VIE PRIVÉE

La centralisation des données à des fins de surveillance n'est pas qu'un fantasme. Pour Elise Degrave (UNamur), l'outil Oasis, utilisé pour la lutte contre la fraude sociale, témoigne de cette tendance insidieuse. Et dangereuse pour la démocratie.

« C'est ce qui s'est passé aux Pays-Bas avec le système Syri, semblable à Oasis. Des études ont démontré que l'outil ciblait en priorité les quartiers de pauvres et de migrants. Les algorithmes étaient biaisés. » © ROGER MILUTIN.

« Aujourd'hui, l'Etat profile déjà les Belges »

ENTRETIEN

PHILIPPE LALOUX

A la faveur de la crise sanitaire, le citoyen a pris conscience de la masse énorme de données à caractère personnel gérées par l'Etat. Et, dans la foulée, des libertés qu'il prend parfois avec la vie privée des citoyens. Ceux-ci découvrent aussi l'existence de projets de croisement de données portés par les administrations, mais sans gage de transparence sur leur finalité, le respect du cadre légal ou le contrôle politique. Elise Degrave, professeure à la Faculté de droit de l'UNamur, y perçoit la confirmation d'une tendance lourde : la centralisation des données, antichambre d'un Etat « automatisé », où le débat démocratique aurait été confisqué par les technocrates.

Plusieurs événements d'actualité ont ravivé le spectre du « profilage » des Belges par l'Etat. A tort ?

Mais non, ce projet existe déjà. Et de manière très aboutie. L'outil s'appelle « Oasis » (NDLR, Organisation antifraude des services d'inspection sociale). Il est fonctionnel depuis 2005. Il s'agit d'une centralisation de nombreuses données de l'ONSS, de l'Onem, du SPF Sécurité sociale et du SPF Emploi. Non seulement on centralise, mais on applique des algorithmes qui vont tenter de deviner le comportement des citoyens et trouver des noms de personnes suspectées de fraude sociale. C'est du profilage.

En réalité, cette base de données n'est créée par aucune loi, ni arrêté royal. Et on ne trouve que très peu d'informations à son propos, si ce n'est par hasard en farfouillant dans des documents de l'administration. Rien sur le site de la Banque carrefour de la Sécurité sociale (BCSS), ni de l'ONSS. Quand on s'adresse à l'administration, on ne reçoit que quelques informations parcellaires, mais jamais la copie des algorithmes, ni même d'information claire à leur sujet.

On apprend par contre, documents publics à l'appui, qu'Oasis va être prochainement remplacé par le projet « Big Data Analytics Platform ». Le marché, estimé à 6,75 millions d'euros, a été attribué par la Smals (NDLR, l'ASBL informatique de l'Etat) à Deloitte Consulting & Advisory le 9 juillet 2019.

Ces algorithmes sont censés traduire le droit pour rendre la lutte contre la fraude plus efficace. N'est-ce pas légitime ?

Oui, mais il faut avoir des outils dont on peut contrôler le fonctionnement. Ce qui n'est pas le cas. On ne sait ni par qui, ni comment ils ont été faits. Or, on sait qu'un algorithme ne peut traduire parfaitement des règles de droit. Il peut être biaisé, discriminatoire. Sans contrôle, les algorithmes peuvent renforcer les inégalités, surtout lorsqu'ils s'appliquent à l'échelle d'une population.

Par ailleurs, il y a une masse énorme de données. Donc, on ne peut pas exclure qu'il n'y a pas d'erreurs. Ni les employeurs ni les travailleurs ne peuvent vérifier ces données. On ne sait même pas que ça existe. Ce qui amène parfois à cibler des gens qui n'ont rien fait. Et celui qui est visé par un algorithme ne va pas comprendre pourquoi il se retrouve dans le radar. Les inspecteurs eux-mêmes disent ne pas comprendre pourquoi ils vont contrôler tel employeur plutôt qu'un autre. On n'a pas la main sur l'outil. Il y a juste un ordinateur qui vous crache des noms.

> *Il faut avoir des outils dont on peut contrôler le fonctionnement. Ce qui n'est pas le cas*

Le conseil des ministres restreint vient d'adopter un avant-projet de loi, révélé par *La Libre,* consacrant la fin des visites du fisc au domicile des contribuables. Tout passerait par le « cloud ».

Cela pourrait être encore pire. On risque de donner tout pouvoir à l'outil informatique. Or, sans garanties spécifiques pour les personnes concernées, une décision prise entièrement par ordinateur est contraire au Règlement général sur la protection des données.

L'informatique peut-elle biaiser le fonctionnement de l'administration ?

C'est ce qui s'est passé aux Pays-Bas avec le système Syri, semblable à Oasis. Des études ont démontré que l'outil ciblait en priorité les quartiers de pauvres et de migrants. Les algorithmes étaient biaisés. Le Rapporteur spécial des Nations unies sur l'extrême pauvreté et les droits de l'homme, le professeur Philip Alston, épinglait que si cela se passait dans la vraie vie, on verrait une masse d'inspecteurs venir systématiquement frapper aux portes dans ce quartier, et jamais ailleurs. Là on verrait qu'il y a un problème. Tandis qu'ici, avec un outil informatique dont on ne sait même pas qu'il existe, on ne voit rien. Et on ne sait même pas qu'il y a un souci. Ce qui pose un problème de démocratie, parce qu'il n'y a même plus de possibilités de dialoguer avec l'administration.

Elise Degrave

Professeure à la Faculté de droit de l'UNamur et directrice de recherches au Namur Digital Institute/Crids, elle codirige également la Chaire E-gouvernement de l'UNamur dédiée notamment aux questions de gestion des données par l'Etat. Elle fait également partie du Conseil du numérique. Régulièrement auditionnée par le Parlement sur les questions liées au traitement des données à caractère personnel, Elise Degrave est aussi autrice de nombreux articles scientifiques, notamment dans *Le Journal des Tribunaux* du 13 février dernier (*Les citoyens contrôlés via leurs données covid ? Le « datamatchning » et le « datamining » utilisés par l'Etat*).

algorithmes « Un Etat "automatisé" est un Etat qui s'asphyxie »

PH.L.

Le modèle belge de gestion des données est historiquement basé sur la décentralisation. Est-il en train de s'effondrer ?

A la base, la Belgique avait un très beau modèle, avec des réseaux décentralisés de données par « événement de vie », par « matière » (santé, sécurité sociale, fiscalité…). Progressivement, au motif d'être efficace, on a commencé à réutiliser ces données à des fins qui ne sont pas celles pour lesquelles on les a collectées. Il y a eu notamment la loi du 5 septembre 2018 qui crée le Comité de sécurité de l'information (CSI), mais qui donne également une base légale générale au rassemblement de données (« datamatching »). Avec la possibilité, après, de faire du « datamining », soit y appliquer des algorithmes, pour renforcer la lutte contre la fraude fiscale et sociale. Mais ces dispositions n'ont jamais fait l'objet d'un débat parlementaire à la hauteur des enjeux. Elles sont passées malgré les avis très critiques du Conseil d'Etat et de l'Autorité de protection des données. En fait, cette loi de 2018 détricote ce modèle d'administration décentralisée. Elle assume la centralisation et le profilage.

La crise covid a-t-elle joué un rôle d'accélérateur de cette tendance à la centralisation ?

Elle a mis en évidence une lame de fond insidieuse et dangereuse à la centralisation des données. L'avant-projet de loi pandémie s'inscrit d'ailleurs dans la suite de cette logique. De même que l'arrêté ministériel du 12 janvier dernier, où, pour la première fois, on organise le croisement de données santé avec des données de sécurité sociale. On donne donc à l'ONSS de nombreuses données collectées durant le covid. On pourrait dès lors imaginer des réutilisations des données de santé à des fins autres que purement sanitaires.

Le citoyen a-t-il perdu la main sur la gestion de ses données ? On nous avait promis l'inverse avec le RGDP…

La Belgique était pionnière dans cette idée du « privacy by design » (NDLR, le respect de la vie privée envisagé comme socle de base d'un projet). C'était le cas, dès les années 90, avec la Banque carrefour de la Sécurité sociale. Mais on n'a pas suffisamment mis le citoyen en situation de comprendre ce qu'il se passait. Par exemple, il manque vraiment un site sur lequel il peut voir où sont enregistrées ses données et qui les a consultées. C'est le cas avec le Registre national, mais cet outil devrait être dupliqué à toutes les administrations.

Le citoyen n'a pas le choix : il doit donner ses informations à l'Etat. Il ne peut même pas mentir, comme il peut le faire quand il s'inscrit sur Facebook. Bref, il a peu de prise sur ses données. Il doit pourtant y avoir un pacte de confiance entre lui et l'Etat. Le fait de mener des projets du type Oasis ou, à présent, « Big Data Analytics Platform », sans débat, sans pédagogie, sans transparence sur le sort réservé à ses données, risque de nuire à cette confiance. On l'a vu pendant la crise : sans cette confiance, certaines mesures de lutte contre le coronavirus ne fonctionnent pas (par exemple le traçage).

Les projets de centralisation semblent motivés par des soucis d'efficacité de l'administration…

On pense « efficacité » de l'administration, en automatisant le processus, mais pas à la place du citoyen par rapport à l'administration, dans un esprit démocratique. Un Etat « automatisé », c'est un Etat qui risque d'être technocratique. En particulier en matière numérique, il confie la clé à des experts qui mettent en place des outils qui ont un impact démocratique important mais qui ne sont pas débattus, voire connus des citoyens. Un « Etat automatisé », c'est un Etat où tout va fonctionner (et encore…), mais où il n'y a plus de dialogue avec le citoyen, perçu par les technocrates comme un élément encombrant, parce qu'il hésite, parce qu'il remet en question… Bref, c'est un Etat qui tourne sur lui-même, qui s'asphyxie. C'est comme mettre des puces sur les bulles à verre pour savoir quand il faut venir les vider, mais sans ne plus jamais avoir de débat sur la gestion des déchets. Il faut impérativement que le numérique, plutôt que de traquer le citoyen, lui permette de s'impliquer en société. Qu'il n'éteigne pas la démocratie, mais au contraire la stimule.