Numérisation de l’administration publique

Degrave, Elise

Published in:
Permanences critiques

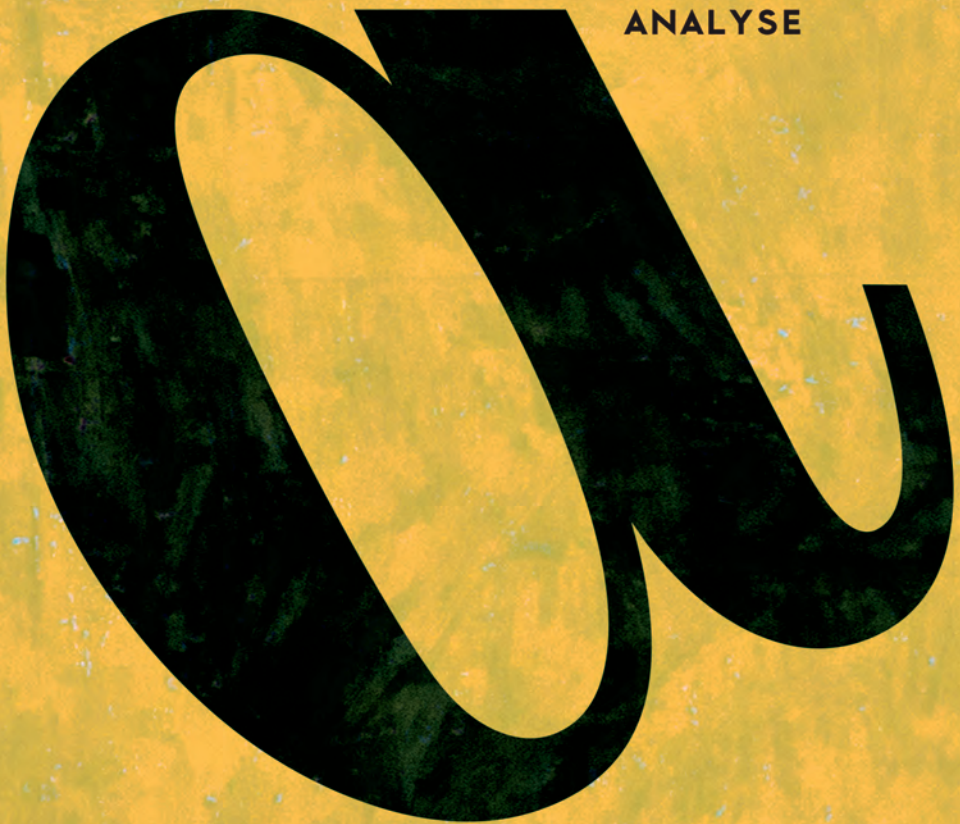
Publication date:
2023

Document Version
le PDF de l'éditeur

NUMÉRISATION DE L'ADMINISTRATION PUBLIQUE : ALLIER TECHNOLOGIE ET DROITS HUMAINS

ÉLISE DEGRAVE

ANALYSE



Des droits octroyés automatiquement, des croisements de données à caractère personnel et des algorithmes "anti-fraude" pour cibler les fraudeurs potentiels, la suppression de guichets humains pour des services publics "100% en ligne" d'ici 2030, sont autant de signes d'une accélération vers le "tout numérique" dans la relation entre le citoyen et l'État. Si les outils numériques, quand ils fonctionnent, offrent effectivement des avantages en termes d'efficacité et de flexibilité, ils peuvent à certains égards s'apparenter à des voitures sans ceinture de sécurité lancées en dehors de tout code de la route. Pour éviter le crash, il est urgent de ralentir, d'en revenir aux piliers de l'État de droit et de réfléchir ensemble à la définition d'une régulation à la hauteur des enjeux sociétaux en présence.

1. RALENTIR POUR RÉFLÉCHIR

« Numérique », « intelligence artificielle », « automatisation », « croisement de données », « efficacité », « économies », sont des mots qui imprègnent le quotidien et accompagnent ce qui semble bien être désormais une accélération vers le « tout numérique », comme en attestent notamment certaines décisions politiques qui modulent le rapport entre le citoyen et l'État dans le cadre de l'administration numérique. Entre autres exemples, la « boussole numérique » de la Commission européenne indique que les services publics seront « 100% en ligne » d'ici 2030, sans prévoir corollairement le maintien de guichets humains.

Pourtant, peut-on vraiment considérer qu'il doit y avoir une « transition numérique », au sens d'un basculement inéluctable à terme vers une société numérique, comme il y a une « transition écologique » ? Si la seconde est une évidence, au risque de mettre nos vies en péril, on perçoit plus difficilement le danger lié à un ralentissement du rythme vers le « tout numérique », voire un renoncement à cet objectif.

Au contraire. La vitesse actuelle de la numérisation est dangereuse en ce qu'elle nous prive du temps de la réflexion pour réguler adéquatement les technologies qui impactent tous les citoyens n'ayant d'autres choix que de s'y soumettre. Si nous souhaitons que ces outils et pratiques financés par l'argent public subsistent à long terme, il est urgent de ralentir. Et de réfléchir à la manière dont on peut associer la performance des outils numériques à leur durabilité, non seulement écologique, mais aussi juridique. En effet, aujourd'hui, on s'inquiète de voir que la performance technologique prend le pas sur le débat politique - souvent appauvri en la matière - et l'encadrement juridique – bien souvent insuffisant. Au final, la protection des droits humains est menacée et, avec elle, la démocratie et l'État de droit.

Les lignes qui suivent abordent la raison d'être du droit du numérique (I.), soulignent plusieurs inquiétudes dans les faits (II.) et évoquent quelques pistes de solution pour allier l'efficacité des technologies et le respect des droits humains dans l'État de droit numérique (III.).

I. LA RAISON D'ÊTRE DU DROIT DU NUMÉRIQUE

2. LE JURIDIQUE, CONDITION D'ÉPANOUISSEMENT DU NUMÉRIQUE

Le droit du numérique, entendu comme l'ensemble des règles juridiques encadrant la mise en place des outils numériques, fixe des balises pour éviter un « far west » numérique, en veillant notamment à ce que les outils soient mis en place dans le respect des droits de chacun.

En d'autres termes, le droit n'entend pas freiner l'enthousiasme technologique, mais bien lui permettre de trouver sa place, de manière pérenne, au sein d'une société qui, pour s'épanouir, doit notamment éloigner le chaos en organisant un équilibre des forces entre les différents protagonistes. En l'occurrence, cela signifie qu'une attention particulière doit être portée notamment à la réciprocité des avantages offerts par la technologie. En d'autres termes, l'administration numérique doit bénéficier tant à l'État qu'aux citoyens (tous les citoyens…). Et puisque l'administration utilise les technologies pour renforcer l'efficacité de son action, cette même technologie doit être organisée au bénéfice des individus, pour faciliter notamment l'exercice de leurs droits. C'est l'idée que « *dans une démocratie, les citoyens ne doivent pas avancer à pieds pendant que les autorités conduisent des limousines*[1] ».

3. LES GARANTIES JURIDIQUES CONCERNÉES

Chacun peut se prévaloir de droits à l'égard des outils numériques. Il s'agit même de droits fondamentaux, consacrés dans notre Constitution.

Ainsi, le *droit à la protection de la vie privée* (article 22), complété par le Règlement européen général sur la protection des données (RGPD), encadre strictement l'usage que l'État peut faire des données que chacun lui confie obligatoirement. Par exemple, seules les données nécessaires à l'exercice des missions de service public peuvent être réclamées, et il ne peut être question de les réutiliser ensuite pour n'importe quelle raison. Le législateur a également l'obligation de fixer, dans des lois, des règles très claires en la matière. Nous y reviendrons.

En outre, le *droit à l'égalité et à la non-discrimination* (articles 10 et 11) impose de veiller à ce que le numérique ne porte pas préjudice à certaines catégories de la population. Ce constat pose question à l'heure du « tout numérique » qui risque de renforcer davantage la situation de vulnérabilité de certaines personnes et de rendre plus fragiles des catégories de la population qui ne le sont pas encore nécessairement.

Le *droit à la transparence administrative* (article 32) peut être mobilisé pour faire la lumière sur les outils utilisés par l'État pour croiser les données des citoyens, par exemple. On songe notamment aux algorithmes du secteur public, ces formules mathématiques qui jouent un rôle de plus en plus décisif dans la prise de décision individuelle et dont on sait pourtant très peu de choses.

1 Schartum Dag Wiese, « Access to Government-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology*, 1998/1, §7.1. (traduction libre).

4. LA NÉCESSITÉ D'UN DÉBAT ET D'UNE RESPONSABILITÉ POLITIQUE CLAIRE.

Certes, s'agissant de la technique, quand on peut, on veut… Il peut donc être tentant d'aller rapidement de l'avant. Mais le numérique doit être soumis au juridique. Ce n'est alors que quand on veut, au terme d'un débat démocratique, que l'on peut. En d'autres termes, ce qui est technologiquement faisable n'est pas nécessairement démocratiquement acceptable. Pour s'en rendre compte, il importe de revenir aux piliers de l'État de droit qui protègent le citoyen d'une administration toute puissante, une administration qui, emportée par la rapidité technologique, serait hors la loi, incompréhensible et incontrôlable[2].

Un pilier fondamental de l'État de droit à l'ère du numérique est l'exigence de légalité. Découlant notamment de l'article 22 de la Constitution qui, rappelons-le, protège la vie privée de chacun, l'exigence de légalité impose au législateur d'encadrer chaque outil numérique dans une loi accessible au public et rédigée clairement, pour que chacun puisse comprendre ce qu'il advient des données qu'il confie à l'État.

Par exemple, faut-il mettre les empreintes digitales sur la carte d'identité électronique ? Est-il pertinent d'utiliser les données de consommation d'eau pour identifier la fraude au domicile des allocataires sociaux ? Peut-on utiliser les données des réseaux sociaux pour lutter contre la fraude fiscale ? Est-il prudent de recourir à un algorithme[3] pour lutter contre le travail au noir dès lors que cet algorithme n'est pas contrôlé et qu'on ignore comment il a été paramétré ? Ce sont quelques exemples d'usages de technologies ayant un impact sociétal fort, puisqu'ils concernent toute la population, et qu'ils sont rendus possibles par la réutilisation des données à caractère personnel de chacun.

Vu leur importance, ces questions, loin de se limiter à de la configuration technique, doivent être soumises à la réflexion et aux décisions des députés, à l'occasion d'un débat éclairé par des experts et des professionnels

2 À ce sujet voir. Degrave Elise, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014, accessible ici : https://researchportal.unamur.be/fr/studentTheses/le-gouvernement-et-la-protection-de-la-vie-priv%C3%A9e. Pour une conférence récente à ce sujet, voy. Cour de cassation de France, « Intelligence artificielle et administration publique numérique », 20 octobre 2022, avec les professeures Lucie Cluzel (Paris-Nanterre), Elise Degrave (UNamur), Daniel Agancinsky (membre du Défenseur des droits en France) et Simon Chignard (consultant) accessible ici : https://www.youtube.com/watch?v=ppeDpCBYOkk&t=3909s.

3 Un algorithme peut être défini comme un ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. (Dictionnaire Larousse). Pour des cas d'application dans l'administration belge, voir Degrave Elise, « Les citoyens contrôlés via leurs données Covid ? Le 'datamatching' et le 'datamining' utilisés par l'État. » *Journal des Tribunaux*, 2021, pp. 125-128.

du terrain. Ce débat devra aussi être éclairant pour la population, notamment grâce au relais qui en sera fait via les médias.

Ce débat devra mener à l'adoption d'une loi qui identifie clairement les éléments essentiels de ces traitements de données (quelles données, quels usages de celles-ci, quels objectifs poursuivis, etc.), en ce compris les autorités responsables de ces outils. Par exemple, la norme encadrant un outil de lutte contre la fraude en matière sociale pourrait identifier le Ministre du Travail en tant que responsable de cet outil et de ses conséquences, notamment en cas de « bug ».

En effet, on entend dire parfois qu'« il faut mettre le numérique devant ses responsabilités ». Or, le numérique n'est qu'un outil. En réalité, ce sont les responsables politiques prenant la décision de recourir aux technologies qui doivent être mis devant leurs responsabilités. Il ne faudrait donc pas que ceux-ci se réfugient derrière l'opacité et la complexité de l'outil par crainte de devoir endurer les conséquences massives d'un bug technique dans les outils numériques au service de l'État…

Corollairement au travail des députés, la norme en projet devra être soumise à des contrôles juridiques. Celui de l'Autorité de protection des données et de la section de législation du Conseil d'État, deux autorités publiques chargées de rendre un avis sur le texte, dans l'idée d'aider le Parlement à l'améliorer avant son adoption.

Une fois la norme adoptée, le droit organise sa propre contestation en permettant aux personnes concernées d'introduire un recours en annulation contre les normes inconstitutionnelles devant la Cour constitutionnelle ou devant le Conseil d'Etat et d'obtenir, le cas échéant, l'invalidation desdites normes et la cessation des dispositifs techniques litigieux. En d'autres termes, si les balises juridiques ne sont pas respectées lors du déploiement de l'administration numérique, les outils et pratiques mis en place devront être invalidés, causant alors perte de temps, d'argent, d'énergie ainsi que de possibles dégâts sur le plan humain.

II. INQUIÉTUDES DANS LES FAITS

5. SOLUTIONNISME TECHNOLOGIQUE ET TECHNOCRATIE

Concrètement, depuis plusieurs années, on est poussé dans le dos par le fantasme du solutionnisme technologique, l'idée que le numérique serait la solution à tout. Souvent, cela se passe comme suit. Des consultants frappent aux portes des cabinets ministériels, des administrations, des institutions, en proposant une solution « qui marche ». Du côté des autorités, cela passe

pour une simple « modernisation » de l'administration, qui nourrit l'image d'un État « branché » et l'idée d'un progrès social. Dans l'urgence et parmi une multitude de dossiers à traiter, l'outil est mis en place, parfois même sans que les marchés publics octroyés aux prestataires techniques ne cadenassent suffisamment les pratiques. C'est d'ailleurs ce que regrettent certains consultants soucieux notamment de la protection des données personnelles qu'ils sont chargés de manipuler.

On est là face au phénomène de la technocratie, le pouvoir de la technique, qui se place en concurrence de la démocratie. Finalement, du développeur informatique ou du député, qui décide réellement ?

Pourtant, il ne s'agit pas d'une simple modernisation de l'administration, comme le serait le changement des imprimantes… Ces outils ont un rôle déterminant pour décider de l'octroi ou du refus d'allocations chômage, d'un logement social, d'une bourse d'étude, de l'identification de possibles fraudeurs, etc.

Il est donc nécessaire de veiller à un encadrement juridique rigoureux et un débat politique minutieux autour de ces outils à l'impact sociétal majeur.

Or, actuellement, le manque d'encadrement juridique et de débat politique entourant ces outils créent une situation inquiétante. On songe par exemple au flou entourant le profilage des citoyens, via les techniques de « datamatching[4] » et de « datamining[5] », et l'utilisation d'algorithmes. Le « datamatching » et le « datamining » sont des techniques informatiques applicables à des données. Le « datamatching » est la première étape du processus, qui consiste à « croiser » les données, c'est-à-dire les rassembler et les comparer entre elles. La seconde étape est le « datamining ». On applique aux données des algorithmes qui vont induire de ces données des informations nouvelles, comme le ferait une boule de cristal. Cela permet de réaliser du profilage[6], c'est-à-dire de prédire la probabilité, pour chaque individu, d'adopter le comportement de tel profil d'individu (le profil de fraudeur par exemple[7]). Ce type de profilage est utilisé notamment pour

4 En français « couplage de données ».

5 En français « extraction de données ».

6 L'article 4.4 du RGPD définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

7 En guise d'exemple simple, prenons le cas de John, dont les données fiscales montrent qu'il gagne 2.000 euros par mois. Or, ses données à la DIV montrent qu'il détient 7 Ferrari neuves. Le Registre national indique qu'il est propriétaire de deux châteaux. Les algorithmes « anti-fraude » vont cibler John. Il sera rattaché à la catégorie des présumés fraudeurs fiscaux et sociaux et un contrôle fiscal et/ou social sera encouragé.

identifier les fraudeurs sociaux dans la lutte contre le travail au noir ou encore dans le contrôle des allocataires sociaux au départ de leurs données de consommation d'eau, de gaz et d'électricité[8].

6. LE CAS DES ALGORITHMES SECRETS

Entre autres préoccupations pour les droits humains, soulignons qu'en Belgique, les algorithmes utilisés par l'État sont, à quelques rares exceptions près, secrets, non encadrés par des lois, et non contrôlés. On ignore qui les crée, selon quelles instructions, s'ils sont contrôlés et par qui. On ne peut donc exclure que ces algorithmes soient affectés de défauts, appelés « biais », qui pourraient entraîner des discriminations sur la base de la situation financière ou sur l'origine ethnique, notamment.

Le manque d'encadrement des algorithmes du secteur public notamment a déjà mené à de grands scandales à l'étranger. Aux Pays-Bas, par exemple, ce qui est désormais appelé « le scandale des allocations familiales » a révélé que des milliers de familles, en particulier des familles d'origine étrangère, ont été accusées à tort de fraude et injustement contraintes de rembourser des sommes importantes à l'État. Cela provoqua des divorces, des suicides, des situations de pauvreté conduisant à expulser des personnes de leur logement et à retirer des enfants de leur famille. En réalité, les algorithmes utilisés pour lutter contre la fraude avaient été mal paramétrés, insuffisamment contrôlés, ce qui provoqua ces conséquences dévastatrices humainement. En raison de ce problème technique invisible qui créa des discriminations très concrètes et dramatiques, le gouvernement des Pays-Bas chuta en janvier 2021[9]. En France, les algorithmes de la Caisses des Allocations familiales (« Caf ») sont actuellement sous le feu des projecteurs[10]. En Belgique, l'outil OASIS notamment, qui organise du profilage pour lutter contre le travail au noir, est toujours très problématique[11].

En dehors de ces scandales, au quotidien, les algorithmes et de manière générale, les processus qui visent à automatiser l'octroi des droits et le

8 Loi 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.

9 Voir notamment le rapport d'Amnesty international, *Xenophobic Machines,* 25 octobre 2021, accessible ici : https://www.amnesty.org/en/documents/eur35/4686/2021/en/.

10 La Quadrature du Net, « Notation des allocataires : fébrile, la CAF s'enferme dans l'opacité », 22 décembre 2022, accessible ici : https://www.laquadrature.net/2022/12/23/notation-des-allocataires-febrile-la-caf-senferme-dans-lopacite/.

11 Degrave Elise, « The use of secret algorithms to combat social fraud in Belgium », *European Review of Digital Administration & Law,* 2020, pp. 167-177 accessible ici: http://www.aracneeditrice.it/pdf2/9788825538960l5.pdf.

contrôle des citoyens via des outils numériques soulèvent des problèmes. Entre autres difficultés, des erreurs dans les données utilisées peuvent provoquer un refus de droit et aggraver le phénomène de « non-recours au droit[12] ». Ainsi, s'agissant de l'automatisation des droits, même de tels croisements de données vertueux peuvent générer des inégalités. Si une donnée du processus est erronée, en bout de chaîne, le citoyen se verra refuser la réduction escomptée, alors même qu'il est dans les conditions légales pour l'obtenir. Et l'autorité sera bien en peine d'en expliquer la raison : actuellement, retrouver une erreur dans une donnée équivaut à chercher une aiguille dans une botte de foin, tant il reste à faire pour que la transparence dans l'utilisation des données des citoyens soit une réalité.

III. STIMULER LA DÉMOCRATIE ET CONSTRUIRE L'ÉTAT DE DROIT NUMÉRIQUE

7. MORATOIRE ET PISTES D'ACTION

Compte tenu de ces éléments, il est urgent de stimuler la démocratie malgré l'opacité et la distance créés par les technologies, et de construire ensemble l'État de droit numérique. À cette fin, il pourrait être judicieux de s'intéresser à une demande portée par plusieurs spécialistes internationaux du numérique[13], prolongée en Belgique par une cinquantaine d'académiques[14], celle d'un moratoire dans le développement de l'intelligence artificielle et, de manière générale, des outils numériques ayant un impact sur la société.

En Belgique, ce moratoire pourrait être appliqué au déploiement des outils numériques qui touchent à la relation entre le citoyen et l'État, le temps d'adopter une régulation juridique plus adéquate.

Trois pistes concrètes pourraient être étudiées par les responsables politiques afin d'être concrétisées dans des normes juridiques.

Premièrement, pour garantir effectivement la protection de la vie privée de chaque citoyen tout en luttant contre les discriminations provoquées par le numérique, chaque dispositif devrait faire l'objet d'une *analyse d'im-*

12 À ce sujet voir notamment Dumont Daniel, « Le phénomène du non-recours aux prestations, un défi pour l'effectivité (et la légitimité) du droit de la sécurité sociale », *TSR-RDS*, 2020/3, n° 19 ; Noël Laurence, « Non recours aux droits et précarisations en Région bruxelloise », 2021, accessible ici https://journals.openedition.org/brussels/5569.

13 Le Soir, « Elon Musk et des centaines d'experts réclament une pause dans l'IA », 29 mars 2023, accessible ici https://www.lesoir.be/504223/article/2023-03-29/elon-musk-et-des-centaines-dexperts-reclament-une-pause-dans-lia.

14 La Libre, « Le Chatbot Eliza a brisé une vie : il est temps d'agir face à l'IA manipulatrice », 29 mars 2023, https://www.lalibre.be/debats/2023/03/29/le-chatbot-eliza-a-brise-une-vie-il-est-temps-dagir-face-a-lia-manipulatrice-BSGGRV7IBRDNROO33EWGFVMWAA/.

pact avant sa mise en place, et avant le débat démocratique au Parlement, permettant de mesurer notamment l'impact de ces dispositifs sur les droits humains et de nourrir le travail critique des députés qui auront à décider de recourir ou non à ces outils, des Ministres qui devront en endosser la responsabilité et des citoyens qui doivent être éclairés sur les outils qui participent substantiellement à la gouvernance étatique.

Deuxièmement, pour obvier au risque d'erreurs en chaîne dans les décisions fondées sur des échanges de données, la transparence des traitements de données devrait être renforcée en mettant en place *un « tracking »* des données, à l'image de ce qui se fait lorsque l'on commande un produit sur internet et que le parcours du produit est disponible en temps réel. Il y va du respect du droit à l'égalité et la non-discrimination, du droit à la vie privée et du droit à la transparence administrative.

Troisièmement, puisque les biais algorithmiques mettent en péril le droit à l'égalité et à la non-discrimination et peuvent provoquer des conséquences humaines désastreuses, ils devraient être contrôlés, en mettant en place *une « AFSCA » des algorithmes*, autorité indépendante spécifiquement dédiée à cette mission. La recette de Coca-Cola est secrète, mais les éléments essentiels de sa composition sont connus et contrôlés. Il doit en être de même des algorithmes afin d'en étudier l'impact sociétal et corriger les éventuels effets injustes ou disproportionnés.

Ce sont là quelques pistes de réflexion pour inciter, on l'espère, à la stimulation de la démocratie et de l'État de droit à l'ère du numérique, en consacrant un subtil équilibre entre la performance de la technologie et le respect des droits humains, grâce à une indispensable vivification du débat politique et de l'encadrement juridique des outils techniques.