

L'Obs > Economie

***A* L'algorithme de Bercy qui sait tout de vous (et va peut-être trouver vos petits arrangements fiscaux)**

L'OBs

Géolocalisation, photos de vacances sur les réseaux sociaux, virements et retraits bancaires, données patrimoniales et allocatives... Le fisc a mis au point un outil informatique qui analyse les données personnelles des contribuables pour mieux cibler de potentiels fraudeurs.

Par **Sara Daniel**

Publié le 04 octobre 2019 à 07h00

Pour lutter contre les infractions fiscales, Bercy a depuis quelques années recours à l'intelligence artificielle pour collecter et analyser les données administratives des contribuables. Il entend désormais chasser les fraudeurs sur les réseaux sociaux et les places de marché (Amazon, etc.). **Gregory Lewkowicz**, professeur de droit à l'université libre de Bruxelles, enseignant à Assas, HEC Paris et Sciences-Po, explique à « l'Obs » comment le tournant numérique transforme l'Etat en profondeur et questionne les limites de la surveillance généralisée des particuliers par la puissance publique.

Bercy a discrètement annoncé, il y a deux ans, qu'il travaillait sur un algorithme d'identification de la fraude fiscale fondé. Où est-on actuellement ?

Bercy poursuit bel et bien actuellement le développement d'un outil informatique portant le nom un peu barbare de « ciblage de la fraude et valorisation des requêtes » (CFVR). Concrètement, ce CFVR mobilise en effet des techniques d'intelligence artificielle pour analyser les données des contribuables et identifier automatiquement les cas suspects de fraude.

S'il visait initialement les entreprises, il a été étendu aux particuliers en 2017 pour une phase test de deux ans. Bercy cherche à pérenniser l'utilisation de cet outil pour scruter le comportement de tous les contribuables et étendre la liste des données qui peuvent être collectées pour alimenter le système.

LIRE AUSSI



LIRE AUSSI



En fait-on assez contre la fraude fiscale ?

La Commission nationale de l'Informatique et des Libertés (Cnil) s'est réunie le 12 septembre dernier pour examiner le projet d'arrêté qui doit lancer cette nouvelle étape. Tout le monde attend de lire son avis car il s'agit d'une petite révolution qui pose la question des limites de la surveillance généralisée des particuliers par la puissance publique.

Cependant, le mouvement est en marche, puisqu'un projet de loi vient d'être déposé à l'Assemblée, ce vendredi 27 septembre, qui autorise les administrations fiscales et douanières à collecter et exploiter les données rendues publiques sur les réseaux sociaux et les plateformes.

Quelles sont exactement les données des contribuables qui sont collectées et analysées ?

Avec ce système, tout passe au crible de la fouille des données (ce que l'on appelle le *data mining*) : les coordonnées des contribuables, leurs données bancaires et patrimoniales, celles issues d'autres administrations ou d'organismes sociaux, celles provenant de bases de données privées... jusqu'à celles disponibles sur les réseaux sociaux, tels que Twitter ou Facebook. Sur cette base, le CFVR permet de visualiser les données et les réseaux de relations économiques entre les personnes, d'extraire des modèles prédictifs de comportements frauduleux ou d'identifier des incohérences dans les données d'un contribuable.

LIRE AUSSI > « Name and Shame », algorithmes... Le gouvernement dévoile son arsenal antifraude fiscale

Pour les particuliers, il s'agira notamment de définir leur style de vie grâce à l'analyse automatique des données. Si votre style de vie n'est pas en adéquation avec vos revenus, vous ferez l'objet d'un

signalement et, sans doute, d'un contrôle. A moyen terme, l'administration fiscale souhaite que 50 % des contrôles soient diligentés sur cette base.

Bercy poursuit ainsi deux objectifs : un ciblage plus efficace de la fraude et une réduction substantielle des effectifs de la Direction générale des Finances publiques. On parle à terme d'une réduction d'un tiers des effectifs...

Ce système informatique de ciblage fiscal est-il propre à la France ou est-il appliqué ailleurs en Europe ?

Dans toutes les économies développées, la tendance est à l'utilisation de l'intelligence artificielle pour traquer la fraude fiscale. Le Royaume-Uni est particulièrement avancé dans le domaine avec son système d'analyse « Connect », qui exploite une masse affolante de données personnelles. De l'autre côté de la Manche, plus de 90 % des contrôles résultent actuellement d'un signalement par le système. Le rôle de l'administration fiscale dans la programmation des contrôles est clairement devenu marginal. Ses effectifs ont d'ailleurs fondu.

Quelles leçons ont pu être tirées de cette expérience britannique ?

La première leçon est que ce système a conduit le Royaume-Uni à adopter une politique de contrôle plus agressive et à augmenter significativement ses rentrées fiscales, sans pour autant modifier formellement son droit fiscal.

Cette transformation a toutefois un coût. La Chambre des Lords a souligné en décembre 2018 que, dans l'ensemble, l'augmentation de l'efficacité de l'administration fiscale dans la perception de l'impôt s'est faite au détriment d'un traitement équitable des contri-

buables, en particulier des contribuables lambda, plus démunis que les grandes entreprises et les contribuables mieux nantis qui sont entourés de conseils professionnels. Entre 2015 et 2018, le contentieux fiscal a également augmenté de 43 %.

La deuxième leçon est que la soif de données de l'administration n'a pas de limite naturelle. Depuis l'entrée en vigueur de l'*Investigatory Power Act*, le fisc peut ainsi passer au crible du système Connect les transactions des cartes de crédit, les données de plateformes comme eBay ou Airbnb et même l'historique de navigation des contribuables sur internet. Les juridictions britanniques comme européennes sont certes intervenues. Mais le mouvement vers une administration fiscale obèse de données demeure.

N'est-on pas ici en face d'une dérive juridique ?

Je dirais même qu'il s'agit à mes yeux d'une véritable subversion du droit. En surface, rien ne change. En pratique, rien n'est plus pareil. Lorsqu'on ne contrôle que les contribuables dont les données correspondent aux modèles prédictifs identifiés par des algorithmes, il ne faut pas être grand clerc pour comprendre que ces modèles ont, en pratique, transformé la règle de droit, autrefois interprétée par l'administration soit au cas par cas, soit dans des circulaires interprétatives. Mais, alors que les circulaires interprétatives sont publiées, ce n'est pas le cas des modèles et des algorithmes en question. Cela prive le contribuable d'une information utile pour la défense de ses droits.

Le contribuable français a-t-il la possibilité de réagir ?

Sous l'angle de la protection des données personnelles, il faut attendre de connaître l'avis de la Cnil pour se prononcer. Elle avait insisté jadis pour que le CFVR soit seulement un outil d'aide à la décision et non un outil de profilage destiné à identifier directe-

ment des fraudeurs potentiels. Je ne crois pas à cette distinction. Les expériences étrangères montrent que la pente naturelle va vers le profilage des contribuables. Quant à l'accès aux modèles et aux algorithmes utilisés par le logiciel, la Commission d'Accès aux Documents administratifs (Cada) a déjà indiqué que cette information n'était pas communicable car cela nuirait à la recherche des infractions fiscales.

Des actions individuelles seront possibles. Elles me paraissent toutefois insuffisantes. Nous avons affaire à une reformulation de la règle par des modèles mathématiques généraux. Or, nos états de droit sont fondés sur la distinction entre la règle générale, qui est l'apanage du pouvoir politique, et son application par l'administration ou par le juge. A partir du moment où l'administration applique de manière homogène une règle générale qui est issue d'un traitement de données par des algorithmes – c'est-à-dire qu'elle ne contrôle plus que les contribuables dont les données correspondent à un modèle prédictif –, il faut inventer des voies pour contester directement ces modèles et non simplement l'une ou l'autre de leur application.

Récemment, le logiciel Parcoursup, qui préside à l'admission des étudiants dans le supérieur, a fait couler beaucoup d'encre. Est-ce un autre exemple concret, ordinaire, de ces algorithmes qui gouvernent nos vies ?

Les cas des logiciels Admission Post-Bac (APB) puis Parcoursup, ont été l'occasion pour le grand public d'une véritable prise de conscience des effets de la transformation numérique de l'Etat et de son administration. Il illustre le même phénomène que le CFVR. Le logiciel APB avait été conçu pour appliquer le code de l'éducation et gérer de manière automatisée l'admission des étudiants dans les établissements d'enseignement supérieur. Les dé-

veloppeurs se sont attelés à la tâche de bonne foi. Mais la règle de droit n'est pas un algorithme. Elle n'a pas été écrite pour être appliquée par un logiciel. Tant et si bien que les critères du code de l'éducation ne suffisaient pas à départager les candidats dans les filières en tension.

LIRE AUSSI > Derrière l'algorithme de Parcoursup, un choix idéologique

A un moment, on aurait dû avoir une forme d'appréciation ou de jugement d'opportunité dans la prise de décision. Mais les logiciels ne savent pas poser un jugement d'opportunité car nous sommes incapables d'en formaliser les paramètres. Les développeurs ont donc programmé un tirage au sort lorsque l'application successive des critères légaux ne permettait pas de départager les candidats. Pour ceux qui pensent qu'un jugement d'opportunité est une formule élégante pour « décision arbitraire », c'est peut-être satisfaisant. Pour les autres, remplacer un jugement d'opportunité par un tirage au sort, c'est une modification significative du sens de la règle. Une subversion du droit par son application automatisée.

Avec Parcoursup, la situation est plus difficile à apprécier. Le Conseil d'Etat a en effet décidé que les fameux « algorithmes locaux » utilisés par les établissements n'étaient pas communicables. Lorsqu'on observe les démissions en cascade au sein du comité éthique et scientifique de Parcoursup, on se demande toutefois de quoi ces démissions sont le nom. Surtout lorsqu'un scientifique comme Julien Grenet dit craindre que « *les conditions ne soient pas réunies pour que le comité soit en mesure d'analyser sereinement et en toute indépendance le déroulement de la deuxième année de Parcoursup* » dans sa lettre de démission du mois d'août dernier.

Quels autres algorithmes de gouvernance peut-on identifier ?

Il faut bien comprendre que le tournant numérique, ce n'est pas juste une évolution économique ou sociale. C'est aussi une transformation en profondeur de l'Etat, des pouvoirs publics et de leur mode de fonctionnement. Qu'il s'agisse de l'inscription à l'état civil ou de l'attribution des prestations sociales, du contrôle des marchés financiers ou des banques, de la résolution des litiges ou du contrôle de l'égalité salariale, de la surveillance du trafic automobile ou encore du contrôle des frontières, absolument toutes les missions de l'Etat suivent à des vitesses et à des degrés divers le chemin de l'informatisation, de l'automatisation et de l'algorithmisation.

LIRE AUSSI > « Les algorithmes sont une arme de domination sociale »

La montée en puissance de cette nouvelle figure de l'Etat qu'on qualifie parfois d'« Etat-plateforme » est en cours en France comme à l'étranger. On commence à en mesurer plus précisément les risques en termes de discrimination, de renforcement des inégalités sociales, de limitation des libertés individuelles, de captation de l'Etat par les producteurs commerciaux de solutions informatiques, de technocratisation du pouvoir, etc.

Dans cet « Etat-plateforme » dont vous parlez, quelles garanties avons-nous encore que nos sociétés respectent les droits fondamentaux ?

Je vais vous répondre en partant d'un pays lointain que l'on observe avec effarement en détournant les yeux de ce qui se passe chez nous. En Chine, le système de crédit social, qui vise à attribuer à tous les citoyens un score social basé sur l'analyse d'une plé-


thore de données et à en tirer des conséquences juridiques, est en cours. Ce système est souvent présenté comme un exemple repoussoir de l'Etat-plateforme. La Chine mettrait en place Big Brother alors que, se défend-on, ce ne serait pas le cas dans les démocraties libérales. Bien qu'elles soient le fruit d'initiatives plus disséminées, les évolutions dans les démocraties libérales ne me semblent toutefois pas tellement différentes. La Chine exporte du reste ses technologies de surveillance dans plus de 63 Etats, dont la France, par exemple, à Marseille ou à Valenciennes. Cela fait réfléchir...

LIRE AUSSI > Chine, la dictature high-tech

Je crois que le respect des droits fondamentaux et des principes de l'état de droit est en effet le grand enjeu de la transformation en cours. Certains vous diront que la solution est déjà là grâce au Règlement général sur la Protection des Données (RGPD) et à l'éthique de l'intelligence artificielle. Ce n'est pas suffisant. Nous avons besoin d'une grande ingéniosité politique et juridique. Nous devons réinventer les contre-pouvoirs, les mécanismes de contrôle et la participation citoyenne si nous ne voulons pas sacrifier nos principes sur l'autel de l'intelligence artificielle et de la digitalisation.



Sara Daniel

 Vous avez aimé cet article ?
Offrez-le à un ami (10 restant s)

Offrir