Elise Degrave[1], Clément Maertens[2] et Laurent Roy[3]

Les droits fondamentaux face aux algorithmes du secteur public[4]

Les pouvoirs publics n'échappent pas à l'usage des technologies, notamment les algorithmes, pour faciliter certaines tâches. La gouvernance algorithmique, que l'on entend ici comme l'utilisation des algorithmes dans l'exercice du pouvoir, affecte de façon inédite les libertés citoyennes.

Des spécificités dans le secteur public

Promesse d'efficacité pour l'agent de l'administration et de simplicité pour l'administré, la réutilisation des données des citoyen·nes via des algorithmes est de plus en plus fréquente au sein de l'administration et de la police. En Belgique, citons par exemple l'utilisation policière de la reconnaissance faciale pour identifier des suspects[5], les algorithmes utilisés en Communautés française[6] et flamande[7] pour répartir les élèves dans les écoles secondaires, le ciblage des fraudeur·euses sociaux·ales opéré par le logiciel OASIS[8], la détection des domiciliations fictives sur base des données de consommation d'eau, de gaz et d'électricité des assuré·es sociaux·ales[9], ou encore la création de l'immense base de données biométriques européenne Eurodac pour la gestion de la crise migratoire[10]. Derrière leur caractère anodin, ces dispositifs sont en réalité porteurs de grands risques pour les droits fondamentaux, parmi lesquels on retrouve la discrimination des individus, la dégradation de leurs conditions de vie, ou encore l'atteinte à leur liberté de circuler, de manifester, de s'exprimer et d'être protégé dans leur vie privée et familiale[11].

À la différence du secteur privé, le déploiement de ces technologies est **contraignant** dans le secteur public. Là où les citoyens peuvent refuser de se créer un compte Instagram, ils n'ont pas d'autre choix que d'inscrire leurs enfants à l'école, de demander des allocations familiales, ou de décliner leurs identités aux frontières.

Ainsi qu'on l'a dit, certains droits fondamentaux s'en trouvent bousculés, à commencer par le droit à la vie privée. C'est pourquoi des balises doivent être respectées parmi lesquelles la **légalité** qui exige que le Parlement encadre ces outils au terme d'un débat démocratique ayant notamment

1 Professeure à la Faculté de droit de l'UNamur ; Directrice de recherches au Nadi/Crids et à la Chaire E-gouvernement de l'UNamur.
2 Maître en Droit ; Etudiant du Master de spécialisation en droit de l'internet (DTIC) à l'UNamur ; Membre de la Commission Nouvelles technologies et Vie Privée de la Ligue des Droits Humains.
3 Maître en Éthique ; Etudiant du Master de spécialisation en droit de l'internet (DTIC) à l'UNamur ; Membre de la Commission Nouvelles technologies et Vie Privée de la Ligue des Droits Humains.
4 Cet article s'inspire largement du cours de Gouvernance de l'Internet- E-gouvernement de la professeure Elise Degrave, dispensé dans le Master de spécialisation en droit de l'internet (DTIC) à l'UNamur, durant l'année académique 2022-2023.
5 A. Sente, « Reconnaissance faciale : une enquête cinglante sur l'usage du logiciel Clearview par la police », Le Soir, 9 mars 2022.
6 Plusieurs pages du site de la Fédération Wallonie-Bruxelles sont dédiées à expliquer le fonctionnement de l'algorithme mettant en œuvre le décret inscription : https://inscription.cfwb.be/lalgorithme-doptimalisation-des-preferences/, consulté le 19 mai 2023.
7 N. Havermans et T. Wauters, « Simulatie op het toewijzingalgoritme in het secundair underwijs », *SONO*, OL3.2/2, 2020.
8 E. Degrave, « The Use of Secret Algorithms to Combat Social Fraud in Belgium », *European review of digital administration & law*, vol. 1, no. 1-2, 2020, pp. 167-178.
9 Voy. la loi programme du 13 mai 2016 modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale. A ce sujet, voy. E. Degrave, « Contrôle des assurés sociaux et profilage dans le secteur public » J.T., 2015, pp. 517-519.
10 Voy. C. Berthélémy, « Eurodac Database repurposed to surveil migrants », *EDRI*, accessible sur : https://edri.org/our-work/eurodac-database-repurposed-to-surveil-migrants/
11 L. Cluzel, Cours-Conférence donnée dans le cadre de la Chaire Francqui en E-gouvernement de l'UNamur, 10 mars 2023.

permis de peser leurs avantages et inconvénients. Ils doivent également être proportionnés par rapport au but poursuivi. Or, en étant bien souvent présentés comme une simple modernisation de l'administration papier, ces algorithmes n'ont, en réalité, presqu'aucune existence en droit, empêchant les pouvoirs judiciaire et législatif d'exercer un quelconque contrôle.

En outre, le secret qui entoure les algorithmes est problématique au regard du devoir de l'administration de **motiver** ses décisions. Autrement dit, les citoyens doivent être en mesure de comprendre les motifs qui sous-tendent les décisions qui les visent, et les agents de l'administration doivent être en mesure de les leur expliquer. Comment atteindre cet objectif quand on ignore l'existence même d'algorithmes dans le processus décisionnel ?

LE CONTRÔLE ALGORITHMIQUE DE LA FRAUDE SOCIALE

Les problèmes réels dans l'utilisation de ces technologies sont plus nombreux qu'on pourrait le croire. À cet égard, le scandale qui a éclaté aux Pays-Bas est très parlant. Les faits sont les suivants. À partir de 2013, le gouvernement néerlandais décide de s'attaquer davantage aux fraudes aux allocations familiales en se dotant d'un algorithme qui attribue pour chaque citoyen·ne un score de risque en fonction de la probabilité que sa demande d'aide sociale soit frauduleuse. Cet algorithme fonctionne en « boîte noire », c'est-à-dire que personne n'en connait véritablement le fonctionnement. Rapidement, l'administration, suivant aveuglément les préconisations des algorithmes anti-fraude, se met à exiger toujours plus de justificatifs de la part de certain·es allocataires, souvent d'origine étrangère ou vivant dans des quartiers défavorisés. Se voyant dans l'impossibilité de prouver ce que les autorités exigeaient, ces derniers ont dû faire face à des demandes de remboursement d'allocations pouvant s'élever à plusieurs dizaines de milliers d'euros. Au final, entre 25 000 et 35 000 personnes ont été victimes de cette pratique et ont fini noyées sous les dettes[12]. À la suite du scandale, une autorité de contrôle des algorithmes a été instaurée. Depuis début 2023, elle s'assure que les systèmes utilisés par les organismes publics néerlandais respectent les droits humains et qu'ils soient consignés dans un registre public[13].

Un système identique est-il à l'œuvre en Belgique ? Depuis 2005, l'administration belge s'est dotée de l'outil OASIS (Organisation Anti-fraude des Services de l'Inspection Sociale), un algorithme qui utilise les données de différentes administrations fédérales (ONSS, ONEM, SPF Sécurité Sociale, ...) afin de détecter les comportements frauduleux des allocataires sociaux. Problème : c'est l'administration elle-même qui a développé l'outil, sans aucun encadrement juridique, lui permettant ainsi d'éviter un contrôle du Parlement et de la justice. À cause de cette opacité, il est impossible de savoir si ce système est aussi discriminatoire que son homologue néerlandais, sauf à attendre qu'un scandale ne vienne tout dévoiler au grand jour[14].

12 Voy. not. le rapport d'Amnesty international, Xenophobic Machines, 25 octobre 2021, accessible ici :https://www.amnesty.org/en/documents/eur35/4686/2021/en/
; A. Eychenne, « Aux Pays-Bas, un algorithme discriminatoire a ruiné des milliers de familles », Mediapart, 11 novembre 2022, accessible sur https://www.mediapart.fr/journal/international/111122/aux-pays-bas-un-algorithme-discriminatoire-ruine-des-milliers-de-familles?userid=18214e0f-b200-48b4-af66-4e0888cc18c9

13 L. Bertuzzi, traduction d'A. Riffaud, *Les Pays-Bas prennent les devants en matière de supervision des algorithmes*, accessible sur : https://www.euractiv.fr/section/economie/news/les-pays-bas-prennent-les-devants-en-matiere-de-supervision-des-algorithmes/

14 E. Degrave, propos receuillis par P. Laloux, Le Soir, 22 mars 2021, accessible sur https://www.lesoir.be/362211/article/2021-03-22/elise-degrave-aujourdhui-letat-profile-deja-les-belges

La réponse normative en Belgique et en Europe

En septembre 2021, une loi a été proposée en Belgique afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration[15]. L'intention est bonne, mais comme souligné dans l'avis de l'Autorité de Protection des Données, la transparence visée par le projet se limite à révéler le code source de l'algorithme. Même si c'est un bon début vers davantage de transparence, on peut se demander si cette solution sera suffisante pour permettre aux citoyen·nes de comprendre le dispositif technique. La question se pose d'autant plus pour des algorithmes complexes comme ceux de *machine learning*[16]. Comment faire si la publicité ne suffit pas ?

Depuis lors, le 10 février 2023, le Sénat a voté une intéressante proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes[17]. Curieusement, cette initiative a fait peu de bruit autour d'elle, alors qu'elle est particulièrement intéressante dans le contexte actuel.

Par ailleurs, très récemment, le 11 mai 2023, le Parlement Européen a trouvé un accord sur la première législation qui encadrera l'intelligence artificielle[18], l'*AI Act.* Lorsque des systèmes impactent l'exercice des droits et libertés des individus, ils rentrent dans la catégorie des risques élevés, imposant à leurs développeur·euses de respecter certaines exigences de qualité des données d'entrainement, de transparence, et un cadre qui permet une supervision humaine et une responsabilité suffisante. Désormais les autorités qui feront l'usage d'IA à haut risque devront effectuer et publier une analyse d'impact au regard des droits fondamentaux avant de les déployer.

Conclusion

Le secret qui entoure actuellement les algorithmes en Belgique est source d'inquiétude et ne le sera encore que davantage au fur et à mesure que de tels dispositifs se déploieront au sein de l'administration et seront utilisés pour prendre des décisions aussi importantes que l'identification de fraudeur·euses, le refus de droits, le choix d'une école.
Certes, le projet de règlement européen sur l'intelligence artificielle propose des pistes intéressantes. Mais, outre le fait qu'il ne sera pas en vigueur dans l'immédiat, encore faudra-t-il espérer qu'il soit réellement effectif.
En attendant, n'oublions pas que le droit belge peut d'ores et déjà être mobilisé par les avocat·es, les magistrat·es, les associations, les citoyen·nes, pour amener les pouvoirs publics à lever le voile sur les dispositifs algorithmiques et identifier, le cas échéant, leurs effets néfastes. Plutôt que d'attendre qu'un nouveau scandale éclate au grand jour, on ne peut qu'espérer que la Belgique prenne les choses en main, en rejoignant les Pays-Bas dans l'équipe des « bons élèves européens ». À cet égard, la création d'une autorité de contrôle comme celle que l'on retrouve aux Pays-Bas est une idée intéressante pour travailler de concert avec l'Autorité de Protection des Données dans le contrôle effectif des outils algorithmiques.

15 Proposition de loi modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par l'administration, *Doc.*, Ch., 55, 2020-2021, n°1904/001.
16 Avis de l'Autorité de Protection des Données n° 157/2021 du 10 septembre 2021.
17 Proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes, *Ann. Parl.*, Sén., 2022-2023, séance du 10 février 2023, n°7-328/4,.
18 Communiqué de presse du Parlement Européen, « AI Act: a step closer to the first rules on Artificial Intelligence », accessible sur : https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence