

Intelligence artificielle et services publics – le rôle des autorités publiques au service de la « troisième voie » dessinée par la Commission européenne¹

Yves Poulet² et Noémi Bontridder³

Citer cette publication : Yves Poulet et Noémi Bontridder, « Intelligence artificielle et services publics – le rôle des autorités publiques au service de la « troisième voie » dessinée par la Commission européenne », Revue générale du droit, 2022.

¹ Cet article n'aurait pu être écrit sans l'appui de l'Agence du Numérique de la Région Wallonne (AdN) (Belgique). Il s'inscrit dans le cadre d'un rapport commandité au CRIDS/NADI et rédigé par les deux auteurs sur le cadre réglementaire et éthique d'une IA au service des autorités publiques wallonnes.

² Professeur émérite à la Faculté de droit de Namur – Co-président du Namur Digital Institute (NADI), Professeur associé à l'UCLille, Membre de l'Académie royale de Belgique.

³ Chercheuse au CRIDS (Université de Namur).

« *L'intelligence artificielle se définit comme le contraire de la bêtise naturelle.* »
(Woody Allen)

Introduction

L'Europe poursuit, c'est du moins la volonté des autorités européennes et en particulier de la présidente de la Commission, une troisième voie de développement de l'intelligence artificielle (ci-après « IA ») et entend par cette troisième voie décrocher le *leadership* mondial de cette technologie profondément innovante par les applications qu'elle autorise. L'IA est devenue un '*buzzword*' et mille vertus lui sont attribuées. Ainsi, on brandit les avancées d'une recherche médicale salvatrice de vies, la généralisation des voitures 'intelligentes' qui réglera nos problèmes de sécurité et de mobilité, l'utilisation des outils de reconnaissance faciale qui nous protégera des terroristes, le développement des villes 'intelligentes' au service de leurs citoyens, etc. Cette troisième voie baptisée '*excellence et confiance*' (*Excellence and Trust*) constituera l'avant-propos de notre exposé.

La description de la stratégie européenne en matière d'IA amène à comprendre le rôle essentiel qui est réservé aux services publics. Nous procéderons en deux temps. Le premier temps montre comment les données générées par les entités publiques et privées constituent ce qui est désormais le '*new oil*'⁴, nécessaire au développement de ressources informationnelles, condition de la génération d'applications d'IA tant dans le secteur privé ... que public. L'ajout « que public » est important et constitue une originalité de l'approche européenne. Si la mise à disposition des données du secteur public au bénéfice du secteur privé est consacrée depuis plus d'une dizaine d'années en Europe, est à l'inverse neuve la stratégie qui au nom de l'intérêt public consacre ce qu'il est convenu

4 Voy. le document de l'EPRS : *Is data the new oil? Competition issues in the digital economy*, PE 646.117, janvier 2020, disponible en ligne sur [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf) (consulté le 25 mai 2021).

d'appeler le '*reverse PSI*', c'est-à-dire le transfert de données du secteur privé vers le secteur public.

Le second temps souligne un versant différent de la politique européenne en ce qui concerne l'apport possible des services publics au développement de technologies d'IA. Les services publics se doivent de concevoir et d'exploiter des outils d'IA au service de l'intérêt général et des citoyens. À ce propos, nous examinerons non seulement les outils mis à disposition du secteur public pour encourager l'adoption d'outils d'IA, mais également quelques éléments du cadre réglementaire spécifique au service public, dans lequel ce développement aura lieu.

I. Avant-propos – la troisième voie européenne : « excellence et confiance »

Cette option européenne d'une troisième voie, sans doute préparée par la précédente Commission européenne⁵ et le Parlement d'alors⁶, est désormais clairement affirmée par la nouvelle Commission⁷ et sa présidente. Elle se présente comme une stratégie clairement énoncée et progressivement mise en œuvre à travers des textes qui se suivent à un rythme effréné⁸. Elle peut se résumer comme suit : « *[L]e leadership mondial*

5 Voir notamment les textes suivants : *Coordinated Plan on the Development and Use of Artificial Intelligence Made in Europe*, décembre 2018 (coopération entre pays membres sur 4 points : augmentation des investissements, formation, création de gisements de données et confiance).

6 Cf. en particulier la Résolution du 12 février 2019 sur une politique industrielle globale sur l'intelligence artificielle et la robotique (2018/2088(INI)) (dite résolution Ashley Fox), disponible en ligne sur https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_FR.html (consulté le 25 mai 2021).

7 Commission européenne, *Livre blanc sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance*, COM (2020) 65 final, 19 février 2020, disponible en ligne sur https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf (consulté le 25 mai 2021).

8 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, Une stratégie européenne pour les données, 19 février 2020, COM(2020) 66 final, disponible en ligne sur https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.: « *The European data strategy aims to make the EU a leader in a data-driven society. Creating a single market for data will allow it to flow freely within the EU and cross sectors for the benefit of*

de l'Europe dans l'adoption des dernières technologies, la saisie des avantages et la promotion du développement d'une intelligence artificielle (IA) centrée sur l'humain, durable, sûre, inclusive et digne de confiance dépend de la capacité de l'Union européenne (UE) à accélérer, agir et aligner les priorités politiques et les investissements en matière d'IA »⁹. Il s'agit d'une troisième voie dans la mesure où l'Union européenne entend mener une politique de développement de l'IA fondée sur des principes différents de ceux qui fondent, d'une part, la politique américaine que, sans doute à tort, on résumera par un 'tout au marché' ou plus justement par la volonté de maintenir et de développer le *leadership* américain¹⁰ et, d'autre part, la politique chinoise marquée – mais sans doute sommes-nous proches de la caricature – par un interventionnisme de l'État et une IA au service de l'économie, de la gouvernance sociale par l'État et de la sécurité de ce dernier (voir en particulier et de manière emblématique, les applications sécuritaires de reconnaissance faciale)¹¹. Nous caractériserons cette 'troisième voie' par quelques axes stratégiques.

businesses, researchers and public administrations. People, businesses and organisations should be empowered to make better decisions based on insights from non-personal data, which should be available to all.)".

9 ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence, 21 avril 2021, COM (2021) 205 final, disponible en ligne sur <https://www.kowi.de/Portaldata/2/Resourcen/fp/2021-COM-AI-Annexes.pdf> (consulté le 25 mai 2021), p. 2 (traduction libre).

10 Le récent rapport du National Select Committee on AI publié le 1er mars 2021 et soumis au Président des Etats-Unis et au Congrès pour adoption, maintient la même position : « *The NSCAI Final Report presents an integrated national strategy to reorganize the government, reorient the nation, and rally our closest allies and partners to defend and compete in the coming era of AI-accelerated competition and conflict. It is a two-pronged approach. Part I, "Defending America in the AI Era," outlines the stakes, explains what the United States must do to defend against the spectrum of AI-related threats, and recommends how the U.S. government can responsibly use AI technologies to protect the American people and our interests. Part II, "Winning the Technology Competition," addresses the critical elements of the AI competition and recommends actions the government must take to promote AI innovation to improve national competitiveness and protect critical U.S. advantages* ». https://www.nsc.ai.gov/wp-content/uploads/2021/03/Final_Report_Executive_Summary.pdf (consulté le 25 mai 2021).

11 J. DING, *Deciphering China's AI dream - The context, components, capabilities, and consequences of China's strategy to lead the world in AI*, Centre for Governance of AI, Future of Humanity Institute, University of Oxford, Oxford, mars 2018, disponible en ligne sur https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf (consulté le 25 mai 2021); E. B. KANIA, *China's embrace of AI: Enthusiasm and challenges*, European Council on Foreign Relations, 6 novembre 2018, https://ecfr.eu/article/commentary_chinas_embrace_of_ai_enthusiasm_and_challenges/ (consulté le 25 mai 2021).

Le premier concerne le financement d'un investissement au profit d'un marché que l'on entend européen. L'annexe à la Communication « *Fostering a European Approach to Artificial Intelligence* », qui contient la mise à jour du plan coordonné de 2018, a été publiée par la Commission européenne le 21 avril 2021¹². Le plan 2021 annonce l'objectif d'atteindre progressivement un investissement public et privé de 20 milliards d'euros par an au cours de la décennie 2020-2030 et plaide énergiquement pour une meilleure synergie des instruments de financement au niveau national et au niveau européen entre des fonds de pure recherche et des fonds de coopération entre l'industrie et la recherche. Les autorités publiques doivent avoir à cœur la mise sur pied d'instruments tant réglementaires que d'appui au développement, par le secteur privé, de systèmes d'IA et ce notamment par une politique de financement, d'aide à la recherche, de fiscalité, etc. L'Europe, au-delà de ces mécanismes classiques, prône, en matière d'IA, la coopération européenne en matière de recherche et la mise à disposition d'une plateforme pour le développement de tests et d'expérimentation, en particulier à destination des petites et moyennes entreprises, des autorités publiques et dans les secteurs de l'environnement, de la santé, du secteur public, de la justice, de la mobilité et de l'agriculture.

Le deuxième axe stratégique promeut une politique de la donnée et de son partage. La politique européenne en faveur de l'IA souligne la valeur économique de la donnée, et la reconnaissance de cette dernière comme un '*new oil*'¹³ commande en effet une politique de libre circulation des données. A cet égard, le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne¹⁴ institue un cinquième principe de libre circulation :

12 ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *Fostering a European approach to Artificial Intelligence*, op. cit.

13 Cf. le très intéressant document de l'EPRS : *Is data the new oil? Competition issues in the digital economy*, op. cit.

14 Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union

celui portant sur les données non personnelles. Le texte de 2018 prône en particulier la disponibilité des données et le portage des données pour les utilisateurs professionnels.

Ce second axe de la politique européenne, qui souligne l'absolue nécessité du partage des données¹⁵, constitue un prérequis absolu pour la création de mégadonnées¹⁶ ou *Big data* proprement européennes, condition d'une émergence d'applications de l'IA. Cette politique d'encouragement au partage des données¹⁷, au sein et au-delà des secteurs¹⁸ mais également entre le public et le privé, s'explique par l'absence dans l'Union européenne de champions du *big data* que sont les plateformes américaines (les GAFAM) et chinoises (les BATX) et donc la nécessité de constituer ces *big data* européennes à partir des lieux de collecte privés ou publics, en

européenne, PE/53/2018/REV/1, JOUE, L 303, 28 novembre 2018, disponible en ligne sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2018.303.01.0059.01.FRA (consulté le 25 mai 2021), pp. 59–68.

15 Sur ce point, voy. les conclusions (pp. 6 et 7) du document EPRS : *Is data the new oil ? Competition issues in the digital economy*, op. cit.: « A widely debated method to address the competition concerns discussed above is to regulate the sharing of data, and even to make it mandatory in specified cases. As long as privacy and security are safeguarded, sharing data may indeed generate a broader social good. Pooling together the same type of, or complementary, data may enable firms to develop new or improved goods and services, and to base their algorithms on a broader, more meaningful basis. The relatively short history of the digital economy indicates that preventing data portability and inter-operability, which are essential prerequisites for data sharing, creates barriers to entry and limits competition ».

16 On connaît les 5V qui caractérisent ou plutôt doivent caractériser la qualité des mégadonnées. Ces 5V sont le Volume (le nombre de données à disposition), la Vitesse (de traitement afin d'offrir si possible des résultats en temps réel), la Variété (voix, données faciales, données transactionnelles, *web analytics*, textes, images, etc.), la Valeur (la fraîcheur, la pertinence des données) et la Vérité (pas de données subjectives) des données.

17 « Les données sont vitales pour le développement économique : elles constituent la base de nombreux produits et services nouveaux à l'origine de gains de productivité et d'efficacité dans l'utilisation des ressources dans tous les secteurs de l'économie, permettant de proposer des produits et des services plus personnalisés, d'améliorer l'élaboration des politiques et de moderniser les services publics. » Elles représentent une ressource essentielle pour les start-ups et les petites et moyennes entreprises (PME) aux fins du développement de produits et de services. La disponibilité de données est essentielle pour la formation de systèmes d'intelligence artificielle, avec des produits et services évoluant rapidement au-delà de la reconnaissance des caractéristiques et de la production de connaissances vers des techniques de prédiction plus sophistiquées et, partant, des décisions plus judicieuses ». Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions, Une stratégie européenne pour les données, op. cit., p. 3.

18 Ainsi, la Commission encourage la création de neufs espaces sectoriels communs de données (industrie manufacturière, environnement, mobilité, santé, finances, énergie, agriculture, administration publique, compétences) et intersectoriels. *Ibid.*, pp. 27-28.

créant des mécanismes vertueux de solidarité. Dans le cadre de cette politique, la Commission a pris diverses initiatives. Le lancement d'un *cloud* européen qui garantit aux utilisateurs la non-surveillance par les autorités policières ou de renseignement est sans doute à noter, alors que l'utilisation du *cloud* par nos entreprises reste à la traîne. La proposition de Règlement sur la gouvernance européenne des données (*Data Governance Act*) présentée le 25 novembre 2020¹⁹ mérite notre attention. Nous y reviendrons lorsqu'il s'agira d'analyser le rôle que l'Union européenne souhaite conférer aux services publics dans sa politique de l'IA mais notons dès à présent que « [7] *instrument vise à favoriser la disponibilité de données en vue de leur utilisation, en augmentant la confiance dans les intermédiaires de données et en renforçant les mécanismes de partage de données dans l'ensemble de l'UE* ». Quatre objectifs sont visés :

- « *la mise à disposition de données du secteur public en vue d'une réutilisation, lorsque de telles données sont soumises à des droits d'autrui (nous reviendrons sur ce point) ;*
- *le partage de données entre entreprises, contre rémunération sous quelque forme que ce soit ;*
- *permettre l'utilisation de données à caractère personnel avec l'aide d'un « intermédiaire de partage de données à caractère personnel », conçu pour aider les personnes physiques à exercer leurs droits au titre du règlement général sur la protection des données (RGPD) ;*
- *permettre l'utilisation de données pour des motifs altruistes ».*

Le troisième axe stratégique est sans doute le plus original mais également le plus difficile à réaliser. La volonté exprimée à de nombreuses reprises par les autorités européennes est de fonder le développement des outils et des applications d'IA sur deux valeurs : « *excellence et confiance* », selon le titre même du Livre blanc de l'Union européenne en matière d'IA (*White Paper*

19 Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, 25 novembre 2020, COM (2020) 767 final, disponible en ligne sur <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52020PC0767> (consulté le 25 mai 2021).

on AI) de février 2020²⁰. Lors de l'annonce de ce Livre blanc, la Présidente de la Commission soulignait lors d'un point de presse : « *Nous voulons que l'application de ces nouvelles technologies soit digne de la confiance de nos citoyens [...] Nous encourageons une approche responsable de l'intelligence artificielle centrée sur l'humain* ». L'excellence s'appuie sur le développement d'une recherche scientifique de pointe que l'Union européenne entend financer à côté des financements de chaque État européen²¹. La confiance dans les applications de l'IA doit permettre l'acceptation sociale de celles-ci, nécessaire à leur développement. A cet égard, les textes européens constatent les risques inhérents aux algorithmes « *statiques et opaques* » et la nécessité de garantir, dès la conception, la transparence et l'explicabilité des algorithmes, afin d'empêcher toute discrimination liée à la prise de décision automatisée. Il est en outre recommandé de mettre en place des règles éthiques intégrant l'idée que l'IA est une « *technologie centrée sur l'humain* » qui est conçue comme un outil qui aide l'humain et qui est contrôlé par lui, et que ses applications doivent s'effectuer dans le respect des droits fondamentaux tels que la dignité, l'autonomie,

20 Commission européenne, Livre blanc sur l'intelligence artificielle, *op. cit.* En matière d'excellence, selon le résumé de la Commission elle-même, la Commission propose les mesures suivantes : « 1. Mettre en place un nouveau partenariat public-privé dans les domaines de l'IA et de la robotique ; 2. Renforcer les centres d'excellence en matière d'IA et les relier ; 3. Faire en sorte qu'au moins un pôle d'innovation numérique par État membre soit spécialisé en IA ; 4. Fournir davantage de financement au développement et à l'utilisation de l'IA, avec le soutien du Fonds européen d'investissement ; 5. Utiliser l'IA pour améliorer l'efficacité des procédures de marchés publics ; 6. Soutenir l'acquisition de systèmes d'IA par des organismes publics ».

En matière de confiance, la Commission propose de : « 1. Veiller à ce que la nouvelle législation sur l'IA tienne compte des risques mais n'entrave pas l'innovation ; 2. Exiger que les systèmes d'IA à haut risque soient transparents, traçables et sous contrôle humain ; 3. Donner aux autorités les moyens de vérifier la conformité des systèmes d'IA, tout comme elles le font avec les cosmétiques, les voitures ou les jouets ; 4. Veiller à ce que les ensembles de données ne soient pas entachés de biais ; 5. Lancer un débat à l'échelle de l'UE sur l'utilisation de l'identification biométrique à distance (ex.: reconnaissance faciale) ». Commission européenne, *Excellence et confiance dans le domaine de l'intelligence artificielle : façonner l'avenir numérique de l'Europe*, 2020, disponible en ligne sur <https://europe-en-sarthe.eu/wp-content/uploads/2020/03/Excellence-et-confiance-dans-le-domaine-de-IA.pdf> (consulté le 25 mai 2021).

21 Le récent document stratégique de la Commission (Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions : *Fostering a European approach to Artificial Intelligence*, *op. cit.*) donne le détail, pays membre par pays membre, des investissements nationaux en la matière (pp. 60 et s.).

l'autodétermination, la non-discrimination, et le respect de l'environnement et d'une démocratie fondée sur l'État de droit.

La responsabilité sociétale de tous les acteurs qui concourent au développement des outils d'IA est impliquée par le respect de ce cadre éthique. Le Livre blanc s'appuie notamment sur les travaux d'un groupe d'experts de haut niveau (GEHN IA) commandité par la Commission, ces travaux ayant abouti en avril 2019 à des recommandations éthiques pour une IA digne de confiance²² et plus récemment à la publication d'une liste reprenant les critères d'évaluation des sept caractéristiques d'une IA digne de confiance (ALTAI ou *Assessment List for Trustworthy AI*)²³. A cette impulsion éthique de la Commission et en pleine concertation avec cette dernière, le Parlement européen a entendu répondre par une résolution du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes²⁴. Le texte de la proposition de règlement mis sur la table le 21 avril 2021 par la Commission

22 GEHN IA (Groupe d'experts indépendants de haut niveau sur l'intelligence artificielle). Sur ce groupe et ses travaux, voy. <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> et notamment sa publication des *Lignes directrices en matière d'éthique pour une IA digne de confiance* (publiés le 8 avril 2019), disponible en ligne sur <https://op.europa.eu/fr/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1> (consulté le 26 mai 2021) ; voy. aussi la page <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> (consultée le 26 mai 2021).

23 Les sept critères dégagés par le GEHN IA dans ses lignes directrices sont les suivantes : Action humaine et contrôle humain ; Robustesse technique et sécurité ; Respect de la vie privée et gouvernance des données ; Transparence ; Diversité, non-discrimination et équité ; Bien-être sociétal et environnemental ; Responsabilité. Sur les méthodes d'évaluation et les critères à prendre en compte, voir le site de présentation de l'ALTAI : <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence>. Nous notons que ces critères et la méthodologie de l'ALTAI ont été évalués pendant une durée d'un an et ont reçu les apports de *l'AI Alliance*.

24 Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012(INL)) P9 TA (2020) 0275, disponible en ligne sur https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_FR.pdf (consulté le 26 mai 2021). Ce texte a reçu l'appui de la Commission européenne. Il est à noter que la Résolution contient une proposition de Règlement qui n'attend qu'à être reprise par les autres autorités de l'Union européenne.

européenne²⁵ nous apparaît plus pragmatique mais moins généreux que le texte parlementaire. Il s'agit bien, comme l'a affirmé Margrethe Vestager lors de la présentation de la proposition, de mettre en œuvre par ce texte les principes mêmes d'excellence et de confiance : « *[e]n matière d'intelligence artificielle, la confiance n'est pas un luxe mais une nécessité absolue. En adoptant ces règles qui feront date, l'UE prend l'initiative d'élaborer de nouvelles normes mondiales qui garantiront que l'IA soit digne de confiance. En établissant les normes, nous pouvons ouvrir la voie à une technologie éthique dans le monde entier, tout en préservant la compétitivité de l'UE. À l'épreuve du temps et propices à l'innovation, nos règles s'appliqueront lorsque c'est strictement nécessaire : quand la sécurité et les droits fondamentaux des citoyens de l'Union sont en jeu* ». Le but de la proposition est quadruple :

- « *ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;*
- *ensure legal certainty to facilitate investment and innovation in AI;*
- *enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;*
- *facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation* »²⁶.

Nous retenons du texte les définitions de l'IA et des acteurs. Ainsi, « *'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with* »²⁷. L'annexe I se réfère non seulement aux techniques de « *machine learning* » supervisé ou non incluant le *deep learning*, les approches dites symboliques

25 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, 21 avril 2021, COM (2021) 206 final, disponible en ligne sur <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN> (consulté le 26 mai 2021).

26 Exposé des motifs de la proposition de Règlement, p. 3.

27 Article 3 (1) de la proposition de Règlement.

fondées sur des systèmes experts (*logic and knowledge based*) et les approches statistiques comprenant les méthodes d'optimisation²⁸. Concernant les acteurs, la proposition de Règlement prend soin de distinguer les obligations des fournisseurs, des distributeurs, des importateurs, des utilisateurs opérant dans le cadre de leurs activités professionnelles, et des utilisateurs opérant dans le cadre d'activités privées²⁹. Ces distinctions sont utiles³⁰ car elles permettent, au-delà des nécessités d'interaction entre ces acteurs de la '*supply chain*', d'allouer à chacun des responsabilités précises.

Enfin, quelques mots sur le contenu de la proposition. Celle-ci entend établir un compromis entre les exigences légales et éthiques, traduisant les valeurs de l'Union et la nécessité de ne pas contraindre de manière exagérée le développement et l'initiative technologiques. Pour ce faire, le texte adopte une approche réglementaire strictement proportionnée, évolutive et fondée sur la distinction entre pratiques illégales de l'IA³¹ (art. 5), systèmes d'IA à haut risque (art. 6), systèmes d'IA à risque limité (art. 52) et systèmes d'IA à risque moindre (dont l'usage est libre). L'annexe III reprend la liste susceptible d'évolution de huit types de systèmes à haut risque³² : systèmes biométriques d'identification ; systèmes de gestion des

28 Ainsi, le concept regroupe des méthodes fondées tant sur des systèmes de rapprochement de données fonctionnant de manière plus ou moins autonomes et opaques et des systèmes fondés sur un raisonnement logique transparent. Il est clair que les risques liés à ces deux types de techniques et d'approche sont loin d'être les mêmes. Par ailleurs, la liste des techniques et méthodes est évolutive, la Commission étant, en vertu de l'article 4 et conformément à l'article 73, habilitée à adopter des actes délégués en vue de mettre à jour cette liste contenue dans l'annexe I.

29 Voy. les définitions à l'article 3 et leurs obligations respectives aux articles 16 à 29 de la proposition de Règlement.

30 Sans doute, eût-il été nécessaire d'ajouter à côté de la catégorie « fournisseur » (ou « développeur ») d'un système d'IA, celle de fournisseur d'un élément du système IA, tel que, le fournisseur des données ou des algorithmes sur lesquelles se base le fonctionnement du système. Des obligations de documentation, de qualité des données ou de non biais pourraient leur incomber.

31 Ainsi, les systèmes de manipulation par messages subliminaux, l'exploitation des vulnérabilités, l'utilisation par le secteur public de systèmes de « *social ranking* » entraînant de potentielles discriminations entre personnes ou groupes, de systèmes biométriques fonctionnant en temps réel et à distance, placés dans des endroits publics (par exemple, des systèmes de reconnaissance faciale).

32 On s'étonnera de la liste qui mélange des critères différents, tantôt basés sur le type de données (exemple : données biométriques d'identification), tantôt fondés sur le secteur en

infrastructures critiques ; applications dans le secteur de l'éducation et de la formation ; applications en matière d'emploi ; applications en ce qui concerne l'accès ou la jouissance de services publics ou de services privés essentiels ; systèmes utilisés par les forces de l'ordre ; systèmes utilisés en matière de migration ou de contrôle des frontières ; et systèmes d'administration de la justice. D'emblée, nous notons le rangement parmi les systèmes à haut risque de nombre d'applications du secteur public. Nous reviendrons sur ce point.

II. Pour une politique de la donnée et de l'IA propre aux services publics

Le partage de données, avons-nous dit, constitue un prérequis absolu pour la création de mégadonnées ou *Big data* proprement européennes, condition d'une émergence d'applications de l'IA. En la matière, le rôle des services publics, prôné par l'UE, est double. Premièrement, les autorités publiques doivent avoir à cœur la mise sur pied d'instruments tant réglementaires que d'appui au développement par le secteur privé de systèmes d'IA, et ce notamment par une politique de financement, d'aide à la recherche, de fiscalité, etc. En amont, comme nous le disions dans l'introduction, l'Europe promeut l'exploitation la plus large possible des données du secteur public par le secteur privé. Deuxièmement, les autorités publiques doivent promouvoir, en interne cette fois, l'utilisation d'outils d'IA au service de l'intérêt général et des citoyens³³. Ainsi, l'Europe

cause (exemple : le secteur financier), tantôt sur la finalité (recrutement de personnel, accès à des services publics ou privés essentiels), tantôt par une combinaison de plusieurs critères (exemple : dans le secteur éducatif, l'évaluation des étudiants). L'utilisation de tels critères rend la lecture et l'interprétation du texte difficile et peut poser problème. Ainsi, un système expert (IA symbolique) traditionnel qui traduirait en algorithmes les règles de délibération est un système à haut risque, alors que les systèmes d'IA de contrôle des agriculteurs fondés sur la géomatique à des fins de contrôle ne le seraient pas.

33 Voir en particulier le texte : Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government* (COM(2016) 179 final), 19 avril 2016, disponible en ligne sur <https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation> (consulté le 26 mai 2021). Voir

se distingue par une politique qui entend combiner les deux rôles des services publics : pourvoyeurs de données vis-à-vis du secteur privé à travers les directives dites d'« *Open Data* » ou « *Public Sector Information* » (en abrégé *PSI*)³⁴ mais également récepteurs de données cette fois en provenance du privé de manière à nourrir les bases de données informationnelles qui lui permettront de mettre au point de meilleurs services au bénéfice de l'intérêt général. Ce mouvement que d'aucuns qualifient de « *reverse PSI* » s'est développé récemment à la faveur du souci de la Commission de permettre la création de mégadonnées au sein du secteur public et donc du développement par cette dernière d'outils d'IA. Alors que les États Unis se concentrent quasiment exclusivement sur le premier rôle du secteur public, à savoir celui de pourvoyeur de données, que nous ne manquerons pas d'analyser ci-après, le second rôle nous intéressera dans les considérations qui suivront.

A. L'État, pourvoyeur de données – de l'Open Data au Data Governance Act

Le premier rôle de l'État renvoie aux textes relatifs à l'utilisation et l'exploitation des informations du secteur public par les entreprises (**partage de données du secteur public vers le secteur privé**) – G2B : « *L'ouverture des informations détenues par les pouvoirs publics est une politique de longue date de l'UE. Les données ont été produites avec des fonds publics et devraient donc bénéficier à la société. La directive sur les données ouvertes récemment révisée³⁵, ainsi que les autres dispositions législatives sectorielles, garantiront que le secteur public mette un plus grand volume des données qu'il produit à la disposition de tous³⁶, notamment*

aussi la Communication 'Artificial Intelligence for Europe' du 25 Avril 2018 : « A strategy on AI for Europe » (repris par le Conseil en juin 2018).

34 Voy. Directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *J.O.U.E.*, L 172, 20 juin 2019, disponible en ligne sur <https://op.europa.eu/en/publication-detail/-/publication/a6ef4c41-97eb-11e9-9369-01aa75ed71a1/language-fr/format-PDFA2A> (consulté le 26 mai 2021).

35 Directive (UE) 2019/1024 abrogeant la directive 2003/98/CE telle que révisée par la directive 2013/37/UE.

36 Le portail européen des données ouvertes contient des exemples d'entreprises de toute l'UE qui ont bénéficié des données ouvertes, et dont certaines n'existeraient pas sans la

des PME, mais aussi de la société civile et de la communauté scientifique, dans le cadre d'évaluations indépendantes des politiques publiques. Les pouvoirs publics peuvent cependant aller plus loin. Les ensembles de données de grande valeur ne sont souvent pas disponibles dans les mêmes conditions dans toute l'UE, au détriment de l'utilisation des données par des PME qui ne peuvent faire face financièrement à cette fragmentation. Dans le même temps, les données sensibles (par exemple les données de santé) dans les bases de données publiques ne sont souvent pas mises à disposition à des fins de recherche, en l'absence de capacités ou de mécanismes permettant des actions de recherche spécifiques dans le respect des règles de protection des données à caractère personnel»³⁷.

L'encadrement légal de la réutilisation des données du secteur public par l'Union européenne mérite quelques réflexions. Nous notons que l'Union en est à la quatrième mouture du cadre législatif de la matière. Il y eut tout d'abord, premier temps, la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public³⁸. Cette première directive entendait réaliser une harmonisation minimale des réglementations des États membres afin de permettre la réalisation du marché intérieur et l'instauration d'un régime de concurrence non faussée³⁹. Le champ d'application de la directive est le suivant : il s'applique à la réutilisation de « documents » – définis comme « *tout contenu quel que soit son support (écrit sur support papier ou stocké sous forme électronique, enregistrement sonore, visuel ou audiovisuel)* » détenus par des « organismes du secteur public » – définis comme « *l'État, les collectivités territoriales, les organismes de droit public et les associations formées par une ou plusieurs de ces collectivités ou un ou plusieurs de ces organismes de droit public* »⁴⁰. Point important, cette directive n'imposait

disponibilité de ces données : <https://www.europeandataportal.eu/fr/using-data/use-cases> (consulté le 26 mai 2021).

37 COM (2020) 66 final, *op. cit.*

38 Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *J.O.C.E.*, L 345, 31 décembre 2003, p. 90 ; ci-après « la directive 2003/98/CE ».

39 M. Knockaert, « La réutilisation des informations du secteur public : l'*open data* et les organismes publics », *J.T.*, 2018, p. 614.

40 Directive 2003/98/CE, article 2, al. 1er, 1) et 3).

aucune obligation aux États de mettre leurs données à disposition ni d'en autoriser la réutilisation.

Dix ans plus tard, deuxième temps, l'Union a décidé de modifier cette directive. Cela fut fait par l'intermédiaire de la directive 2013/37/UE du 26 juin 2013⁴¹. Deux points sont principalement modifiés par rapport au texte de 2003⁴² :

- Premièrement, la directive modifiée contraint désormais les États membres à une « *obligation claire de rendre tous les documents réutilisables* »⁴³. Ainsi, la réutilisation des informations du secteur public passe du rang de simple possibilité à celui de principe ;
- Deuxièmement, la modification de 2013 étend le champ d'application de la directive aux informations détenues par les bibliothèques, les musées et les archives.

Ensuite, troisième temps, le 20 juin 2019, le Parlement européen et le Conseil ont adopté la directive 2019/1024/UE concernant les données ouvertes et la réutilisation des informations du secteur public. Dans un souci de clarté, cette directive ne modifie pas le texte originel de 2003 mais procède à une refonte de la matière. La directive 2019/1024/UE doit être transposée pour le 17 juillet 2021 au plus tard⁴⁴. La nouvelle directive ne révolutionne pas la matière. Cependant, outre des modifications techniques concernant les licences et les formats interopérables et ouverts,

41 Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, *J.O.U.E.*, L 175, 27 juin 2013, p. 1 ; ci-après « la directive 2013/37/UE ».

42 On remarque également des modifications concernant les licences de réutilisation (incitation à utiliser des licences ouvertes), la tarification des réutilisations, et l'utilisation de formats de documents interopérables et lisibles par machine.

43 Directive 2013/37/UE, considérant 8.

44 C'est également à cette date que la directive 2003/98/CE sera abrogée.

auxquels les documents doivent être fournis, elle introduit selon nous deux modifications fondamentales :

- Premièrement, elle étend le champ d'application de la réutilisation des informations du secteur public aux entreprises publiques :
 - actives dans les secteurs de l'eau, de l'énergie, des transports, et des services postaux ;
 - qui exploitent ou organisent des services publics de transport de voyageurs par chemin de fer ou par route ;
 - qui agissent en qualité de transporteur aérien ou d'armateur communautaire.

Nous notons cependant que les entreprises publiques bénéficient d'un régime moins contraignant que celui applicable aux organismes publics. Renouant en quelque sorte avec les dispositions de la directive de 2003, la directive 2019/1024/UE ne leur impose pas le principe de la réutilisation. Sauf disposition nationale contraire, il appartient donc à l'entreprise publique concernée d'autoriser ou non la réutilisation⁴⁵.

- Deuxièmement, elle entrouvre la porte à une potentielle application de la Directive aux acteurs du secteur privé. En effet, le considérant 19 de la directive 2019/1024/UE dispose que « *[l]es États membres peuvent également décider d'appliquer les dispositions de la présente directive aux entreprises privées, notamment celles qui fournissent des services d'intérêt général* », comme par exemple les fournisseurs d'énergie ou de moyens de communication. Il s'agit, on le pressent, de maximiser les données susceptibles d'être utilisées par le marché privé dans la mesure où ces données ont été collectées dans l'intérêt général.

45 Directive 2019/1024/UE, article 3, §2 et considérant 26.

Enfin, et c'est le quatrième temps de cette valse de textes européens, la proposition de règlement sur la gouvernance des données du 25 novembre 2020⁴⁶, évoquée dans l'avant-propos, propose d'avancer encore sur un point, à savoir ouvrir la réutilisation des données protégées et jusque-là exclues de tout accès. En effet, les données à caractère personnel ou protégées par des droits de propriété intellectuelle étaient jusqu'ici exclues par les directives *PSI* de toute possibilité d'accès et d'exploitation. Or, l'utilisation de certaines données à caractère personnel, le cas échéant après pseudonymisation et strict contrôle du respect de la protection des données, pourrait être utile à certaines entreprises du secteur privé. Les documents, inventions ou données couvertes par des droits de propriété intellectuelle peuvent de même servir aux entreprises qui souhaiteront les réutiliser. L'exemple de l'accès à la recherche commanditée par une administration et menée sur base de questionnaires, peut être cité. Cet exemple mêle des données et documents protégés par les droits de propriété intellectuelle et des traitements de données à caractère personnel. Des entreprises peuvent souhaiter avoir accès aux éléments collectés et produits dans le cadre de la recherche pour des raisons de marketing ou d'amélioration de leurs services ou produits. La proposition de règlement⁴⁷ entend permettre cet accès tout en fixant, sans désormais les interdire, les conditions de cette réutilisation des données.

46 COM (2020) 767 final.

47 C'est l'objet du chapitre II de la proposition de règlement (Exposé des motifs, p. 8) : « *Le chapitre II crée un mécanisme de réutilisation de certaines catégories de données protégées du secteur public, qui est subordonné au respect des droits d'autrui (notamment pour des motifs de protection des données à caractère personnel, mais aussi de protection des droits de propriété intellectuelle et de confidentialité des informations commerciales). Ce mécanisme est sans préjudice de la législation sectorielle de l'UE sur l'accès à ces données et sur leur réutilisation. La réutilisation de ces données ne relève pas du champ d'application de la directive (UE) 2019/1024 (directive sur les données ouvertes). Si les dispositions du présent chapitre ne créent aucun droit de réutilisation de ces données, elles définissent cependant un ensemble de conditions de base harmonisées dont le respect autoriserait une telle réutilisation (l'exigence de non-exclusivité, par exemple). Les organismes du secteur public autorisant ce type de réutilisation devraient être équipés sur le plan technique afin que la protection des données, le respect de la vie privée et la confidentialité soient pleinement préservés. Les États membres devront mettre en place un point de contact unique pour aider les chercheurs et les entreprises innovantes à sélectionner des données appropriées, et ils seront tenus de mettre en place des structures qui soutiendront les organismes du secteur public par des moyens techniques et une assistance juridique ».*

B. L'autorité publique, bénéficiaire de données collectées et traitées par le secteur privé voire de données des citoyens – le 'reverse PSI' ou le C or B2G

La proposition de règlement faite par la Commission sur la gouvernance des données, que nous venons d'évoquer, consacre une politique de *reverse PSI* en faveur des autorités publiques et ce, au service de l'intérêt général. Le document '*Une stratégie européenne pour les données*⁴⁸ consacrait déjà cette politique : le secteur public a un rôle central à jouer dans la politique européenne des données, à la fois comme **pourvoyeur** de données vis à vis des entreprises et des citoyens et ce sur base du principe de transparence, lui-même dérivé de la liberté d'expression, mais il doit également pouvoir, par la mise à disposition cette fois à son profit de données et l'utilisation d'outils d'IA, améliorer son activité, la définition de ses stratégies et l'effectivité des réglementations qu'il produit: « *L'Europe vise à tirer parti des avantages d'une meilleure utilisation des données, notamment une productivité accrue et des marchés plus concurrentiels, ainsi que des améliorations dans les domaines de la santé et du bien-être, de l'environnement, une gouvernance transparente et des services publics efficaces. [...] Les politiques publiques peuvent accroître la demande d'offres fondées sur des données, à la fois en renforçant la capacité propre du secteur public à employer les données aux fins du processus décisionnel, et en actualisant la réglementation et les politiques sectorielles afin de tenir compte des possibilités offertes par les données et de garantir qu'elles ne maintiennent pas d'éléments décourageant l'utilisation productive des données* »⁴⁹.

Le projet de règlement consacre cette politique qualifiée d'« *altruisme de données* »⁵⁰ et les moyens de rendre effective sa réalisation. Il s'agit de créer

48 COM (2020) 66 final, *op. cit.*

49 COM (2020) 66 final, *op. cit.*

50 « *Le chapitre IV facilite l'altruisme des données (données mises volontairement à disposition par des particuliers ou des entreprises, pour le bien commun). Il prévoit la possibilité, pour les organisations qui pratiquent l'altruisme des données, de s'enregistrer en tant qu' « organisation altruiste en matière de données reconnue dans l'UE » afin de renforcer la confiance dans leurs activités. Par ailleurs, un formulaire européen commun de consentement à l'altruisme des données sera élaboré afin de réduire les coûts liés au recueil du consentement et de faciliter la portabilité des données (lorsque les données à mettre à disposition ne sont pas détenues par la personne).* » COM (2020) 767 final, Exposé des motifs, pp. 8-9.

des mécanismes qui tout en garantissant le respect des législations, en particulier de protection des données, permettront à des entreprises et à des particuliers qui y consentent de nourrir de leurs données les bases de données du service public et ce à des fins précises d'intérêt général. On conçoit l'intérêt que peut présenter par exemple en matière de recherche publique médicale, le transfert de données en provenance du secteur pharmaceutique, ou en matière de mobilité, l'exploitation des données collectées par Waze ou Uber. Comme le décrit le document stratégique de la Commission cité au paragraphe précédent, « *[L]es données sont créées par la société et peuvent servir à lutter contre les situations d'urgence, telles que les inondations et les feux de forêt, à faire en sorte que les personnes vivent plus longtemps et en meilleure santé, à améliorer les services publics et à lutter contre la dégradation de l'environnement et le changement climatique et à permettre une lutte plus efficace contre la criminalité. Les données générées par le secteur public ainsi que la valeur créée devraient être disponibles pour le bien commun en faisant en sorte, par le recours à un accès préférentiel, que ces données soient utilisées par des chercheurs, d'autres institutions publiques, des PME ou des start-ups. Les données provenant du secteur privé peuvent également apporter une contribution significative au bien public* »⁵¹. Cette politique « altruiste » des données au profit du bien public ou, selon l'appellation retenue par la Commission, les « **données pour le bien public** » exige le partage et l'utilisation de données privées par les pouvoirs publics (partage de données d'entreprises aux pouvoirs publics) – B2G⁵².

L'effectivité du règlement repose sur la création d'un nouveau métier d'intermédiation, contrôlé par des instances nationales : les services de partage des données. Ces prestataires de services de partage de données (intermédiaires de données) doivent jouer un rôle clé dans l'économie fondée sur les données, en tant qu'instruments facilitant l'agrégation et

51 COM (2020) 66 final, op. cit., p. 8.

52 « *Les volumes de données du secteur privé à la disposition du secteur public sont actuellement insuffisants pour améliorer l'élaboration des politiques sur la base d'éléments concrets et les services publics tels que la planification de la mobilité ou l'amélioration de la portée et de l'actualité des statistiques officielles et, partant, de leur pertinence dans le contexte des nouveaux développements sociétaux* ». COM (2020) 66 final, op. cit., section 4.

l'échange de quantités substantielles de données pertinentes⁵³. Les intermédiaires de données qui proposent des services mettant en relation les différents acteurs contribuent potentiellement à la mise en commun efficace des données ainsi qu'à la facilitation du partage bilatéral des données. En ce qui concerne le partage des données à caractère personnel, ils sont chargés de veiller au respect des dispositions du Règlement général de protection des données (RGPD) et assistent, le cas échéant, les personnes concernées à exercer leurs droits. Ces intermédiaires de données spécialisés, qui sont indépendants et neutres à la fois par rapport aux détenteurs de données et aux utilisateurs de ces données, faciliteront, on peut l'espérer, l'« émergence de nouveaux écosystèmes fondés sur les données qui soient indépendants de tout acteur jouissant d'une puissance significative sur le marché »⁵⁴. Par ailleurs, dans le cadre du règlement proposé, les « organisations altruistes en matière de données reconnues dans l'Union » devraient, selon des exigences dont le respect est vérifié par l'autorité nationale *ad hoc*, être en mesure de collecter des données pertinentes directement auprès de personnes physiques et morales ou de traiter les données collectées par d'autres et ce moyennant le consentement des personnes concernées, au sens du RGPD⁵⁵. Par « organisation altruiste », on entend des entités publiques ou privées servant des fins d'intérêt général « *comme les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, l'établissement plus aisé de statistiques officielles ou l'amélioration de la prestation de services publics. Le soutien à la recherche scientifique, et notamment au développement technologique et à la démonstration, à la recherche fondamentale, à la recherche appliquée et à la recherche financée par des fonds privés, devrait également être considéré comme une finalité d'intérêt général* »⁵⁶. L'objectif de ces dispositions reconnaissant l'altruisme des données est clairement de permettre à ces entités de disposer de données en nombre suffisant pour lancer des

53 Ces intermédiaires peuvent ainsi veiller à adapter les données, les enrichir, les convertir à un format standard et interopérable, etc.

54 COM (2020) 767 final, Considérant 22.

55 COM (2020) 767 final, Considérant 38.

56 COM (2020) 767 final, Considérant 35.

initiatives d'utilisation de l'IA⁵⁷, que par ailleurs l'Union européenne entend promouvoir.

Deux dernières remarques concluront ce second titre. En premier lieu, il est intéressant de noter que la politique européenne de la donnée et de l'IA contribue à estomper les frontières autrefois rigides entre le secteur privé et le secteur public. Ainsi, le document stratégique évoque le besoin d'une véritable politique de coopération entre ces secteurs. Il indique qu'il est nécessaire de « *renforcer les mécanismes de gouvernance au niveau de l'UE et dans les États membres présentant un intérêt pour l'utilisation de données transsectorielles et pour l'utilisation de données dans des espaces de données communs sectoriels, associant des acteurs privés et publics. Il pourrait notamment s'agir d'un mécanisme permettant de fixer des priorités pour les activités de normalisation et d'œuvrer à une description et une vue d'ensemble plus harmonisée des séries de données, des objets de données et des identificateurs de données afin de favoriser l'interopérabilité des données (c'est-à-dire la possibilité de les utiliser à niveau technique) entre secteurs et, le cas échéant, à l'intérieur des secteurs* »⁵⁸. Le règlement de la Commission sur la gouvernance des données est fondé précisément sur ces échanges possibles et, à plusieurs reprises, les documents européens évoquent la nécessité de se référer aux principes FAIR⁵⁹ pour gérer les données tant du secteur public que du secteur privé (données faciles à trouver, accessibles, interopérables et réutilisables) afin de faciliter les transmissions intersectorielles des données. On ajoutera que certains secteurs sont particulièrement identifiés comme porteurs de ce besoin de coopération et de synergie, tels que les secteurs de la santé, de la mobilité, de l'environnement, de l'agriculture,

57 « Le présent règlement vise à contribuer à l'émergence de réserves de données mises à disposition selon le principe de l'altruisme en matière de données, qui soient d'une taille suffisante pour permettre l'analyse des données et l'apprentissage automatique ». COM (2020) 767 final, Considérant 35.

58 COM (2020) 66 final, *op. cit.*, p. 8.

59 Sur ces principes, lire notamment leur description à l'adresse : <https://www.go-fair.org/fair-principles/>. Et l'article de M. WILKINSON et al., "The FAIR Guiding Principles for scientific data management and stewardship", *Nature Scientific Data* [Internet]. 2016;(160018), disponible en ligne sur <https://scholar.harvard.edu/mercecosas/publications/fair-guiding-principles-scientific-data-management-and-stewardship> (consulté le 26 mai 2021).

mais aussi les administrations publiques⁶⁰. La seconde remarque note que les obligations créées par les textes prescrivant l'accès aux données détenues par le secteur public contribuent à intensifier la circulation des données au sein de l'administration⁶¹ afin de faciliter cet accès, à se doter de sources authentiques et à constituer des mégadonnées centralisées ou non, en recourant à ses propres sources de données, collectées dans le cadre de ses missions publiques et donc disponibles en interne. Le partage des données entre les pouvoirs publics peut grandement contribuer à l'amélioration des politiques et des services publics, et aussi à la réduction de la charge administrative qui pèse sur les entreprises opérant sur le marché unique (principe « une fois pour toutes »). Cette circulation doit bien évidemment tenir compte des règles qu'impose le cloisonnement administratif et l'application des règles de protection des données⁶².

III. Les autorités publiques, moteur du développement d'applications d'IA

Le Livre blanc sur l'IA⁶³, dans sa section 4.F intitulée '*Encourager le secteur public à adopter l'IA*', indique qu'*« [i]l est essentiel que les administrations publiques, les hôpitaux, les services d'utilité publique et de transport, les autorités de*

60 EU Data Policy – European Data governance, mars 2021, accessible sur le site <https://digital-strategy.ec.europa.eu/en/policies/data-governance> (consulté le 26 mai 2021) : « *Data-driven innovation will bring benefits for companies and individuals by making our lives and work more efficient through: Health data: improving personalised treatments, providing better healthcare, and helping cure rare or chronic diseases; saving approximately €120 billion a year in the EU health sector; providing a more effective and quicker response to the global COVID-19 health crisis; Mobility data: saving more than 27 million hours of public transport users' time and up to €20 billion a year in labour costs of car drivers thanks to real-time navigation; Environmental data: combatting climate change, reducing CO2 emissions and fighting emergencies, such as floods and wildfires; Agricultural data: developing precision farming, new products in the agro-food sector and new services in general in rural areas; Public administration data: delivering better and more reliable official statistics, and contributing to evidence-based decisions* ».

61 « *Les internautes citoyens, gestionnaires et agents de l'Etat sont en mesure de communiquer, partager et échanger des informations. Compte tenu de ce contexte, le cadre juridique relatif à l'information qui est nécessairement en possession de l'Administration, devrait s'attacher à en régir les conditions d'accès par chaque agent de l'Etat plutôt que d'en interdire la circulation.* » P. TRUDEL, « *Gouvernement algorithmique et interconnexions de fichiers administratifs dans l'État en réseau* », 35 *Revista catalana de dret public*, 2007, pp. 206 et s.

62 E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée*, Cahier du CRIDS, n° 36, Bruxelles, Larcier, 2014, en particulier pp. 237 et s.

63 *Livre blanc sur l'intelligence artificielle, op. cit.*

surveillance financière et d'autres domaines d'intérêt public commencent rapidement à déployer dans leurs activités des produits et des services fondés sur l'IA. Les domaines de la santé et des transports, notamment, feront l'objet d'une attention particulière [...] ». L'UE entend ainsi promouvoir l'utilisation de l'IA par le secteur public, comme nous commencerons par le relever. Nous exposerons ensuite les bénéfices possibles d'une telle utilisation pour les autorités publiques et les citoyens, ainsi que, subséquemment, l'encadrement réglementaire opéré par l'Union européenne. Dans ce dernier point, nous mentionnerons les lois du service public qui sont d'application en Belgique et se retrouvent à tout le moins en France et certainement au-delà, celles-ci étant particulièrement pertinentes en la matière.

A. La promotion de l'utilisation de l'IA dans le secteur public

Précisément en ce qui concerne le développement d'applications d'IA dans le secteur public, les Annexes au plan stratégique de la Commission, publiées le 21 avril 2021⁶⁴, contiennent tout un chapitre (le chapitre 14) relatif à son importance. Elles rappellent le rôle crucial que cette technologie peut jouer dans l'amélioration des services aux citoyens, souligne le modèle pour le secteur privé que le secteur public peut constituer en développant des systèmes d'IA dignes de confiance et pleinement éthiques, et plaide pour des ressources financières et humaines adéquates en la matière⁶⁵. Le texte promeut également une meilleure collaboration entre administrations nationales, annonce le lancement d'un

64 ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions *Fostering a European approach to Artificial Intelligence*, COM (2021) 205 final, *op. cit.*

65 « *AI applications can contribute to better public services, e.g. by improving citizen-government interaction, enabling smarter analytical capabilities or improving efficiency across public-sector domains and supporting democratic processes. Use of AI systems can bring benefits across all key public-sector activities. Through early adoption of AI, the public sector can be the first mover in adopting AI that is secure, trustworthy and sustainable. For deeper and wider AI uptake to become a reality, Europe's public sector should have access to adequate funding and be equipped, skilled and empowered to conduct strategic and sustainable purchasing and adoption of AI-based systems. The RRF provides an unprecedented opportunity to accelerate the uptake of AI in public administration across Europe through its Modernise flagship which aims at boosting investments and reforms in digitalisation of public administration.* » Annexes to the Communication COM (2021) 205 final, *op. cit.*, p. 47.

programme (*Adopt AI*⁶⁶) particulièrement centré sur le lancement de projets IA dans le secteur public et s'attarde sur la question des marchés publics collaboratifs et transfrontières, notamment par la création d'un « *public procurement data space* ». La Commission entend également aider les initiatives des administrations, des cités (villes intelligentes) et des communautés de citoyens, d'une part, en créant des registres d'algorithmes et d'applications dignes de confiance et, d'autre part, « *by developing a set of minimal capabilities for algorithms to be used in contract conditions* » (e.g. *Fair AI MIM*⁶⁷).

Outre ces textes fondateurs, de manière plus pragmatique, nous évoquons les études coordonnées ou réalisées par le JRC (*Joint Research Centre* de la Commission)⁶⁸ relatives à l'IA dans les services publics. Ces études relaient les préoccupations de l'Union européenne auprès des autorités publiques, éclairent la Commission sur les réalités du terrain et sur les données contextuelles à prendre en compte et servent pour les autorités publiques nationales des États membres à identifier des '*best Practices*' chez leurs voisins.

66 « *The programme aims to help Europe's public sector to use its strong collective purchasing power to act as a catalyst and stimulate demand for trustworthy AI. The public sector can lead the way in developing, purchasing and deploying taking in use trustworthy and human-centric AI applications, for example, by utilising public procurement of innovative solutions or by steering the development of new solutions towards its needs through pre-commercial procurement practices.* » *Ibidem*, p. 47 et les détails p. 48.

67 'Open and agile smart cities (OASC)', MIM 5: Fair AI and Algorithms (2020), document développé par la ville d'Amsterdam et mis à jour pour la dernière fois le 18 décembre 2020, accessible sur le site: <https://oasc.atlassian.net/wiki/spaces/OASCMIM/pages/91521069/MIM+5+Fair+Artificial+Intelligence+and+Algorithms> (consulté le 28 mai 2021). Cf. également, le document : 'Join, boost, sustain – the European way of digital transformation in cities and communities', repris en ligne sur <https://digital-strategy.ec.europa.eu/en/news/join-boost-sustain-european-way-digital-transformation-cities-and-communities> (consulté le 28 mai 2021).

68 Nous citons en particulier les deux études suivantes : G. MISURACA, (éd.), *Exploring Digital Government transformation in the EU - Analysis of the state of the art and review of literature*, Publications Office of the European Union, 2019, <https://doi.org/10.2760/17207> ; G. MISURACA et C. VAN NOORDT, *AI Watch - Artificial Intelligence in public services - Overview of the use and impact of AI in public services in the EU*, Publications Office of the European Union, 2020, <https://doi.org/10.2760/039619>.

Dans cette lignée, la Commission, dans sa proposition de règlement du 21 avril 2021, prévoit des « *measures in support of innovation* », contributives à l'utilisation de l'IA dans les services publics. Elle y prône ainsi l'utilisation de mécanismes législatifs dits « bac à sable » (*AI regulatory sandboxes*)⁶⁹ et impose des conditions pour le traitement de données à caractère personnel dans le cadre de ces législations « bac à sable » lorsqu'il s'agit de développer des systèmes innovants pour des raisons d'intérêt public⁷⁰.

Nous soulignons en outre la création en 2018 de l'*innovative public services (IPSO) platform* qui liste plus de 43 cas d'utilisation (*use cases*) de l'IA dans les services publics. Cette plateforme entend suivre les utilisations développées dans le secteur public.

B. L'IA au service des autorités publiques et des citoyens

Le Livre blanc sur l'IA résumait ainsi cet intérêt : « *Dans le domaine des services d'intérêt public, par exemple, les coûts de fourniture de services (transports, éducation, énergie et gestion des déchets) seront réduits, la durabilité des produits sera améliorée et les services répressifs disposeront d'outils appropriés pour assurer la sécurité des citoyens, avec des garanties adéquates en matière de respect des droits et des libertés* »⁷¹.

69 Proposition de règlement COM (2021) 206 final, art. 53.

70 Proposition de règlement COM (2021) 206 final, art. 54: « *In the AI regulatory sandbox: personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the following conditions:*

(a) the innovative AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas:

(i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;

(ii) public safety and public health, including disease prevention, control and treatment;

(iii) a high level of protection and improvement of the quality of the environment;

(b) the data processed are necessary for complying with one or more of the requirements referred to in Title III, Chapter 2 where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data [...] ». D'autres conditions sont reprises. Elles confirment les recommandations du HLGE on B to G data sharing.

71 *Livre blanc sur l'intelligence artificielle, op. cit.*, p. 2.

L'utilisation des ressources informatiques comme outil d'aide à la décision de l'administration n'est pas neuve. Elle s'est traduite depuis des décennies par la mise au point de systèmes dits experts, qui entendent, grâce à l'expertise de fonctionnaires particulièrement expérimentés, traduire en algorithmes les règles en usage suivies par l'administration dans ses décisions, suivant une logique de type '*if...then*'. Des lois, en particulier techniques, se prêtent de même à cette formulation logique. Ainsi, l'attribution d'une prime d'environnement dans ces systèmes experts suit une démarche simple : la vérification d'autant de conditions objectives peu interprétables (dimension des locaux, revenus du citoyen demandeur, nature du travail projeté, ...) s'opère facilement et l'algorithme administratif se contente d'en vérifier la présence selon les règles d'une causalité purement logique. L'utilisation de ces méthodes reste de mise au sein de l'administration mais de tels algorithmes dont, par ailleurs, la logique suivie est aisément transparente, constituent ce qu'il est convenu d'appeler l'« IA symbolique ».

D'autres méthodes, basées cette fois sur des méthodes de '*machine learning*', sont désormais privilégiées par la puissance sans comparaison de leurs résultats. Ainsi, l'ajout dans une '*big data*' de l'ensemble des déclarations fiscales, de certaines caractéristiques des déclarants, et des résultats des contrôles opérés par l'administration, permettra en quelques secondes de détecter des fraudes et de définir des stratégies fondées sur la comparaison de toutes les données. Dans de tels cas, le résultat ou la prédiction ne se définit pas par la causalité logique mais bien par la corrélation statistique, à travers des réseaux de neurones auto-apprenants, entre des données qui reprennent les résultats déjà observés. Ce sont donc principalement ces applications de '*machine learning*', qu'elles soient supervisées ou non, qu'elles soient dites de « *deep learning* » ou non, que l'Union européenne entend promouvoir afin d'en comprendre l'intérêt pour les pouvoirs publics et les administrés.

Chacun reconnaîtra que l'on peut accorder trois plus-values à l'utilisation de l'IA dans le secteur public comme d'ailleurs dans le secteur privé et pour les citoyens. L'IA est un instrument d'amélioration de l'efficacité et de la disponibilité de l'administration : il sécurise les données de l'administration ; il permet l'optimisation tant des stratégies et décisions des autorités publiques que de la mise en place des réglementations. Enfin, l'IA objective, apparemment du moins, les décisions prises ou à prendre. Sans doute, chacune de ces plus-values contient le revers de sa médaille, dans la mesure où s'y attachent des risques sociétaux ou individuels. Quelques mots sur chacune de ces 'plus-values' et sur les risques y associés qui justifient l'intervention du 'Droit'.

- **IA et sécurisation** : les exemples ne manquent pas. L'IA – et on pointe notamment les systèmes de reconnaissance faciale – facilite la lutte contre la criminalité⁷² et le contrôle du respect des législations fiscales ou de sécurité sociale. On sait combien dans le cadre d'opérations de secours urgents, l'IA a permis un repérage rapide des personnes sinistrées et à aider. En matière de recherches dans le domaine médical, les exemples d'utilisation des systèmes d'IA dans la lutte contre la maladie d'Alzheimer ou les maladies rares peuvent être cités⁷³ ou actuellement dans la lutte contre la *coronavirus disease* (COVID). A l'échelle d'une ville, dans le cadre de *smart cities*, ou d'une région, des systèmes d'IA peuvent repérer les habitations non conformes à des normes environnementales ou des quartiers criminogènes. Sans doute, ce souci de la sécurisation peut conduire à une surveillance de tous les instants et expliquer la

72 C'est ce que souligne la Commission européenne dans son Livre blanc, p. 2 note 5 : « L'IA peut fournir des outils permettant de mieux protéger les Européens contre les actes criminels et terroristes. Ces outils pourraient, par exemple, permettre de détecter la propagande terroriste en ligne, de mettre au jour des transactions suspectes dans la vente de produits dangereux, d'identifier des objets cachés ou des substances ou produits illicites dangereux, de prêter assistance aux citoyens en cas d'urgence et de guider les premiers intervenants ».

73 On note que des projets de recherche entendant faire usage de système d'IA pour permettre une médecine personnalisée de patients atteints, par exemple, de la maladie de Parkinson, sont cofinancés par la Commission européenne. Voy. <https://erapermed.isciii.es/joint-transnational-call-2020/> (consulté le 27 mai 2021).

tendance des autorités publiques à exiger la collaboration du secteur privé.

- **IA et optimisation :** l'IA supporte ou devrait supporter, à condition d'être de qualité, les choix stratégiques de l'autorité publique et aider voire assurer l'effectivité de l'application des réglementations. Ainsi, l'IA est, ou pourrait être demain, un adjuvant important pour des décisions en termes de développement urbain, de mobilité et de recherche médicale⁷⁴. Le profilage des citoyens ou des entreprises grâce à des systèmes de *machine learning* s'avère utile pour assurer l'octroi d'aides appropriées, le repérage d'actions à entreprendre, etc. Enfin, on utilisera, dans le secteur public comme dans le secteur privé, l'IA comme outil de réduction des coûts et d'optimisation des dépenses. On conçoit que ce souci de l'optimisation rencontre nombre d'appréhension : les risques de biais et d'erreur font craindre certaines discriminations tant individuelles que collectives des citoyens voire des entreprises, et les possibilités d'anticiper les besoins des personnes voire leur état de santé soulèvent des réactions hostiles face à ce qui est perçu comme un *big brother*.

Le recours à l'IA trouve également argument par le fait qu'il serait ainsi possible de consacrer plus de temps aux questions délicates ou plus complexes posées par les citoyens, le système mis en place par des *chatbots* pouvant en effet suffire pour les demandes récurrentes ou aisées des administrés⁷⁵. On ajoute à cela un argument, celui de la réduction des dépenses publiques de personnel. Un rapport de l'IWEPS estime qu'en

⁷⁴ Voir ce qui est dit dans le cadre de la plus-value précédente (IA et sécurisation).

⁷⁵ Voir à cet égard, à titre d'exemple, le projet de *chatbot* nommé *DIPLO* et mené par la Communauté française pour répondre aux demandes des étudiants. Voir aussi le *chatbot* utilisé par *Partenamut*.

Région Wallonne, l'équivalent de 55% des fonctionnaires (soit 65.000 personnes) pourrait ainsi être remplacé par des ordinateurs intelligents⁷⁶.

- **IA et objectivation** : L'attribution de logements sociaux ou de bourses d'étude, l'examen des candidatures à des postes de fonction publique, lorsqu'elles sont opérées par des systèmes automatisés, offrent aux décideurs l'argument de l'objectivité que représente le calcul de la machine, loin de la subjectivité de décideurs humains. « *Data do not lie* », sous-entendu tel n'est pas le cas des humains. Ainsi, le choix d'un collaborateur proposé par un système d'IA travaillant sur les *curricula vitae*, un système d'*affective computing* analysant les mouvements faciaux lors d'un interrogatoire, l'analyse de la frappe sur l'ordinateur, diverses bases de données relatives aux formations suivies et appuyés par des logiciels de prédiction médicale etc., apparaîtra plus objectif que les appréciations personnelles d'un jury qui peut avoir été 'sous le charme' d'un candidat. A cet argument d'objectivité apparente des 'vérités sorties de l'ordinateur', nous objectons que l'humain ne se réduit pas à des données qui nécessairement sont décontextualisées (e.g. le candidat à l'emploi vient de perdre un ami ou un parent). Outre ce réductionnisme, une fois de plus, nous craignons les biais et erreurs générés par les systèmes d'IA. Au-delà, nous soulignons la crainte d'une tendance à la déresponsabilisation des décideurs et à la délégation du pouvoir de décision aux machines, ce que d'aucuns qualifient pour le rejeter de 'solutionnisme technologique'⁷⁷. En amont, il est aussi important de garder à l'esprit que la programmation des

76 C. ALBESSART, V. CALAY, J.L. GUYOT, A. MARFOUK et F. VERSCHUEREN, *La digitalisation de l'économie wallonne : une lecture prospective et stratégique*, Rapport de recherche de l'IWEPS, 27 juin 2017, pp. 43-45, disponible en ligne sur <https://www.iweps.be/publication/digitalisation-de-leconomie-wallonne-lecture-prospective-strategique/> (consulté le 27 mai 2021).

77 CNIL, « Thématique » : *Coronavirus (COVID-19)*, disponible à l'adresse suivante : <https://www.cnil.fr/fr/coronavirus-covid-19> (consultée le 27 mai 2021). Voy. aussi *Point d'étape sur les activités de la CNIL dans le contexte du COVID-19*, 21 janvier 2021, disponible à l'adresse : <https://www.cnil.fr/fr/point-detape-sur-les-activites-de-la-cnil-dans-le-contexte-du-covid-19> (consultée le 27 mai 2021).

systèmes d'IA se fait par des agents humains qui posent donc des choix, et que par ailleurs, comme relevé par Paula Boddington, philosophe et chercheuse à l'université d'Oxford, « *it is always a human being who has decided to use AI to make decisions* »⁷⁸.

Nous ajoutons que l'IA constitue en outre une aide à la fois à la conception et à l'application des législations. Ainsi, en ce qui concerne l'aide à la conception de législations, au risque de contourner les processus de délibérations démocratique, l'IA offre des instruments particulièrement appropriés tant pour concevoir des contenus législatifs, au sens le plus large (lois, décrets, arrêtés, circulaires ministérielles...), que pour assurer l'effectivité de ceux-ci. Cette double vocation de l'IA doit être soulignée. Aider à la conception de contenus législatifs est évident. Prenons un exemple : la fixation du prix des médicaments et de leur remboursement sera grandement facilitée si un système de *machine learning* bien nourri de données relatives aux consommateurs de ces médicaments, à leur profil, à la fréquence de leurs consommations, au coût de leur non prise, etc. instruit voire conduit la décision du législateur⁷⁹.

L'IA pourrait également être mise au service des administrations dans leur lutte contre le non-respect des législations, comme par exemple pour lutter contre les fraudes à la sécurité sociale (Cf. en Belgique, le système *OASIS*) ou aux législations fiscales. Ainsi, des drones capturent des images de nos campagnes pour détecter automatiquement le respect des prescrits des législations et décisions prises en matière agricole. Demain, des capteurs placés dans nos véhicules connectés pourront automatiquement détecter nos infractions à la circulation routière voire – et là on touche à une

78 Paula Boddington, *Does AI make better decisions than humans? Thinking Ethics of AI*, UNESCO, 19 octobre 2020, <https://www.youtube.com/watch?v=2E711hdjHsg> (consulté le 27 mai 2021).

79 A tout le moins en droit belge, la question de l'admissibilité d'une telle pratique se pose notamment au regard de l'article 33 de la Constitution : « *Tous les pouvoirs émanent de la Nation. Ils sont exercés de la manière établie par la Constitution* ».

effectivité quasi parfaite de la loi – nous contraindront à les respecter, par exemple en bridant nos moteurs et en les contraignant à la vitesse réglementaire. Enfin, l'IA peut assurer l'application des législations. Ainsi, pour reprendre des exemples déjà cités, des systèmes de *machine learning* pourraient demain remplacer les agents de l'administration dans les décisions d'attribution de logements ou d'aides publiques. On peut même imaginer, fantasme du juge-robot, qu'en cas de litige, ce soit un système d'IA qui tranche et non plus un humain.

Les citoyens et les entreprises trouvent dans l'utilisation de l'IA par les administrations et services publics, d'indéniables avantages. Quelques exemples suffisent : un employeur tout comme un candidat employé trouveront ou pourront trouver, grâce à des plateformes 'intelligentes' et interactives, mises en place par des organismes publics d'aide à l'emploi, la réponse à leurs demandes plutôt que d'être confrontés à des bases de données dans lesquelles ils trouvent leurs chemins avec difficulté. Le projet *DIPLO* déjà cité se targue de la convivialité plus grande obtenue grâce au *chatbot*, de préférence aux traditionnelles FAQ. Le choix d'itinéraires de transports multimodaux peut être de même facilité par des systèmes d'IA communs à différents services publics. On sait qu'en matière de santé, des systèmes de télédiagnostic épargnent à des patients des déplacements et offrent des réponses largement satisfaisantes en termes de détection de maladie. Comme pour les autorités publiques, les trois valeurs ajoutées de l'IA s'appliquent : sécurisation, optimisation et objectivation. Ces valeurs ajoutées de l'IA expliquent que l'intérêt des citoyens rejoint souvent celui de l'autorité publique et que les premiers peuvent dès lors souhaiter bénéficier de tels avantages, en acceptant certaines limites à leurs libertés : ainsi, le citoyen peut accepter de livrer des informations y compris sensibles pour 'optimiser' sa recherche d'emploi ou l'octroi d'une bourse d'études. Nous reviendrons sur ce dilemme au cœur des choix de l'IA publique. Au-delà, nous soulignons que les services de l'IA permettront une accessibilité 24h/24 et 7j/7 des administrations publiques, qu'ils peuvent faciliter une traduction en temps réel des demandes de personnes étrangères et un dialogue interactif

totalément ou non automatisé entre l'administré et l'administration, bien utile lorsque le premier peut difficilement se déplacer. On ajoute que des bornes interactives dans les musées publics facilitent la découverte des œuvres.

C. L'encadrement réglementaire

Avant d'analyser l'encadrement réglementaire européen de l'utilisation de l'IA par les services publics, nous tenons à mentionner les lois du service public qui sont à tout le moins en vigueur en droit belge⁸⁰. Il s'agit premièrement de la loi de mutabilité ou de changement : celle-ci peut justifier le recours aux systèmes d'IA par les services publics. La deuxième loi du service public est la loi de continuité : celle-ci requiert la prise de précautions, notamment en matière de sécurité, afin que le service, qui par nature est essentiel, ne souffre d'aucun dysfonctionnement. La loi d'égalité des usagers du service public constitue la troisième loi : le respect de cette dernière est particulièrement épineux eu égard aux divergences quant à l'accès aux services digitalisés de différentes fractions de la population, mais aussi eu égard à l'automatisation des discriminations que pourrait aisément engendrer l'utilisation de systèmes d'IA par les administrations. La loi de transparence est également essentielle en la matière : elle requiert en particulier des mesures de publicité active et passive à charge de l'administration, ainsi que la compréhension par l'administré des motifs de droit mais aussi de fait de toute décision le concernant. Enfin, le droit du citoyen à un service public humain, fondé sur le droit à la dignité humaine, est avancé comme une cinquième loi du service public : ainsi, la relation entre l'administration et l'administré ne peut se réduire à une interaction entre une machine et l'administré.

Pour en revenir au droit européen, le RGPD accorde des droits aux citoyens et aux entreprises tant en ce qui concerne leur 'droit de savoir'

⁸⁰ Pour le détail, nous renvoyons la lectrice/ le lecteur aux développements réalisés dans le cadre du rapport commandité par l'AdN.

que leur ‘droit de comprendre’ (y compris les ‘bases’ de la décision qui leur est opposée). À ces balises, s’en ajoutent deux.

La première : dans la mesure où le rapprochement de données venant de diverses administrations, le cas échéant situées hors zone, représente un risque important pour les individus, il importe que le projet fasse l’objet d’une évaluation interne *a priori* des impacts possibles de la décision. La portée et les conditions de cette évaluation portent, comme l’indique l’article 35 du RGPD, sur les conséquences potentielles sur les libertés individuelles et la vie privée, mais elle sera également attentive aux discriminations possibles d’individus ou de groupes d’individus, et aux effets économiques et sociaux du partage projeté.

La seconde : l’article 22 du RGPD qui s’applique exclut qu’une décision puisse être fondée exclusivement sur un traitement automatisé mais introduit cependant des exceptions notamment sur base d’une autorisation légale, moyennant « *des mesures appropriées de sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée* »⁸¹. Cette disposition vaut bien évidemment pour toute décision administrative automatisée. Le droit français traduit cette exigence de la manière suivante : « [...] *une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande* »⁸². Cette disposition oblige ainsi à révéler autant que possible les codes sources au rang de documents administratifs communicables. Elle implique *qu'a posteriori*, à la simple demande de l’administré, des informations soient données par l’administration, sous une forme intelligible. Ces informations visent ainsi le degré et le mode de contribution du traitement algorithmique à la prise de décision, les

81 Article 22.2 b) du RGPD.

82 Article L. 311-3-1 du Code français des relations entre le public et l’administration, disponible en ligne sur https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033205535/ (consulté le 31 mai 2021).

données (personnelles ou non) traitées, leurs sources (privées ou publiques), et les paramètres de traitement. Le cas échéant, les informations porteront également sur la pondération des paramètres, appliquée à la situation de la personne concernée ainsi qu'aux opérations effectuées par le traitement. L'idée principale de cette disposition est d'offrir à la personne concernée un meilleur contrôle de la décision et de lui donner les moyens de la contester. On passe progressivement d'une obligation d'information à une obligation d'explication. A cet égard, mérite d'être citée une décision française du 12 juin 2018 à propos de la loi du 20 juin 2018 visant à adapter le droit français aux règles posées par le RGPD. Le Conseil constitutionnel a décidé que « *ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement* »⁸³.

Certaines dispositions de la proposition de règlement, soumise au Parlement européen et au Conseil le 21 avril 2021 par la Commission européenne⁸⁴, que nous avons brièvement exposée *supra* dans l'avant-propos, posent des questions quant à l'utilisation de l'IA par les services publics, auxquelles ces derniers se devront d'être particulièrement attentifs.

Tout d'abord, certaines utilisations de l'IA sont prohibées. Parmi celles-ci, sont interdites en vertu de l'article 5 certaines applications de l'IA qui concernent, ou plutôt qui auraient pu concerner, les services publics. Nous relevons comme telles l'interdiction des pratiques suivantes :

- « (c) *the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality*

83 Décision n° 2018-765 DC du 12 juin 2018, disponible en ligne sur <https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm> (consulté le 31 mai 2021).

84 Artificial Intelligence Act proposal, *op. cit.*

characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity ». Un système de *ranking* social tel qu'il en existe en Chine, ne pourrait donc voir le jour en Europe ;

- « (d) *the use of 'real-time' remote biometric identification systems⁸⁵ in publicly accessible spaces⁸⁶ for the purpose of law enforcement⁸⁷, unless and in as far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA 62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State* ». Sauf les exceptions strictement listées, les autorités chargées de l'application de la loi (*law enforcement authorities*) ne pourront donc pas faire usage de systèmes d'identification biométrique en temps réel en vue de la prévention, de la recherche, de la détection ou de la poursuite d'infractions pénales ou de

85 « *In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality* ». Artificial Intelligence Act proposal, Considérant 8.

86 « *'publicly accessible space' means any physical place accessible to the public, regardless of whether certain conditions for access may apply* ». Artificial Intelligence Act proposal, Article 3 (39).

87 « *'law enforcement' means activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security* ». Artificial Intelligence Act proposal, Article 3 (41).

l'exécution de sanctions pénales, y compris la protection et la prévention des menaces pour la sécurité publique.

Comme déjà relevé, l'annexe III liste huit domaines ou types de systèmes d'IA à haut risque, dont un grand nombre ont trait aux services publics. Nous pointons ainsi l'utilisation de l'IA pour :

- la gestion ou l'opération du trafic routier et la fourniture d'eau, gaz, chauffage et électricité ;
- la détermination de l'accès à l'éducation ou aux formations mais aussi l'évaluation des élèves, des étudiants ou des participants à des tests requis pour l'admission dans des institutions éducatives ;
- le recrutement ou la sélection des travailleurs ou la prise de décision pour la promotion ou la fin de contrat professionnel, pour allouer les tâches ou pour évaluer les performances et comportements des contractants ;
- l'évaluation de l'éligibilité des personnes physiques aux prestations et services d'assistance publique, ainsi que pour accorder, réduire, révoquer ou réclamer ces prestations et services ;
- l'évaluation de la solvabilité des personnes physiques ou l'établissement de leur score de crédit ;
- l'envoi ou l'établissement de la priorité dans l'envoi de services de première intervention d'urgence ;
- certaines pratiques par les services répressifs⁸⁸ ;

88 Il s'agit plus précisément des systèmes suivants : « (a) *AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;*
(b) *AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;*
(c) *AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);*

- certaines pratiques en matière de migration, de demandes d'asile et gestion des frontières⁸⁹ ;
- l'assistance d'une autorité judiciaire dans la recherche et l'interprétation des faits et du droit et dans l'application du droit à un ensemble concret de faits.

Les obligations envers les acteurs impliqués dans la *supply-chain* de systèmes d'IA à haut risque se voient multipliées par le texte. A leur simple lecture, on devine les modifications profondes qu'elles impliquent dans la gestion, l'organisation et le fonctionnement de nos administrations, en particulier si les autorités publiques peuvent être qualifiées de fournisseurs du système d'IA qu'elles entendent utiliser. En effet, les fournisseurs de systèmes d'IA à haut risque se voient imposer de multiples devoirs (article 16)⁹⁰. La proposition entend instituer, pour les systèmes dits à haut-risque,

(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data. »

89 Il s'agit plus précisément des systèmes suivants : « *(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;*

(b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

(d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status ».

90 Art. 16 du Artificial Intelligence Act proposal : « *Providers of high-risk AI systems shall:*

(a) ensure that their high-risk AI systems are compliant with the requirements [for high-risk AI systems];

(b) have a quality management system in place which complies with Article 17;

(c) draw-up the technical documentation of the high-risk AI system;

(d) when under their control, keep the logs automatically generated by their high-risk AI systems;

un système de gestion des risques (article 9) qui implique le suivi de bonnes pratiques en matière d'évaluation des systèmes (absence de biais, qualité des données, ...). L'article 10 mentionne divers devoirs liés à la gouvernance des données, tels que le *testing* et la validation des choix de *design* et des données prises en compte, l'examen des biais possibles, etc. On ajoute les obligations de documentation (articles 11 et 18), de *loggings* (articles 12 et 20) et surtout de surveillance humaine (*human oversight*)⁹¹. Le projet mentionne le devoir de coopération avec les autorités nationales compétentes y compris en fournissant l'accès à tous les logs. En particulier, l'article 19 mentionne l'obligation d'une évaluation préventive de conformité du système avant toute mise sur le marché⁹². D'autres obligations concernent d'autres acteurs et ce suivant leur rôle précis lors des diverses étapes qui mènent de la conception à l'exploitation du système d'IA : les producteurs, les distributeurs, les importateurs, les utilisateurs ayant recours à un système d'IA à haut risque dans le cadre de leurs activités professionnelles (telle une administration qui utilise pour sa gestion et la promotion de son personnel un système d'évaluation conçu, développé et commercialisé par une firme privée, même si paramétrée par l'administration cliente).

-
- (e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;
- (f) comply with the registration obligations referred to in Article 51;
- (g) take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements [for high-risk AI systems];
- (h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;
- (i) to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;
- (j) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements [for high-risk AI systems]. »

91 Art. 14.3 du Artificial Intelligence Act proposal : « *Human oversight shall be ensured through either one or all of the following measures:*

- (a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;
- (b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user. »

92 Les annexes VI et VII définissent la procédure soit légère et purement interne si le fournisseur (*provider*) s'appuie sur des systèmes se référant à des standards harmonisés, soit plus lourde, externe auprès d'un organe de notification (autorité de contrôle) si tel n'est pas le cas.

L'article 30 oblige les Etats-membres à créer une autorité dite de notification, « *responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring* ». Le texte soumet en outre à des obligations particulières de transparence certains systèmes d'IA (article 52) : il impose d'informer les personnes interagissant avec un système d'IA de la présence d'un robot comme interlocuteur, de l'utilisation de systèmes de reconnaissance d'émotions ou de profilage sur base de données biométriques, ou de manipulation d'images, de sons ou de vidéos relatives à des personnes (*deepfakes*).

La qualification de l'autorité publique comme fournisseur (*provider*) ou comme utilisateur (*user*) pourrait s'avérer délicate. Le fournisseur est en effet défini comme « *a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge* »⁹³, tandis qu'est, selon le texte, utilisateur « *any natural or legal person, public authority, agency or other body using an AI system under its authority [...]* »⁹⁴. Les autorités publiques entendant faire usage d'un système d'IA pourraient donc se voir considérées comme l'un ou l'autre acteur⁹⁵. Nous notons que si elles ne développeront que rarement le système elles-mêmes, elles sous-traitent à une entreprise soumissionnaire ce soin mais ce dans le cadre d'un cahier des charges précis et peuvent s'en réserver la propriété intellectuelle. Par ailleurs, elles pourraient souhaiter le mettre sur le marché sous leur propre nom. Seront-elles dans ces cas considérées comme « fournisseur » du système au sens du règlement (proposé) et devront-elles conséquemment remplir toutes les obligations listées aux articles 16 à 23, en ce compris l'établissement, la mise en œuvre,

93 Art. 3 (2) du Artificial Intelligence Act proposal.

94 Art. 3 (4) du Artificial Intelligence Act proposal.

95 Voir les propos de Kilian Gross (DG Connect, Commission européenne) lors du webinaire organisé par AI4Belgium : Towards a European AI Regulation, 18 mai 2021, rediffusion disponible en ligne sur <https://www.youtube.com/watch?v=pumw6QOwOBs> (consulté le 31 mai 2021), à 1h31.23min.

la documentation et le maintien d'un système de gestion des risques tel que défini à l'article 9 ? Dans la plupart des cas, elles devront également évaluer la conformité du système avec le règlement, conformément à l'annexe VI. Cela nécessitera certainement la formation d'une nouvelle équipe d'experts au sein du secteur public. Nous notons à cet égard que les « *notified bodies* » instaurées par le règlement évalueront la conformité des systèmes d'IA à haut risque avec le règlement seulement dans le domaine de l'identification biométrique et catégorisation des personnes physiques⁹⁶. Il pourrait pourtant être intéressant de soumettre d'autres systèmes à un tel audit externe, en particulier lorsqu'ils sont utilisés par les autorités publiques.

Dans le cas où l'autorité publique est considérée comme « utilisateur » du système, ce sont les obligations listées à l'article 29 qui lui incombent : respect des « *instructions for use* » ; relevance des données d'apport ; suspension de l'utilisation et information du fournisseur ou distributeur en cas d'identification de risque⁹⁷, incident sérieux ou mauvais fonctionnement du système⁹⁸ ; et conservation des *logs* générés automatiquement par le système d'IA à haut risque dans la mesure où ces *logs* sont sous son contrôle.

Si le texte impose certaines obligations de transparence à charge du fournisseur du système d'IA à haut risque (article 13), celles-ci pourraient s'avérer insuffisantes en cas d'utilisation par une autorité publique. N'est-il pas en effet essentiel que toute personne faisant l'objet d'une décision administrative en comprenne les motifs de droit et de fait ? Or, la transparence imposée par le texte ne vise qu'à permettre à l'utilisateur d'interpréter les résultats donnés par le système et d'utiliser le système de manière appropriée⁹⁹. La nécessaire transparence du service public impose pourtant que les algorithmes utilisés soient publiés. Ainsi, l'autorité publique, qu'elle soit considérée comme « fournisseur » ou comme

96 Article 43 du Artificial Intelligence Act proposal.

97 Au sens de l'article 65.1 du règlement proposé.

98 Au sens de l'article 62 du règlement proposé.

99 Voir le libellé du §1 de l'article 13 du règlement proposé.

« utilisateur », devrait publier les algorithmes qu'elle utilise dans le cadre de sa mission de service public, et fournir aux administrés des explications quant à toute décision prise à leur égard, conformément aux obligations de motivation formelle. En Belgique, une proposition de loi récemment déposée vise ainsi à assurer la transparence quant à l'utilisation d'algorithmes, en obligeant les administrations :

- « à publier en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsque ceux-ci constituent tout ou partie du fondement des décisions individuelles;
- pour tout document administratif à portée individuelle, à communiquer à la personne faisant l'objet d'une décision individuelle prise en tout ou en partie sur le fondement d'un traitement algorithmique, les caractéristiques de cet algorithme;
- à publier l'analyse d'impact des outils mis en place par l'administration, qui est effectuée en vertu de l'article 35 du Règlement général sur la protection des données (RGPD) »¹⁰⁰.

100 Chambre des représentants de Belgique, 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 les administrations, DOC 55 1904/001, 6 avril 2021.

Conclusions

Les textes européens se succèdent à un rythme effréné. Leur lecture laisse clairement entendre le besoin d'une 'révolution' dans la conception et le fonctionnement de nos services publics, à l'occasion d'une utilisation croissante de l'IA, dont chacun mesure à la fois les risques et les bénéfices. Ainsi, cette utilisation implique que l'administration, élargie à l'ensemble des entités dont la mission est de servir l'intérêt général, se transforme en une large plateforme informationnelle travaillant avec des logiciels ouverts, des bases de données répertoriées et des données identifiées, interopérables et de qualité. Les lois de protection des données relayées par des mécanismes de compliance interne veilleront à structurer le fonctionnement de cette plateforme qui permettra le partage des données tant interne au secteur public, qu'externe au bénéfice des citoyens et des entreprises, appelés à collaborer par leurs propres données à nourrir les mégadonnées du secteur public. A cet égard, il est intéressant de noter que la politique européenne de la donnée et de l'IA contribue à estomper les frontières autrefois rigides entre le secteur privé et le secteur public et, en tout cas à instaurer entre eux une politique de partage des données. Ainsi, le document stratégique évoque le besoin d'une véritable politique de coopération entre ces secteurs : *« renforcer les mécanismes de gouvernance au niveau de l'UE et dans les États membres présentant un intérêt pour l'utilisation de données transsectorielles et pour l'utilisation de données dans des espaces de données communs sectoriels, associant des acteurs privés et publics. Il pourrait notamment s'agir d'un mécanisme permettant de fixer des priorités pour les activités de normalisation et d'œuvrer à une description et une vue d'ensemble plus harmonisée des séries de données, des objets de données et des identificateurs de données afin de favoriser l'interopérabilité des données (c'est-à-dire la possibilité de les utiliser à niveau technique) entre secteurs et, le cas échéant, à l'intérieur des secteurs »*¹⁰¹

101 Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence, *op. cit*

L'obligation d'une gouvernance cohérente et collaborative de la donnée au sein du secteur public est la condition même du développement de l'IA. D'autres réflexions s'imposent en ce qui concernent la conception et l'utilisation des applications d'IA. Les autorités publiques, lorsqu'elles mènent des projets d'utilisation de système d'IA, devraient être conscientes des nombreux challenges ethico-juridiques qu'elles devront rencontrer. Le 'White Paper' italien de 2018¹⁰² relève neuf défis essentiels que rencontrent le développement et l'implémentation des technologies d'IA dans le secteur public. Sans les citer tous, relevons les défis éthiques qui nécessiteront la mise sur pied, réclamée dès maintenant par les autorités européennes, d'une procédure d'*'ethical value assessment'*, plus large que le '*Privacy Impact assessment*' et menée si possible avec l'appui d'une cellule multidisciplinaire au sein de cette administration¹⁰³. Nous ajoutons ceux relatifs à la mise à disposition au sein de l'administration d'un personnel de qualité et en corollaire, la nécessité de mise à niveau d'un personnel pas nécessairement adapté à cette révolution. On ajoutera le besoin d'une information et d'une adhésion des agents de l'administration et, au-delà, des citoyens qui doivent trouver dans cette utilisation de l'IA un service de meilleure qualité. Le défi de la transparence ou plutôt de l'explicabilité des systèmes IA et des décisions prises par ces derniers constitue un dernier défi. Promouvoir des « *best practices* », collaborer entre administrations, au-delà des frontières, risquer l'innovation grâce à des législations 'bac à sable', définir des cahiers des charges qui puissent répondre à toutes ces exigences, autant de chantiers enthousiasmants à la hauteur des espérances mises sur cette technologie.

102 Agency for Digital Italy and Department for Public Administration, *White Paper on Artificial Intelligence at the service of citizens*, mars 2018, disponible en ligne sur <https://libro-bianco-ia.readthedocs.io/en/latest/> (consulté le 5 mars 2021).

103 Sur ce point, nous soulignerons la nécessité d'une IA au service de la justice sociale.