Proposition d'un sujet de thèse

Titre : Réduction des biais pour un apprentissage collaboratif et éthique sur des données dynamiques.

Laboratoire d'accueil : LISTIC - Laboratoire d'Informatique, Systèmes, Traitement de l'Information et de la Connaissance - Université Savoie Mont Blanc, Annecy-le-Vieux, France.

Direction de thèse : Prof. Alexandre Benoit
Dr. Faiza Loukil
LISTIC, Université Savoie Mont Blanc, Annecy-le-Vieux, France.

Description du sujet de thèse :

De nos jours, l'apprentissage automatique est appliqué dans de nombreux domaines pour extraire des connaissances à partir de données et guider des processus de prise de décision de plus en plus complexes, des moteurs de recherche au diagnostic de maladies. Il est donc crucial de s'assurer que les prédictions apportées par ces approches ne reflètent pas un comportement discriminatoire envers certaines populations, au sens statistique, que ce soit au niveau des données ou des personnes. L'un des facteurs qui peuvent conduire à des décisions erronées est le biais d'apprentissage. Il est généralement la conséquence de l'utilisation d'ensemble de données et de modèles incomplets, défectueux ou préjudiciables. Ces biais prennent leur origine dès la collecte des données. Cette collecte peut prendre différentes formes selon la manière dont le modèle recherché est optimisé. Les approches classiques optimisent un modèle sur un serveur central. Cela implique de communiquer et d'agréger sur ce serveur toutes les données créées depuis des sources potentiellement distantes et distribuées. Cette approche pose alors des problèmes de coût de communication ainsi que de protection de vie privée (privacy). Finalement, dans cette configuration désormais classique, la réduction des biais peut être réalisée en bénéficiant de l'accès à l'ensemble des données, mais reste un problème ouvert.

Afin de contrer ces différents problèmes, une approche collaborative a été récemment introduite, appelée apprentissage fédéré (FL pour Federated Learning). Elle permet l'optimisation locale de modèles, près de chaque source de données. Par un processus collaboratif, les modèles locaux partagent leurs paramètres des modèles pour gagner en capacité de généralisation et produire un modèle plus général, sans jamais que les données ne soient transmises. Ainsi, réduisant les coûts de communication, protégeant les données privées en étant structurellement compatibles avec le règlement général de protection des données (RGPD), le FL apparaît comme une approche très prometteuse. En revanche, les problèmes de biais doivent être considérés sous un angle nouveau, en prenant notamment en compte le taux de participation et les distributions de données de chaque modèle participant [1]. En outre, les contraintes de protection de vie privée imposées en apprentissage fédéré ne permettent pas d'utiliser les techniques classiques d'atténuation des biais. Ainsi, bien que le FL apparaisse comme une étape majeure en apprentissage automatique, l'étude de ses biais reste un verrou scientifique important à lever.

L'état de l'art rapporte plusieurs approches basées sur différents types de techniques d'atténuation des biais, notamment des **techniques préventives** et des **techniques réactives**. Cependant, ces approches restent néanmoins incomplètes, imposent des compromis et se focalisent sur une approche globale. Au-delà de ces problématiques globales, l'une des finalités de l'apprentissage fédéré est de construire des modèles adaptés à des populations organisées de façon hiérarchique dans le but de générer non pas un seul modèle général, mais également un ensemble de modèles intermédiaires pertinents pour des groupes de populations différentes. D'autre part, il peut être intéressant que ces modèles intermédiaires puissent être dynamiques. *Des questions se posent alors sur la construction potentiellement dynamique de la hiérarchie. En toute cohérence, il est alors nécessaire de s'intéresser aux problèmes de biais et de privacy que cela peut engendrer.* Dans ce cadre réaliste, l'état de l'art ne rapporte pas de travaux et se limite à une approche globale sur l'ensemble des populations [2][3].

L'objectif de cette thèse est alors de proposer des méthodes de détection et d'élimination des biais à la fois globaux et liés à des sous-populations en prenant en compte l'aspect dynamique des données et les contraintes de protection de vie privée. Ainsi, ce travail vise à apporter des réponses sur les questions scientifiques suivantes dont l'ordre pourra guider le programme de recherche :

- Comment définir les biais dans les modèles d'apprentissage fédéré, et comment les mesurer ?
- Quels indicateurs définir pour alerter les utilisateurs, dans les phases de conception et production ?
- Quelles méthodes optimales applicables à l'apprentissage fédéré proposer pour éliminer les biais ?
- Quel est l'impact de cette approche d'élimination des biais sur la convergence et l'efficacité ainsi que sur les performances des modèles finaux ?
- Comment mettre en œuvre ces approches dans un système réel pour lequel les données sont organisées de façon hiérarchique, mais en constante évolution ?

La personne recrutée pourra donc s'intéresser à ces questions en s'appuyant tout d'abord sur des données de référence dans la littérature. Ensuite, les données issues de collaborations au sein de la Solar Academy de l'USMB ou de télédétection au sein du LISTIC pourront être intégrées. Sur les aspects ressources de calcul, la personne recrutée aura accès au mésocentre de calcul MUST de l'USMB.

Profil recherché : Idéalement, le/la candidat(e) suit actuellement une formation (master de recherche, diplôme d'ingénieur, ...) en lien avec le domaine de l'Intelligence Artificielle/Apprentissage Automatique. La connaissance en ingénierie des données et particulièrement en apprentissage distribué sont nécessaires. De bonnes compétences au développement logiciel et la maîtrise de langages de programmation (idéalement Python) sont indispensables. Le/la candidat(e) devra être capable d'apporter ses idées novatrices, son enthousiasme, sa rigueur et devra faire preuve d'un esprit d'équipe prononcé.

Candidatures : Lettre de motivation pour la thèse et la thématique.
CV détaillé.
Relevés de notes M1 et M2 ou équivalent.
Lettre de recommandation si possible.

Informations complémentaires et candidatures par mail :
Dr. Faiza Loukil, faiza.loukil@univ-smb.fr.
Prof Alexandre Benoit, alexandre.benoit@univ-smb.fr.

References

1. Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., et al.: Advances and open problems in federated learning. Foundations and Trends® in Machine Learning **14**(1–2), 1–210 (2021)
2. Sattler, F., Müller, K.R., Samek, W.: Clustered federated learning. In: Proceedings of the NeurIPS'19 Workshop on Federated Learning for Data Privacy and Confidentiality. pp. 1–5 (2019)
3. Silva, A., Metcalf, K., Apostoloff, N., Theobald, B.J.: Fedembed: Personalized private federated learning. arXiv preprint arXiv:2202.09472 (2022)