut que les utilisateurs soient au fait des bonnes pratiques RGPD, car le problème vient souvent des utilisateurs avec, par exemple du phishing.

Domaine	Mesures
Accès et authentification	Pas de mesure, car libre d'accès.
Stockage de données	Les données ne sont pas stockées.
Sauvegarde / restauration	Aucune donnée n'est récupérée.
Journalisation	Aucune donnée n'est récupérée.
Anonymisation / Pseudonymisation	Éviter la localisation, utiliser des référentiels tels que des villes/ quartiers.
Destruction	Aucune donnée n'est récupérée.
Sensibilisation	Formation de l'équipe aux bonnes pratiques RGPD.

Les principes éthiques

Ce projet inclus une démarche éthique by design et privacy by default. Pour l'instant, le choix a été fait de ne pas collecter de données personnelles, car, pour rechercher une maison non n'avons pas d'utilité particulière à demander les données aux utilisateurs. Hors-mis enregistrer un historique, ou des préférences de recherche ce qui est peu intéressant.

Aucune donnée des utilisateurs n'est enregistrée. Ce qui empêche tout effet néfaste.

Le modèle ne contient pas non plus de donnée personnelle. Il est constitué de données publiques. Son usage est juste pédagogique. En l'occurrence pour l'apprentissage supervisé. Le dataset est anonymisé, Les données de longitudes et de latitudes, on était pré-saisies dans le programme et ne sont plus personnalisables, ce qui biaise le prix. Ce modèle est fourni à l'adresse (**https://drive.google.com/file/d/1-Nw2V80Qy1ePUodO6489tEN_t3JVqHbY/view?usp=sharing**) à des fins pédagogiques sur Mon Coach Data (**https://moncoachdata.com/**).

L'éthique a été pensée dès la conception, conformément au principe « Privacy By Default ». Aucune collecte, conservation ou utilisation de donnée personnelle n'est possible par construction technique. Si un utilisateur voulait partager plus que ce qui est demandé à l'interface, le modèle ne permet ni d'intégrer, ni mémoriser ce pourquoi il n'est pas conçu. En conséquence, la protection de la vie privée est donc automatique et intrinsèque.

Si ultérieurement, il devient nécessaire d'ajouter des données, il faudra passer par une revue de conformité pour s'assurer que ces garde-fous restent en place.

Il est entraîné en « Random Forest », car les arbres décisionnels ont pour but d'améliorer la précision. « Random Forest » est également résistant au sur-apprentissage. L'algorithme calcule l'importance relative de chaque variable dans la prédiction globale.

Les choix de modèles et de jeux de données sont documentés, le code est disponible pour une réanalyse, permettant des audits techniques ou éthiques si c'est nécessaire.

L'application n'est pas utilisée en dehors de l'Union Européenne.

Par transparence, il est stipulé à l'utilisateur que « Le prix est estimé à partir du revenu médian, de l'âge des maisons, du nombre de pièces, la population et la proximité de l'océan. ».

Principe	Description dans le projet	Suggestions / Compléments possibles
Transparence	- Information claire sur le fonctionnement du modèle (Random Forest), le dataset est anonymisé, son usage pédagogique. - Il est mention à l'interface que l'application ne collecte ni ne stocke de données personnelles.	- Intégrer une courte explication dans l'interface pour que l'utilisateur comprenne ce qui influence la prédiction (ex. variables principales). - Prévoir un point de contact pour les demandes RGPD et éthiques.
Explicabilité	- Modèle Random Forest, indiquant l'importance des variables dans la prédiction.	- Ajouter une section dans la documentation expliquant le fonctionnement du modèle, pour être plus clair.
Accessibilité	- Fonctionnement au clavier validé. - Parfaitement compatible avec les screenreaders. - Besoin d'améliorer les contrastes en mode clair.	- Réaliser des audits RGAA / WCAG. - Ajouter descriptions alternatives, labels, aides contextuelles. - Ajouter des descriptions alternatives, labels et aides contextuelles pour les éléments interactifs. - Documenter les tests d'accessibilité réalisés et prévoir une procédure de suivi en cas de mise à jour de l'interface.
Privacy by Default	- Absence totale de collecte, conservation, ou traitement de données personnelles par conception technique. - Bloquer toute intégration ou mémorisation de données hors interface utilisateur standard.	- Maintenir cette conception dans toute évolution. - Vérifier régulièrement la conformité par audit.

Principe	Application concrète	Recommandations
Équité	Le dataset est public, anonymisé. Il minimise les biais individuels ainsi que discriminations.	Vérifier que l'entraînement du modèle ne reproduit pas de stéréotypes ou disparités non expliqués (ex : tests sur diversité géographique/ socioéconomique).
Absence de malveillance	Il n'y a pas d'effet néfaste direct pour les personnes (données non personnelles, usage pédagogique).	Préciser les limitations et avertir du caractère non contractuel de la prédiction.
Responsabilité	Le code source est ouvert, la démarche est transparente.	Identifier clairement le respon-sable du projet pour toutes les questions éthiques.