IA et vie privée : Amazon vise un traitement plus confidentiel du langage naturel

La « vie privée différentielle » a la cote chez les GAFA.

L'approche consiste à exploiter des techniques mathématiques pour rendre le plus anonymes possible les résultats que produisent des algorithmes d'IA.

Apple a œuvré à appliquer le concept, notamment à son navigateur Safari. Google l'a intégré à son *framework* de *machine learning* TensorFlow.

Amazon est aussi sur le coup. Ses équipes en témoigneront le mois prochain à l'occasion de la conférence Web Search and Data Mining.

Y sera présenté un cas d'usage de la vie privée différentielle dans le domaine du traitement automatique du langage naturel.
L'idée générale est de reformuler un texte avant de l'analyser.

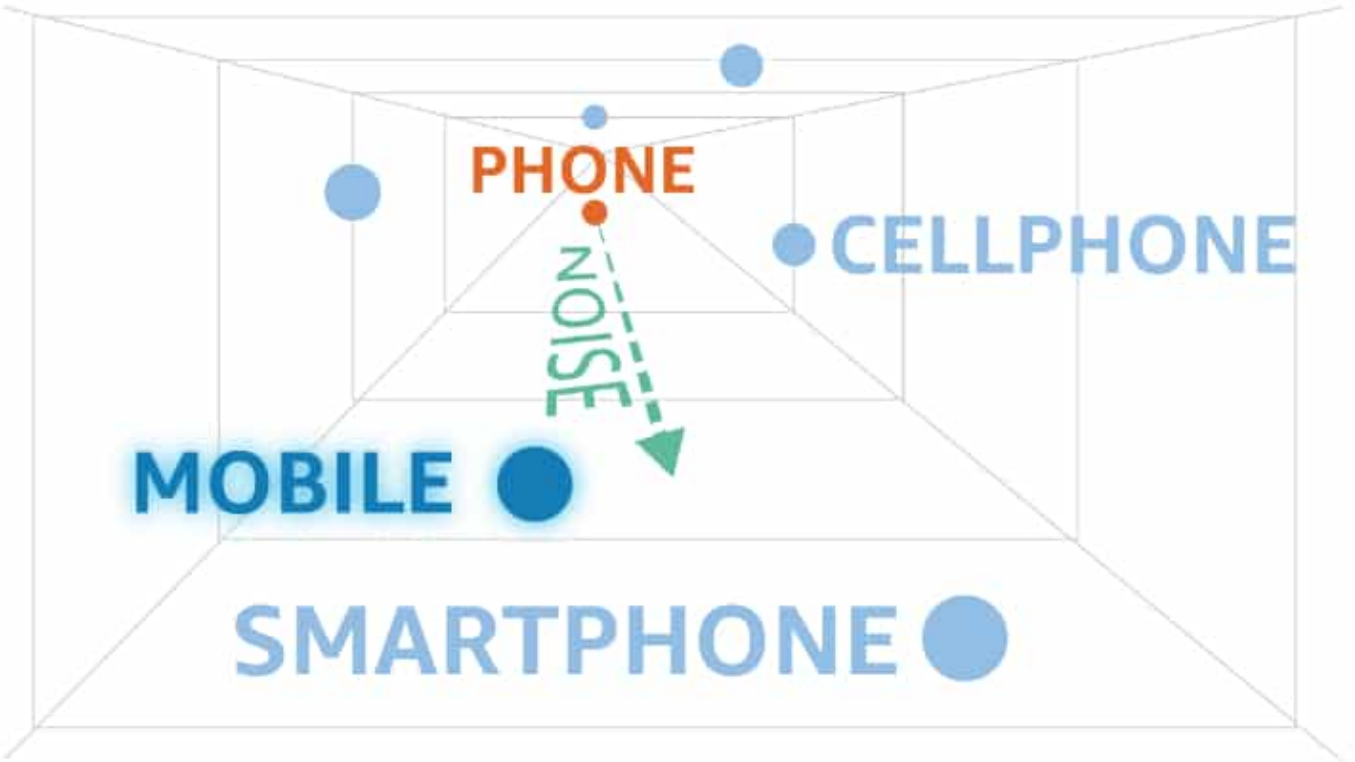
Du bruit dans l'espace

La vie privée différentielle constitue un moyen de calculer la probabilité qu'une analyse de données puisse permettre d'identifier des individus.

L'objectif est de réduire au maximum cette probabilité. Ce en apportant la garantie d'un résultat presque identique avec ou sans les données qui peuvent présenter des risques. Le « presque » est contrôlé par un paramètre epsilon (ε).

L'approche traditionnelle consiste à ajouter du « bruit » dans le jeu de données cocncerné. Mais cela implique souvent une dégradation des résultats.

Les équipes d'Amazon ont choisi d'introduire le bruit ailleurs. En l'occurrence, au sein de l'espace vectoriel où les algorithmes de traitement du langage représentent les mots.



Les mots dont l'occurrence est simultanée au sein des phrases ont tendance à être proches dans cet espace vectoriel.

Les chercheurs s'appuient sur cette caractéristique pour remplacer une donnée par une autre tout en conservant la sémantique du texte.
Ils appellent cela la vie privée différentielle « métrique ».
La tolérance est égale à epsilon fois la distance entre les deux données.

Les courbes du langage

À l'origine, cette technique fut utilisée por des données de géolocalisation.

Il y a néanmoins une subtilité. Si ajouter du bruit à une localisation produit une autre localisation, faire de même avec une représentation de mots ne fait que produire un autre point dans l'espace vectoriel. Et ce point ne correspond probablement pas à la localisation d'une représentation valide. Il faut donc chercher la représentation valide la plus proche de ce point. Parfois, il s'agit du mot lui-même. Dans ce cas, on ne le modifie pas.

Les chercheurs se sont intéressés aux effets que produisaient une variation d'epsilon. Entre autres sur la probabilité de modification d'un mot et sur le nombre de mots se trouvant à une distance fixée d'un autre mot.

Ils avaient présenté, en novembre 2019 à l'International Conference on Data Mining (IDCM), un rapport qui constitue en fait la suite de celui dont ils traiteront le mois prochain.

Il y est question de l'extension de leurs travaux à un espace vectoriel hyperbolique.

Par rapport à l'espace euclidien, la courbure permet de mieux situer des représentations dans une

hiérarchie sémantique. Et ainsi substituer plus efficacement des termes spécifiques à des termes génériques.

Donnant l'exemple des termes « traitement médical », « médicament » et « ibuprofène », Amazon affirme que l'espace hyperbolique apporte 20 fois plus de garanties en matière de protection de la vie privée.