European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 129-148
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 13

*Artificial Intelligence and Public Services – the Role of Public Authorities in the Service of the "Third Way" Drawn up by the European Commission**

Yves Poullet
(Professor Emeritus at the Faculty of Law of Namur)

ABSTRACT In the context of its famous "third way", the EU Commission develops a strong strategy for the development of an AI market founded on "Excellence and Trust" keywords. The public sector is expected to play an important role for achieving this goal. Diverse legal instruments are envisaged for supporting this increasing role. First, the "Open Data Directive" is revised in order to increase the volume and the data put at the disposal of the private sector and the citizens. Reciprocally, according to what EU Commission calls 'The reverse PSI', the public sector would be able to receive data from the companies or directly from the citizens in order to contribute, thanks to the use of AI applications, to better public services and decisions. The Data Governance Act presently in discussion at the EU level organises these exchange between Private and public sector and fixes certain conditions for the ' data Altruism'. As regards the development or the use by the public sector of AI applications, we have to refer to another draft EU regulation: the AI Act. The Proposal distinguishes according a risk based approach different categories of AI applications, especailly it fixes a procedure of assessment and ethical values and principles to take into consideration throughout the entire cyclus of life of these applications.

1. *Introduction*

Europe pursues, at least at will of European Authorities and in particular of its President, a "third way"[1] for development of artificial intelligence qualified "*Excellence and Trust*" by the White Paper on AI[2]. By this strategy, the European Union aims to gain global leadership[3] of this profoundly innovative technology through the applications that the "third way" allows. Another complementary aim of this strategy is the theme: "Data for the public good", described as follows by the Strategy document: "As developed, Data is created by society and can serve to combat emergencies, such as floods and wildfires, to ensure that people can live longer and healthier lives, to improve public services, and to tackle environmental degradation and climate change, and, where necessary and proportionate, to ensure more efficient fight against crime. Data generated by public sector as well as the value created should be available for common good by ensuring, including through preferential access, that this data is used by researchers, other public institutions, SMEs or start-ups. Data from the private sector can also make a significant contribution as public goods. The use of aggregated and anonymised social media data can for example be an effective way of complementing the reports of general practitioners in case of an epidemic."[4]

* Article submitted to double-blind peer review.
This article could not have been written without the support of the Digital Agency of the Walloon Region (AdN) (Belgium) in the context of a report commissioned to CRIDS/NADI (University of Namur) on the legal and ethical framework for the development of AI services by the Walloon authorities.

[1] The "third way" in which the European Union intends to pursue an AI development policy based on principles different from those underlying in the two present leader of the AI market: on the one hand, the American policy which, without doubt, will be summarized by a 'whole to the market' and, more precisely by the will to maintain and develop the American leadership and, on the other hand, the Chinese policy marked – but no doubt we are close to the caricature – by a state interventionism and an AI at the service of the economy, social governance by the State and the security of the State.

[2] European Commission, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, Brussels, COM, 2020, 65 final, 8.

[3] Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data*, Brussels, COM, 2020, 66 final: "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 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".

[4] Commission to the European Parliament, the Council, the European Economic and Social Committee and the

All these elements of the EU Strategy lead to a new approach of the public sector. This European strategy is based on a strengthened role of the public service, considered, from one part, as an operator of new and innovative services using AI system and, from the other part, as a contributor to the development of 'big data' exploitable by the private sector. If this second role is classic even if recent initiatives tend to extend it (Chapter § I), the first one is more innovative.

If the public sector must be grant in position of developing innovative AI systems in the general interest, it needs to have the possibility to enrich its data with data from the private sector, especially as regards certain domains like for instance energy, mobility and health. From now on - it is at least the EU Commission intention -, the public sector will be in position to receive data from the private sector. To be more explicit, while the provision of public sector data for the benefit of the private sector has been a focus for more than a decade in Europe, a new policy, called "reverse *PSI*", is initiated by the E.U. Commission. This strategy aims, in the name of public interest to design a legal framework ensuring possible transfers of data from private to public sector. That data sharing B2G will nourish that big data indispensable for the development of AI services within the public sector. Chapter 2 will develop this point.

Finally, if the public sector has to be a development engine of AI deployment, its AI systems use or development must be a model as regards the respect of ethical and legal framework in order to create the needed trust among citizens and the socio-economic world. Different risks might be evoked: attempts on individual liberties but also on competition, risks of discrimination and also risk to democratic functioning of our society. A last chapter is devoted to future regulation of AI systems and its application within public services. Public services must design and operate AI tools to serve public interests and citizens and taking care not only of individual interest but also of collective and societal ones. Thus, we will examine in the Chapter III the tools available to the public sector to encourage the adoption of AI tools but also some elements of the proposed EU regulatory framework applicable to AI and thus especially to the AI developed or used by the public sector.

2. *Chapter I: The open data directive – towards an enlargement of the information flows G2B*

It is quite clear that machine-learning systems need big data in order to be efficient. In order to have EU big data not depending on the US GAFAM or Chinese BATX companies, the EU promotes a policy of data sharing between EU companies at the sectoral level[5] or not, taking into account the economic value of the data. The recognition of data as a new oil engine[6] indeed requires a policy of free circulation of data. In that perspective, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 establishes a framework for the free flow of non-personal data in the European Union[7], advocates data availability

Committee of the Regions, *A European strategy for data,* Brussels, COM, 2020, 66 final, 4.

[5] See for instance at the mobility sector, the idea of a "Software republic" launched by the Renault CEO, L. de Meo, allowing its founding members to pool their expertise on the topics of mobility, artificial intelligence, big data, or cybersecurity to create the mobility solutions and systems of tomorrow.(On that issue, see M.C. Selmer, *Cinq leaders mondiaux s'unissent pour lancer la software république, un écosystème d'open innovation pour la mobilité*, in *Magazine Forbes,* 2021, available on: www.forbes.fr/technologie/cinq-leaders-mondiaux-sunissent-pour-lancer-la-software-republique-un-ecosysteme-dopen-innovation-pour-la-mobilite.

[6] European Parliament Research Service (EPRS), *Is data the new oil? Competition issues in the digital economy,* 2020, available on: www.europarl.europa.eu/thinktank/pl/document.html?reference=EPRS_BRI%282020%29646117.

See also: "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*"* (Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, A European strategy for data,* Brussels, COM, 2020, 66 final).

[7] The distinction between personal data and not personal data might be criticized at a moment where the reality shows that the frontier between the two categories is

and data portability for business users. The document does underline the absolute necessity of data sharing[89] as a prerequisite for the creation of Big Data[10] specifically European which in turn constitutes a condition for the emergence of applications of AI. Therefore, we might understand the European willingness, including for sovereignty reasons, to build up these[11] European big data. After first preliminary documents in 2018[12], an High Level Group of Experts on Business to Government Data Sharing has been nominated by EU Commission and this experts' group produced its report[13], which was presented by the EU Commission, February 19, 2020 as an integral part of the EU Commission Data Strategy.

EU Commission has undertaken a number of initiatives under this policy. The launch of a European cloud that guarantees users the lack of surveillance by police or intelligence authorities is probably worth noting, while use of the cloud by our companies remains behind. The proposed regulation on European data governance (Data Governance Act) presented on November 25, 2020 deserves our attention. We will come back to that point, when it comes to analyse role that the European Union wishes to give to public services in its AI policy. Let us note right now that the instrument aims to promote the availability of data for use, increasing trust in

more and more flaw and the possibility of our computers makes the possibility of re-identification of so-called "anonymous" data still more possible. On that point, B. van der Sloot, *Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation?*, in *International Data Privacy Law*, 2014, 3: "Finally, this trend of a widening scope may also be witnessed in the proposal for a General Data Protection Regulation, which will replace the Data Protection Directive over time, in which personal data is defined in a slightly broader manner. The reason for this, as is acknowledged by the Working Party and is increasingly emphasized by scholars, is that potentially all data could be personal data. Data which at one moment in time may contain no information about a specific person whatsoever, may in the future be used, through advanced techniques, to identify or individualize a person". See also, our reflections and referrences in Y. Poullet, *L'IA un défi pour nos législations vie privée*, in A. Espiney and S. Rovelli (eds.), *L'intelligence artificielle et la protection des données. Actes des 3èmes journées suisses du droit de la protection des données*, Fribourg, Schultess, 2021, n. 42, 23 and ff.

[8] Regulation (E.U) n. 2018/1807 on the free flow of non-personal data in European Union, PE/53/2018/REV/1, in *JOUE,* 2018, 59-68.

[9] See the definition given by the art. 2.7 of the EU proposal of a Data Governance ACT: "'data sharing' means the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary".

[10] See, the conclusions (pp. 6 et 7) on that point of the EPRS document quoted footnote 6: "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".

[11] This policy of encouraging data sharing within and beyond the sectors but between the public and the private might be explained by the absence in the European Union of champions of big data such as the American (GAFAM) and Chinese (BATX) platforms. The need to build up these European big data public or private, creating between public and private sectors imposes virtuous mechanisms of solidarity. So, the EU Commission encourages this data sharing in eight sectors: finance, mobility, energy, manufacturing, environment, agriculture, health, space… And public administration. On that sectoral approach without excluding the transversal and cross-sectoral one, see European Parliament resolution of 25 March 2021 on *a European Data Strategy* (2020/2217(INI): available on Texts adopted - European Data Strategy - Thursday, 25 March 2021 (europa.eu): "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".

[12] Commission Staff Working Document. Guidance on sharing private sector data in the European data economy: Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards A Common European Data Space*, Brussels, COM, 2018, 232 final.

[13] *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, Luxembourg, Publications Office of the European Union, 2020. On this very important report, see our analysis: Y. Poullet, *From open data to reverse PSI – A new European policy facing GDPR*, in *European Public Mosaic*, 2020, vol. 11, 42-58.

data intermediaries and strengthening data-sharing mechanisms across the EU. The four objectives are: [14]

- making public sector data available for reuse, where such data is subject to the rights of others (we will return to this point);
- data sharing between companies, for remuneration in any form;
- allow the use of personal data with the help of a "personal data sharing intermediary", designed to help natural persons exercise their rights under the General Data Protection Regulation (GDPR);
- allow data to be used for altruistic reasons.

The first and the third objectives pursued by the draft Data Governance Act extend the scope of the Open Data directive modified at different times[15] but recently in 2019. The main aim of this enlargement is to maximize the contribution of the public sector to the development of the private information sector, particularly by facilitating the setting-up of big data[16]. Europe promotes the widest possible use of public sector data by the private sector. The idea that data that has been generated at the expense of public budgets should benefit society has been part of Union policy for a long time. We do insist about the broad definition of the public sector given by the EU Commission proposal covering not only public sector administrations and bodies at strict sense but also public undertakings.

Different points might be underlined.

Firstly, draft regulation definitively draws inspiration from principles for data management and re-use developed for research data. The FAIR data principles[17] stipulate that such data should, in principle, be findable, accessible, interoperable and re-usable. The article 10.1 mentions these principles expressly as regards the research data imposing to member States to adopt actions "at making publicly funded research data openly available ('open access policies'), following the principle of 'open by default' and compatible with the FAIR principles" but implicitly also as regards the other public bodies covered by the Directive[18].

Secondly, the previous Directive excludes certain categories of data, which is not accessible due to commercial and statistical confidentiality and data for which third parties have intellectual property rights. In accordance with the GDPR, personal data fall outside the scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of data protection, privacy. The re-use of data, which may contain trade secrets, should take place without prejudice to Directive (EU) 2016/943 on trade secrets, which sets the framework for the lawful acquisition, use or disclosure of

[14] Proposal for a Regulation of The European Parliament and of The Council on European Data Governance, in *Data Governance Act*, Brussels, COM, 2020,767 final, 12020/0340.

[15] The legal framework for the reuse of public sector data by the European Union deserves some thought. We note that the European Union is in the fourth version of the legislative framework in this area since the Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. On that progressive extension, see Y. Poullet and N. Bontridder, *"Intelligence artificielle et services publics". Proceedings of the Colloquium of the Centre for Comparative Public Law (CDPC),* in *L'état digital/The Digital State*, Paris, University of Paris 1, 2022 (in press). Colloquium organized by in partnership with the Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro (Resp. L. Belli)

[16] "The current proposal complements the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive) 6 . This proposal addresses data held by public sector bodies that is subject to rights of others and therefore falls outside the scope of this Directive. The proposal has logical and coherent links with the other initiatives announced in the European strategy for data. It aims at facilitating data sharing including by reinforcing trust in data sharing intermediaries that are expected to be used in the different data spaces" (Proposal for a Regulation of The European Parliament and of The Council on European Data Governance, in *Data Governance Act*, Brussels, COM, 2020,767 final).

[17] www.force11.org/group/fairgroup/fairprinciples.
These principles initially were published for *Scientific Data*. The authors intended to provide guidelines to improve the capacity of computational systems to find, access, interoperate, and reuse data with little or no human intervention. The 2017 Tallinn EU Ministerial Declaration on e-Government calls on governments to "increase the findability, quality and technical accessibility of data in key base registers" and suggests extending these principles to the private sector in order to facilitate sectoral and inter-sectoral data sharing. On a complete description of these principles, have a look at the website: www.go-fair.org/fair-principles. See also the article of M. Wilkinson, *The FAIR Guiding Principles for scientific data management and stewardship*, in *Nature Scientific Data*, 2016; available at https://scholar.harvard.edu/mercecrosas/publications/fair-guiding-principles-scientific-data-management-and-stewardship.

[18] See notably as regards the "public undertakings", the article 9.2: "Member States shall, in cooperation with the Commission, continue efforts to simplify access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the documents to which this Directive applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means".

trade secrets. All these limitations might prejudice the creation of a real information and data market useful for the private sector. Therefore, the use of certain personal data, if necessary, after pseudonymization and strict control of compliance with data protection rules could be useful for companies in the private sector. Companies who wish to reuse them can also use documents, inventions or data covered by intellectual property rights[19]. The proposed regulation intends to allow and promote[20] this access while setting, without now prohibiting it, conditions for this reuse of data in full compliance with competition law and under non-discriminatory conditions. Article 5.2 enunciates: "Conditions for re-use shall be non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed. These conditions shall not be used to restrict competition", must be published and might contain complementary obligations imposed by public sector bodies as regards the pseudonymisation of the data, the security measures, the need for obtaining consent from data subject with the assistance of the public bodies, the respect of Intellectual Property rights, …. Public sector bodies might impose the control of the respect of these conditions. Art. 6.1 provides: "Public sector bodies which allow re-use of the categories of data referred to in Article 3 (1) may charge fees for allowing the re-use of such data".

Thirdly, Governance Act encourages data sharing solutions but regulates status and the functioning of the data providers sharing services (*data intermediaries*), "that have as a main objective the establishment of a business, a legal and potentially also technical relation between data holders, including data subjects, on the one hand, and potential users on the other hand, and assist both parties in a transaction of data assets between the two[21]". The text underlines their needed independence from both data holders and data users in order to avoid the emergence of player with a significant degree of market power (articles 9 and ff.). It provides specific obligations for providers of data sharing working on personal data[22] and imposes conditions for providing their services especially the obligation of notifying their activities to a competent authority[23] (art. 10) but also the fact that they might not use the data for other purposes than to put them at the disposal of data users, the transparency and the non-discrimination of their conditions, the security and continuity of their services (art. 11).

In the conclusion of this chapter, two main trends must be underlined regarding the role of the public sector *vis-à-vis* the private sector. From now on, it is wished that the public sector, as a counterpart of its active role to share its data to the benefit of the private sector, will develop an active role in the control of the functioning of the private information sector. State has both to ensure maintaining of a competitive market respectful of the human liberties (IPR and data protection especially) but also to proactively encourage the data sharing. Precisely on that second point, as the HLGE on B2G Data sharing[24]: "Member States should put in place

[19] The example of access to research, sponsored by an administration, conducted on the basis of questionnaires can be cited. This example combines documents and data that are both protected by intellectual property rights and some constitute processing of personal data. Companies may wish to have access to items collected and produced for research for marketing reasons or to improve their product service.

[20] Art. 7.2 pinpoints the role of competent authorities nominated by Member States in order to provide support for providing this access for the re-use of data (including technical support of tested techniques ensuring data processing in a manner that preserves privacy of the information contained in the data for which re-use is allowed, including techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data.

[21] See point 22 of the *Explanatory Memorandum* of The Data Governance ACT, in discussion.

[22] See point 23 of the text: "They would assist individuals in exercising their rights under Regulation (EU) 2016/679, in particular managing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure or right 'to be forgotten', the right to restrict processing and the data portability right, which allows data subjects to move their personal data from one controller to the other. In this context, it is important that their business model ensures that there are no misaligned incentives that encourage individuals to make more data available for processing than what is in the individuals' own interest. This could include advising individuals on uses of their data they could allow and making due diligence checks on data users before allowing them to contact data subjects, in order to avoid fraudulent practices".

[23] See the multiple provisions as regards these "competent authorities", notably their status, their independence, the procedure to be followed in case of complaints against a provider lodged (article 12). Furthermore, the Text sets-up a EU Data Innovation Board, expert group in charge to advise and assist the Commission, in developing notably a consistent practice of public sector bodies and competent bodies (art. 27 and 28).

[24] See European Commission, *Towards a European*

national governance structures that support B2G data sharing: a recognised data steward function should be created and promoted in both the public and private sectors. The European Commission should encourage the creation of a network of such data stewards, as a community of practice in the field; B2G data-sharing collaborations should be organised: – in testing environments ('sandboxes') for pilot testing ('pilots') to help assess the potential value of data for new situations in which a product or service could potentially be used ('use cases'), via public-private partnerships[25]". The main aim of all these initiatives suggested by the HLGE would be to foster a data culture within the public sector and at the same time to oblige the public sector, through what the Report call: Data stewards, to have a better knowledge of its informational richness and their potential uses by the private sector[26]. That will be the role of data stewards called 'competent bodies' by the Data Governance Act[27]. At the same time, as extensively demonstrated by the Report, the public sector might be interested by the information held by the private sector in order to ameliorate the public service or to have the means for a better definition of its public strategy. That implies B2G information flows, the other part of the European Data Strategy, better known as 'reverse PSI', object of our Chapter II.

3. *Chapter II: The EU 'Reverse PSI' Policy: the "Data Altruism" or the data flows from the private sector to the public sector (B2G)*

The shift we are describing reverses the traditional unilateral direction of flow, coming from administration to the private sector. It is now the public authorities that have become the recipients of flows from the private sector, hence the name "reverse PSI Policy"[28]. The concept of *reverse PSI* refers to the Public Sector Information (PSI) Directive, which creates a right to re-use all public documents (data) held by Member States' public sector bodies. Reversing the concept of the PSI Directive would entail access by public sector bodies to re-use privately held data.

Reason for this new EU Commission policy seems twofold. Firstly, the public authorities wish to be able to use artificial intelligence (AI) tools both to define their policies and to ensure their effectiveness. Let us take two examples: creating urban traffic plans requires the possibility for public mobility agencies to process, through machine learning systems, precise and huge traffic data. If the public authorities had to put technical means in place to measure it, collection would cost a hundred times more than access to data that transport and navigation software companies or collaborative platforms such as UBER or WAZE are collecting as part of the services they offer. Second example: matching supply and demand for employment together in the best possible way require for public employment agencies (our public employment assistance agencies) to have detailed socio-economic data from companies or professional associations, their forecasts as

strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing, Brussels, 2020, 7.

[25] The question to conciliate that idea of PPP and the requirements of the public procurement legislations remains delicate.

[26] "A key success factor in setting up sustainable and responsible B2G partnerships is the existence, within both public- and private sector organisations, of individuals or teams that are empowered to proactively initiate, facilitate and coordinate B2G data sharing 38 when necessary. As such, 'data stewards' should become a recognised function (74). A data steward should have the required expertise and authority to look for opportunities for productive collaborations or to respond to external requests for data. The primary role of the data steward is to systematise the process of partnering and help scale efforts when there are fledgling signs of success. Some of these tasks might already be carried out by one or more individuals within an organisation, such as a chief data officer, open data officer or chief digital officer. It would be beneficial to group some of these functions together with additional functions in the data steward role" (European Commission, *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 40). About the five missions to be devoted to the data stewards, read S. Verhulst, *The three goals and five functions of data stewards*, in *Medium,* 2018, available on: https://medium.com/data stewardsnetwork/the-three-goals-and-five-functions-of-data-stewards-60242-449f378.

[27] Art. 7.1: "Member States shall designate one or more competent bodies, which may be sectoral, to support the public sector bodies which grant access to the re-use of the categories of data referred to in Article 3 (1) in the exercise of that task".

[4] Commission Staff Working Document, *Towards A Common European Data Space*, in *Guidance on sharing private sector data in the European data economy Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM, 2018, 232 final.

regards their future activities but also data about the present educational programmes existing within the country. AI systems mixing all these data would contribute to guide training efforts' programmes and in concrete cases, where a company is searching for employees, the AI systems will help to better correlate job seekers and existing vacancies. Since AI requires the existence of a sufficiently rich and numerous data set so that complex *machine learning* algorithms can identify statistically significant correlations.

The second reason, in the case of a public authority, is that the source of the data collected was traditionally internal to the public authority. It was only rarely external and even then, limited to very specific files. As the examples show, the need for the administration to use the most adequate technologies to define and achieve the 'common good' (and AI can do this if certain conditions are met) justifies access by the administration to data collected only by the private sector. Last but major point; –if public authorities do not have such access, they find themselves in a position of inferiority and at the mercy of private operators that have more accurate, available and up-to-date information.

The Data Governance Act intends to create the future legal framework of this 'reverse PSI' policy. That will answer to the observation made by the Commission and expressed in its document "A European strategy for Data", "Use of privately-held data by government authorities (business-to-government – B2G – data sharing). There is currently not enough private sector data available for use by the public sector to improve evidence-driven policy-making and public services such as mobility management or enhancing the scope and timeliness of official statistics". Many provisions (See Chapter IV 'Data Altruism' of the Data Governance Act proposal) are dealing with what the proposal calls after the authors of the HLGE Report: the 'data altruism' defined as follows: "the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services". The purpose pursued by this policy is to maximize the possibility of using data including personal data coming from the private sector when these collections deserve the general interest. As asserted by the Proposal: "There is a strong potential in the use of data made available voluntarily by data subjects based on their consent - in the sense of the GDPR definition and thus with the same requirements as regards its validity - or, where it concerns non-personal data, made available by legal persons, for purposes of general interest. Such purposes would include healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well as purposes of general interest. This Regulation aims at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union"[29].

One might summarize the proposal as follows. The draft imposes the passage by specific organisations: the 'Data Altruism organisations', recognized by the 'competent authority' in charge of recognizing, registering and monitoring the compliance with the legal requirements of these organisations. A lot of conditions (article 16) are required from these latter. "In order to qualify for registration, the data altruism organisation shall: (a) be a legal entity constituted to meet objectives of general interest; (b) operate on a non-profit basis and be independent from any entity that operates on a for-profit basis; (c) perform the activities related to data altruism take place through a legally independent structure, separate from other activities it has undertaken".

As regards their functioning, certain things are required (articles 18 and 19), first, the transparency of the beneficiaries of the data[30]

[29] See the European Commission, *Explanatory Memorandum,* in *The Data Governance ACT*, Brussels, 2020, vol. 35, 20.

[30] "Business-to-government data collaborations should be transparent about the parties to the collaboration and their objectives. Where possible, public bodies should also be transparent on the data that has been used and the algorithms applied, as well as on the results of the collaboration, including the relation to subsequent decision-making and the impact on individuals. Moreover, public bodies should ensure ex post transparency to the private companies and civil-society organisations on

and the purposes of these uses; second, the transmission of a report to the national competent authority described *supra*; third, the information to the consenting data subject about the purposes pursued by the different data users and therefore by the different public entities using his or her data. The draft establishes that "these organisations playing the role of interface shall ensure that the data is not to be used for other purposes than those of general interest for which it permits the processing". Therefore, in case of non-respect of the legal provisions, the liability for this non-respect will be supported not by the entity, which was the initial depositor of the data, but by these intermediaries, designed as "data Altruism organisations". As stated in the HLEG commissioned by the EU Commission, in its B2G data sharing report, one can imagine citizens themselves, with their consent, wishing to contribute to the public interest by offering their data. Article 22 gives to the EU Commission the competence to adopt a regulation developing a uniform "data altruism consent form" with a modular approach allowing customization for specific sectors and for different purposes and according with GDPR requirement, the possibility for data subjects to easily withdraw their consent.

Additional reflections could be addressed due to the GDPR application to these B2G data flows. As stated in the HLEG in the B2G data sharing report commissioned by the EU Commission, one can imagine citizens themselves, with their consent, wishing to contribute to the public interest by offering their data. The required consent must be free, informed and unambiguous. This consent might be easily withdrawn according with the GDPR provisions and the organisation will have to ensure this possibility not only as regards their own processing but also as regards the data users' processing. Furthermore, such flows or data sharing can only be justified under Article 6 of the GDPR in the context of a specific public interest purpose, previously set within the context of a "law" in the broad sense of the term, which is transparent, proportionate and necessary in a democratic state. Therefore, the public authority must define the purposes of the B2G data sharing[31].

The public authority must thus precisely define the purposes pursued: for instance, assistance to unemployed people; conception of urban planning; definition of a transport policy; medical research as regards a certain type of disease, etc. We also cannot exclude control of tax or benefit fraud[32]. It is important for the authority to be able to clearly demonstrate that the public interest benefits are greater than the disadvantages for citizens or economic partners. There can be no question of creating big data that can be used for all 'useful' public interest purposes; only those that come within the framework of explicit legal purposes compatible with the GDPR. With the exception of statistical offices, whose operation is subject to strict confidentiality rules, there can be no question that decisions should depend by only on negotiations between supplier companies and the administration[33]. If law provides for possibility of citizens providing data concerning themselves collected or processed by private sector, that consent can only be given within the framework of the legal purposes pursued.

It is in light of such purposes that the extent and quality of the data requested from the private sector should be assessed. Such purposes will determine the extent and quality of the data requested from the private sector, the degree to which data is provided raw or aggregated, and the frequency of updates and access. However, this principle of minimization, called for by the group of

which particular public interest has been advanced with the use of their data and how, and cases where the data has not been used. Good practices should be made publicly available" (European Commission, *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020, 45).

[31] The French Act (Loi du 7 octobre 2019 pour une république numérique, Art. 17 and following) is very interesting regarding this point. It allows the public sector to access data held by the private sector in certain contexts and obtain them from certain actors when it is in the public interest.

[32] The HELG report (i.e., European Commission, *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020) excludes them since it would give B2G data sharing a poor image. Another purpose is excluded: use of private sector data for commercial purposes. It is quite clear that commercialization would go beyond the role of public administration and distort the competitive private market.

[33] This does not exclude discussing the forms of the data flow with the companies (format, compensation for the costs they have incurred, etc.).

experts[34] poses difficulties when it comes to the public authority setting up artificial intelligence systems, especially those that are unsupervised and involve deep learning. These systems are characterized by the fact that the system provides significant correlations without knowing what data will be useful at the outset. Notwithstanding this precaution, we should take into account, firstly, that the administration already has certain data and that there can be no question of duplicating sources. Secondly, we should consider sorting useful data after some testing and, perhaps, experimentation.

To conclude that second chapter, it is quite noteworthy that in the same proposal, the EU Commission tries to find a compromise between the interests of the private sector[35], by enlarging where possible the possibilities of data flows from public authorities to private entities and, in the other sense, the general interest pursued by the public authorities, by giving the possibility even if limited of contributions coming from the private sector to the public one. That double movement increases the cooperation between the two sectors and contributes to making the frontier between them more and more difficult to delineate. "The Commission is convinced that businesses and the public sector in the EU can be empowered through the use of data to make better decisions. It is all the more compelling to seize the opportunity presented by data for social and economic good, as data – unlike most economic resources – can be replicated at close to zero cost and its use by one person or organisation does not prevent the simultaneous use by another person or organisation. That potential should be put to work to address the needs of individuals and thus create value for the economy and society. To release this potential, there is a need to ensure better access to data and its responsible usage"[36].

Many questions about conditions as regards cooperation of private sector to the public good would have to be enacted if we want to install an effective cooperation. Definitively it would be useful to define legal instruments and develop incentives for accelerating this data sharing[37]. Pilot actions would be developed in the context of sandboxes legislations. On that point, it would be interesting to take a look again at certain principles published by the European Commission in its staff working document entitled "Guidance on sharing private sector data in the EU data Economy"[38] and revised by the already cited HLGE report on B2G data sharing[39]. Particularly, solutions must be given - to the problem of risk mitigation[40] (it means

[34] "The requested private-sector data should be necessary, relevant and proportionate in terms of detail (e.g. type of data, granularity, quantity, frequency of access) with regard to the intended public interest pursued" (European Commission, *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020, 80).

[35] The specific position of SME is taking also into account. As mentioned by the Data Governance Act Proposal, it will be one of the role of the Data cooperatives (European Commission, *Explanatory Memorandum*, in *Regulation of the European Parliament and the Council,* n. 24, 17): "Data cooperatives (in the text also called Data sharing service providers) could also provide a useful means for one-person companies, micro, small and medium-sized enterprises that in terms of knowledge of data sharing, are often comparable to individuals". See on that point, article 9(1) c) of the Proposal.

[36] Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data,* Brussels, COM, 2020, 66 final, 3.

[37] T. Klein and S. Verhulst, *Access to new data sources for statistics: business models and incentives for the corporate sector*, in *OECD Statistics Working Papers*, Paris, OECD Publishing, 2017, vol. 6, available on https://doi.org/10.1787/9a1fa77f-en. European Commission, *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020, 41, describes certain instruments which might envisaged for developing that cooperation.

[38] This document dated from April 25, 2018 has been published as an annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a common European data space*, COM, 2018, 232 final.

[39] European Commission, *Towards a European strategy on business-to-government data sharing for the public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020, 81.

[40] "The risks, including damage due to the request for and use of private-sector data, should be taken into account and mitigated. Business-to-government data collaborations must ensure that legitimate private-sector interests, notably commercially sensitive information such as trade secrets, are respected. They should allow private companies or civil-society organisations to continue to be able to use and monetise the private-sector data in question as well as derived insights to their benefit. Private companies and civil-society organisations should not be held liable for the quality of the data in question or its use by public authorities for public-interest purposes. Public-sector bodies may not use private-sector data for commercial purposes or to compete

the fact that the interests of the private sector to see their data protected and to be able to continue the financial and commercial exploitation of its data will not be damaged);

- to the level of compensation to give to the private sector in case of transmission or adaptation of their data bases to the need of the public sector[41];
- to the problem of support from the private sector or intermediaries as regards the quality of data, the absence of bias as regards the selection of data [...][42].

Furthermore, ethical principles are required, since the public authorities will process the data obtained through AI machine learning systems. The third chapter is precisely dedicated to the legal and ethical framework proposed by the Commission in that context.

4. *Chapter III. Public authorities as user of AI systems – Towards an ethical and legal framework?*

The White Paper[43], in its Section 8 entitled: 'Promoting the adoption of AI by the public sector', declares: "it is essential that public administrations, hospitals, utility and transport services, financial supervisors, and other areas of public interest rapidly begin to deploy products and services that rely on AI in their activities', 'with a specific focus in the area of healthcare and transport". Precisely with regard to the development of AI applications in the public sector, the Commission's strategic plan, published on April 21, 2021, contains a whole chapter (Chapter § 14) relating to its importance. It recalls crucial role that this technology can play in improving service to citizens, highlights the model for the private sector that the public sector can constitute by developing trustworthy and fully ethical AI systems and pleads for resources and adequate financial and human resources[44] [45].

commercially with a company that has similar offerings. The risk of not using private-sector data in relation to tackling well-defined societal challenges should also be taken into account. Business-to-government data-collaboration agreements or decisions should contain appropriate safeguards as regards the use of private-sector data in order to protect the rights (e.g. privacy, data security, non-discrimination) of stakeholders, in particular the individuals whose data is used" (p. 84).

[41] "Business-to-government data-collaboration agreements should seek to be mutually beneficial, while acknowledging the public-interest goal by giving the public-sector body preferential treatment. This should be reflected in the level of compensation agreed, the level of which should be determined taking into account the other principles" (p. 85).

[42] "To address the potential limitations of private-sector data, including potential inherent bias, private companies and civil-society organisations should offer reasonable and proportionate support to help assess its quality for the stated purposes (e.g. type, granularity, accuracy, timeliness, format), including the possibility to verify the data, wherever appropriate. Private companies and civil-society organisations should not be required to improve data quality at no cost" (p. 85).

[43] European Commission, *The White Paper on AI (Livre blanc sur l'intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance)*, Brussels, COM 2020, 65 final, 3, available on: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf, summarized this interest: "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". On the different reasons: optimisation, objectivation and security, why AI services deployment within public sector is justified, read Y. Poullet and N. Bontridder, *Intelligence artificielle et services publics*, in *Proceedings of the Colloquium of the Centre for Comparative Public Law* (CDPC, *L'état digital/The Digital State*, 2021, Paris, University of Paris 1, (in press). Made in partnership with the Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro, organized by L. Belli, 22.

[44] European 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*, Brussels, COM, 2021, 205 final.

[45] "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" (European Commission, *Annexes to the Communication*, 48, see note above). The text of the Annexes also promotes better collaboration between national administrations, announces the launch of a program (Adopt AI) particularly focused on the launch of AI projects in the public sector and addresses the issue of collaborative and cross-border public procurement, including the creation of a "*public procurement data space*". The Commission also intends to support the initiatives of administrations, cities (smart cities) and communities of citizens, on the one hand, by creating registers of trustworthy algorithms and applications and, on the other hand,

Profiling allows public authorities and administrations to pursue a variety of objectives[46]. First, it is useful in devising strategies, whether economic expansion policies, or policies on subsidised housing, mobility, education or employment assistance[47]. To this end, the authorities consider myriad factors and combine reams of data from public and private sources to produce "predictive models" for determining what impact a particular policy is likely to have. It is easy to see how, if not programmed correctly (bias, poor data quality or errors in the algorithms), activities of this kind could affect certain groups or, at any rate, how decisions based on such forecasts could affect the members of these groups[48]. One area where AI and profiling systems can be a ready source of efficiency gains is when it comes to implementing rules and regulations. As part of a philosophy of "benevolent government", where the state plays a proactive role with respect to its citizens, such systems can be used not only to spot or even select people who could benefit from special assistance, or to ensure students receive the best possible advice about education pathways, etc, but also to detect problem families (child abuse) or even social security fraudsters or tax evaders. Predictive justice, which is intended to replace judges, is also worth mentioning in this context insofar as any dispute can be "profiled" according to the many and varied characteristics of the case, analysed in the light of previous decisions

Before starting to analyse the ethical and legal framework surrounding the present and future development and usage of AI machine learning systems by the public sector, I would like to pinpoint two preliminary remarks. The first one underlines the fact that the creation of big data within the administration is facilitated by the extension of the notion of public sector. More entities are belonging to the public sector; thus it will be easier to collect data from all these various entities in order to create 'big data' and that even if the public authorities adopt a decentralized model with crossroad platforms of exchanges between the local databases. Therefore, beyond the extension already enacted in the Open Data Directive defining very broadly the "public sector"[49], recent EU Commission's texts, as the Data Governance Act proposal or the HLGE Report already cited, mentions the interest to encompass the data bases created or controlled by the local authorities in the context of their digital cities.

The second remark notes that the obligations created by the texts prescribing access to data held by the public sector help to

"*by developing a set of minimal capabilities for algorithms to be used in contract conditions*".

[46] G. Misuraca (ed.), *Exploring Digital Government transformation in the EU - Analysis of the state of the art and review of literature*, Luxemburg, Publications Office of the European Union, 2019, available on: https://doi.org/10.2760/17207;
G. Misuraca and C. van Noordt, *AI Watch - Artificial Intelligence in public services - Overview of the use and impact of AI in public services in the EU*, Luxembourg, Publications Office of the European Union, 2020, available on: https://doi.org/10.2760/039619.

[47] For information about various examples of decision-making systems in the public sector and in support of governmental strategies, see the report "*Automating Society - Taking Stock of Automated Decision-Making in the EU*": A report by Algorithm Watch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations, 2019, available on: www.algorithmwatch.org/automating-society.

[48] The problem of discriminatory impacts linked with the use of A.I. systems has been studied by numerous authors. See, notably, S. Barocas and A. D. Selbst, *Big Data's Disparate Impact*, in *California Law Review*, vol. 104, 2016, 671; A. Chouldechova, *Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments*, in *Big Data*, vol. 5, 2017, 153; S. Goel, M. Perelman, R. Shroff, and D.A. Sklansky, *Combatting Police Discrimination in the Age of Big Data*, in *The New Criminal Law Review*, 2017, 181.

[49] The Open data Directive enlarges the scope of the Directive both to research performing and research funding organisation (art. 10) and to public undertakings (article 1.1. b) defined as follows: undertakings:

(i) active in the areas defined in Directive 2014/25/EU;
(ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007;
(iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008; or
(iv) acting as Community shipowners fulfilling public service obligations pursuant to Article 4 of Regulation (EEC) No 3577/92". See also, the broad definitions given by article 2 (1) (2) and (3) of the notions 'public sector body', 'bodies governed by public law' and 'public undertakings'.

As regards the explanation of this extension, "Member States often entrust the provision of services in the general interest with entities outside of the public sector while maintaining a high degree of control over such entities. At the same time, Directive 2003/98/EC applies only to documents held by public sector bodies, while excluding public undertakings from its scope. This leads to poor availability for re-use of documents produced in the performance of services in the general interest in a number of areas, in particular in the utility sectors. It also greatly reduces the potential for the creation of cross-border services based on documents held by public undertakings that provide services in the general interest" (Explanatory Memorandum, n. 24).

intensify the circulation of data within the administration. Different reasons might be offered to explain that phenomenon, notably the obligation imposed by the Open Data directive to facilitate the access by private companies and thus the obligation to use the 'fair principles' and to adopt interoperable data and to have meta data correctly defined. We might add the fact that this circulation will be increased by the existence of 'authentic sources', which are able to ensure the quality of data and the possibility to avoid the administrative difficulties linked with the need to acquire the data directly from the citizen. Sharing data between public authorities can greatly contribute to improving public policies and services, and also to reducing the administrative burden on businesses operating in the single market (once-and-for-all principle)[50] . Having said that, it must be emphasized that this circulation must obviously take into account the rules imposed by administrative partitioning and the application of data protection rules[51].

Coming back to the topic of this third chapter: the ethical and legal framework of the development and usage of AI systems by the public service, we might confess that it is probably the most original but also the most difficult to achieve. It is quite clear that the temptation to use artificial intelligence in all areas of government activity[52] is great. AI algorithms are, may be and definitively will be used across the spectrum of government decision-making – from the drafting of legislation, to judicial decision-making, to the implementation of laws by the executive branch and internal decisions like the recruitment of civil servants. Definition of public strategies, improvement of administrative procedures and their monitoring and control might be achieved through the use of adequate AI systems. At the same time, for citizens, the application of AI technologies will result in a more personalized and efficient experience. For people working in the public sector it means a reduction in the hours they spend on basic tasks, which will give them more time to spend on innovative ways to improve services.

The desire expressed many times by the European authorities is to base the development of artificial intelligence tools and applications on two values: "Excellence and Trust", according to the very title of the White Paper on AI (White Paper on AI) of February 2020[53]. When announcing the European Union's "White Paper" on artificial intelligence, the President of the Commission stressed: "We want the application of these new technologies to be worthy of the trust of our citizens.... We encourage a responsible human-centred approach to artificial intelligence." Excellence is based on the development of cutting-edge scientific research that the European Union intends to finance alongside funding from each European State[54]. Trust in the applications of

[50] "Les internautes citoyens, gestionnaires et agents de l'État 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'État plutôt que d'en interdire la circulation", P. Trudel, *Gouvernement algorithmique et interconnexions de fichiers administratifs dans l'État en réseau*, in *Revista Catalana de Dret Public*, 2007, 206.

[51] For instance the AI system used by the Dutch administration for recruiting the civil servants (SIRRIS) has been considered by the Dutch Constitutional Court as non-constitutional due to data Protection infringements. On the data protection rules and their application by the public administrations, see E. Degrave, *L'e-gouvernement et la protection de la vie privée*, in *Cahiers du Centre de Recherche Informatique et Droit*, Bruxelles, Larcier, 2014, 237.

[52] The reader will find more developments on the multiple arguments developed for justifying the recourse by the public sector to AI systems, notably, Central, digital and data Office, *A guide to using artificial intelligence in the public sector*, 2019, available on www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector and the list of examples developed.

[53] European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, Brussels, COM, 2020, 65 final. The EU Commission summarizes (Excellence and trust in AI, Feb. 2020.pdf) the main points recommended by the White Paper as follows*:* "How to achieve EXCELLENCE?: Set-up a new public-private partnership in AI and robotics; Strengthen and connect AI research excellence centres; Have at least one digital innovation hub per Member State specialised in AI; Provide more equity financing for development and use of AI, with the help of the European Investment Fund; Use AI to make public procurement processes more efficient; Support the procurement of AI systems by public bodies. And TRUST?: New legislation on AI should be adapted to the risks, it should be effective but not limit innovation; Require high-risk AI systems to be transparent, traceable and under human control; Authorities must be able to check AI systems, just as they check cosmetics, cars or toys; Ensure unbiased data sets; Launch an EU-wide debate on the use of remote biometric identification (e.g. facial recognition)".

[54] In its annexes, the recent strategy document published by the EU Commission (*Annexes to the Communication from the Commission to the European Parliament, the*

artificial intelligence technology must allow the social acceptance of these, which is necessary for its development. As EDPB and EDPS affirm in their opinion about the draft regulation, "AI will enlarge the amount of predictions that can be done in many fields starting from measurable correlations between data, invisible to human eyes but visible to machines, making our lives easier and solving a great number of problems, but at the same time will erode our capability to give a causal interpretation to outcomes, in such a way that notions of transparency, human control, accountability and liability over results will be severely challenged"[55].

In this respect, the European texts note the risks inherent in "static and opaque" algorithms and the need to guarantee, from the design stage, the transparency and the explicability of algorithms, in order to prevent any discrimination related to automated decision-making. It is further recommended that ethical rules be put in place that incorporate the idea that AI is a "*human-centred technology*" which is conceived as a tool that helps and must be controlled by humans, and that its application must be carried out with respect for fundamental rights such as dignity, autonomy, self-determination, non-discrimination, respect for the environment and a democracy based on the rule of law". The societal responsibility of all actors involved in the development of AI tools is implied by compliance with this ethical framework.

The White Paper draws on the work of a high-level group of experts (HLGE on AI) promoted by the EU Commission, which resulted in ethical recommendations for a trusted AI system in April 2019 and more recently the publication of a list of criteria for assessing the seven characteristics of a trusted AI (ALTAI or[56]Assessment List for Trustworthy AI). With this ethical impetus from the Commission and in full consultation with the latter, the European Parliament responded with a resolution of 20 October 2020[57] containing recommendations to the Commission on a framework for the ethical aspects of artificial intelligence, robotics and related technologies[58]. Finally, on April 21 2021, the EU Commission put on the table its "Proposal for a Regulation of the EU Parliament and of the Council laying down harmonized rules on artificial intelligence and amending certain Union legislative Acts"[59] [60].

European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence, Brussels, COM, 2021, 205 final, 60.

[55] About The European Data Protection Board, *On that increasing possibilities for opaque profiling and the consequences on our liberties* (EDPB/EDPS Joint Opinion), see Y. Poullet and B. Frenay, *Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling*, report of The Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Convention 108, T PD(2019)07 Final, Strasbourg, 2020, available on: https://rm.coe.int/t-pd-2019-7final-en-2757-5764-0706-1-2776-1394-9442-1/1680a0925c.

[56] HLGE (High Level Group of experts on AI). About this group and its work, see https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence) and especially its publication *Des lignes directrices en matière d'ethique pour une ia digne de confiance*, 2019, available on: *Ethics guidelines for trustworthy AI - Publications Office of the EU*, available here: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai/. Seven ethical and legal criteria have been identified by the HLGE and detailed extensively: Human Agency and Oversight; Technical Robustness and Safety; Privacy and Data Governance; Transparency; Diversity, Non-discrimination and Fairness; Societal and Environmental Well-being; Accountability. On the evaluation methodology and the practical significance of each criteria, have a look at the Assessment List Trustworthy AI (ALTAI), see the web site https://futurium.ec.europa.-eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence**.**

[57] European Parliament resolution, 20 October 2020 containing recommendations to the Commission about a framework on ethical aspects of AI, robots and connected technologies (2020/2012(INL)) P9 TA (2020) 0275.

[58] The EU Commission proposal text of the proposed regulation put on the table on 21 April 2021 by the European Commission seems more pragmatic but less generous than the parliamentary text. It is indeed, says Ms Vestager during the presentation of the proposal, to implement through this text the very principles of excellence and trust: "In terms of artificial intelligence, trust is not a luxury but an absolute necessity. By adopting these landmark rules, the EU is taking the lead in developing new global standards that will ensure AI is trustworthy. By setting standards, we can pave the way for ethical technology around the world, while preserving the EU's competitiveness. Time-tested and innovative, our rules will apply when strictly necessary: when the security and fundamental rights of EU citizens are at stake".

[59] Brussels, COM, 2021, 206 final.

[60] The EU Commission proposal text of the proposed regulation put on the table on 21 April 2021 by the European Commission seems more pragmatic but less generous than the parliamentary text. On that comparison, see my reflections in "About some international documents relating to the ethics of artificial intelligence – Some insights", *to be published* in the book edited for the 40th birthday, 18 November 2021. It is indeed, says Ms Vestager during the presentation of the proposal, to implement through this text the very principles of excellence and trust: "In terms of artificial intelligence, trust

As clarified by Commissars VESTAGER, "The purpose of the proposal is fourfold*:*

- 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".

The text is still in discussion at different levels and is subject according to the EU Commission will to a large consultation. Nevertheless, it seems that the approach followed by the present proposal will remain and therefore deserves some comment about its implications on the AI systems' management by our public administrations. It is quite clear that the comment is strictly limited to the content of the proposed Regulation. Other legal aspects will not be covered, as liability, intellectual property, data protection, public procurement and public services obligations[61].

A few words on content of this proposal; it seeks to establish a compromise between legal and ethical requirements, reflecting the values of the Union and the need not to overly constrain technological development and initiatives.

The text contains a definition of artificial intelligence (art. 3 (1) and actors. "'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". Annex I thus refers not only to supervised or non-supervised "machine learning" techniques including deep learning, but also to so-called symbolic approaches based on expert systems (logic and knowledge based) and even statistical approaches including optimization methods. Thus, the concept brings together methods based on both systems for reconciling data operating more or less autonomously and opaquely and systems based on transparent logical reasoning. Obviously, the two categories do not present the same risks even if they might contain bias and lead to automated decisions and for that reason need to be subject to certain similar precautions.

As regards the actors, the proposal carefully distinguishes between AI suppliers, distributors, importers, operators and users operating in the context of their professional activities and those operating in the context of private activities. These distinctions are useful[62] because they make it possible, beyond need for interaction between these supply chain actors, to allocate to each specific responsibility.

Two remarks. First, the Proposal restricts only to "high risks systems" the provisions about these obligations. What is it about the other AI systems in the absence of specific provisions, for instance as regards the transparency obligations *vis-à-vis* the competent authority or the population or the need to take corrective measures? Second, without doubt, it would have been necessary to add alongside the supplier or developer category of an IA system, that of supplier of an element of the AI system, thus, the suppliers of data or algorithms on which the system operate. Documentation, data quality or non-bias obligations could be imposed on them. The Proposal's Chapter 3 (articles 16 and ff.) assigns the main liability to

is not a luxury but an absolute necessity. By adopting these landmark rules, the EU is taking the lead in developing new global standards that will ensure AI is trustworthy. By setting standards, we can pave the way for ethical technology around the world, while preserving the EU's competitiveness. Time-tested and innovative, our rules will apply when strictly necessary: when the security and fundamental rights of EU citizens are at stake".

[61] All these topics are extensively covered in the report written for the Walloon Region: Y. Poullet, N. Bontridder and L. Gerard, *Intelligence artificielle et autorités publiques wallonnes - L'impact des technologies d'intelligence artificielle sur le gouvernement et l'administration numérique en Wallonie*, Centre de recherches Information, Droit et Société - Research Centre Information, Law and Society, Namur, 2021, 180, report drafted for the *Agence du numérique* (in press).

[62] Undoubtedly, it would have been needed to add categories of actors, like furnishers or developer of AI systems, like furnishers of data. Therefore certain obligations like the quality of the data furnished, the documentation accompanying the delivery, the intervention in case of AI systems' errors, bias or malfunctioning would have to be supported by these actors.

providers[63] and not to users. Article 3 (2) defines 'provider' as such: 'provider' means 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. Under articles 17 and ff.), the providers have to put into place a documented quality management system; to draw up technical documentation in accordance with the requirements of the Annex 4; to operate a conformity assessment; to keep the logs automatically generated except if the user is ensuring that storage under a contractual agreement; take corrective actions; to inform the competent authority and to cooperate with this latter. Users (article 29) "shall use such systems in accordance with the instructions of use accompanying the systems", particularly as regards the human oversight. Additionally they have the obligation to exercise control over the input data, to keep the logs which are under his control and if needed, to carry out a data Protection impact. That distinction applied to public authorities might be difficult. Traditionally, the public authorities made use of public procurement to answer their needs of computerization. As regards the conception and design of AI systems, it must be feared that this delegation will continue and that the algorithms ensuring the functioning of the AI systems will be developed entirely under the control of the private company, which will also often define the conditions of testing and the way to manage and maintain the system. In that frequent situation, we can consider that the public authority would be the provider simply because they have launched the project, defined the objective, will nourish the system with the data they are collecting in the performance of their public missions and that they are using the system under its own name. It is quite clear that the question has to be answered by using a specific regulation defining the respective obligations in different hypothesis following the role of the two partners: the private company and the public authority.

As said, the obligations of actors under the proposals are limited to high-risk systems. The White Paper distinguishes different kinds of AI systems[64]: prohibited AI practices (art. 5), high-risk AI applications (articles 8 and ff.), and other ones. Furthermore, the text imposes certain transparency obligations to certain (high risk or not) AI systems. The aim of these distinctions proposed is to adopt a strictly proportionate regulatory approach[65].

The article 5 enumerates exhaustively the practices belonging to the first category. Most

[63] "Providers of high-risk AI systems shall:
(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;
(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;
(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 set out in Chapter 2 of this Title;
(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 set out in Chapter 2 of this Title."

[64] That distinction initially was proposed by the multi-stakehoders German Data Ethics Kommission created in 2018. This Kommission published in 2019 a major report on AI systems and ethical aspects (see the report available on: https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf.
The Report propose a regulation based on a risk approach according with the potentiality of individual or societal harms: "On this point, the central recommendation of the commission is to apply different regulations to autonomous systems based on a 5-point scale:
1. Systems with low potential harm such as drink dispensers should not be regulated;
2. Systems with some potential harm such as dynamic pricing in e-commerce should be lightly regulated and post-hoc controls should be set up;
3. Systems with regular or obvious potential harm such as personalized pricing should undergo an approval procedure associated to regular controls;
4. Systems with considerable potential harm, such as companies that have quasi-monopolies in credit scoring, should publish the details of their algorithms, including the factors used in the calculations and their weights, the data processed and an explanation of their inner logic. Controls should be possible via a real-time interface;
5. Systems with unwarranted potential harm such as autonomous weapons should be "fully or partially" forbidden.".

[65] As EDBP/EDPS (Joint opinion 5/2021 on the proposal for a Regulation laying down harmonised rules on artificial intelligence, 18 June 2021), welcome this risk-based approach.

of them are concerning public sector activities. Therefore, in particular, the Proposal prohibits "social scoring" when performed "over a certain period of time" or 'by public authorities or on their behalf"[66]. If the authors of the proposal had definitively in mind the Chinese general social scoring system, the absence of definition might lead to envisage the prohibition of others more specific social scorings for instance as regards their accessibility to certain social benefits or assistance to educational programs. Remote biometric identification of individuals in publicly accessible spaces poses a high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in public spaces. For these reasons, the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context. A ban is equally recommended on AI systems categorizing individuals from biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination under Article 21 of the Charter. Furthermore, the EDPB and the EDPS consider that the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited.

In that sense, the distinction between high-risk systems and the other ones is to restrict the new regime of regulation and conformity assessment only to these high-risk applications. According to the White Paper, high-risk AI applications are those used in a sector where "significant risks" can be expected. In complement to a very large list of other systems regulated by other regulation like the 2017 Regulation on medical devices, the Annex III lists (subject to revision) eight types of high-risk systems[67]: biometric identification systems; critical infrastructure management systems; applications in the education and training sector; employment applications; applications for access to or enjoyment of essential public services or private services; systems used by law enforcement; systems used for migration or border control, systems for the administration of justice. From the outset, many public sector applications are classified as high-risk systems. Nevertheless, it would have been interesting to enunciate more clearly the scope of the risks considered. On that point, we consider that not only risks incurred by individuals but also collective risks suffered by groups of persons and even risks to our society (democracy, rule of law[68]) have to be taken into account[69].

[66] Article 5 (1) c) forbids "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 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". As EBBP/EDPS underlines it, private companies, such as social media companies and cloud services providers process huge amount of data and use them for profiling, including for social scoring. The extension of the prohibition to social scoring by private companies ought to be enacted.

[67] The fact that the list is mixing AI applications following different criteria is surprising. Ones are based on the nature of data (e.g. biometric data) and others as regards the sector concerned (credit sector) or as regards the purposes of the processing (e.g ; recruitment of employees, access to public or private essential services). Using such non coherent criteria makes reading and interpreting the text difficult and can be problematic. Thus, a traditional expert system (symbolic AI) that translates the rules of deliberation into algorithms is a high-risk system, while AI systems of farmers based on geomatics for control purposes are not.

[68] On that point, see the excellent article of M. Zalnieriute, L. Burton Crawford and others**,** *From Rule of Law to Statute Drafting: Legal Issues for Algorithms in Government Decision-Making*, in W. Barfield (ed.)*, The Cambridge Handbook of the Law of Algorithms*, Cambridge, Cambridge University Press, 2021, 251-272. Also published in the University of New South Wales Law Research Paper, n. 19-30, available on: https://ssrn.com/abstract=3380072, or http://dx.doi.org/10.2139/ssrn.33800¬72.

[69] In that sense, see extensively, Y. Poullet and B. Frenay, *Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling*, report of the Consultative Committee of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Convention 108, T PD (2019)07 Final, Strasbourg, 2020. Available on https://rm.coe.int/t-pd-2019-7final-en-2757-5764-0706-1-2776-139. More recently, N. Smuha, *Beyond the individual: Governing AI's societal harm*, in *Internet Policy Review*, special issue *Governing European values inside data flow's* (in press), suggests to distinguish three categories of risks according to their very nature. Individual risks: "one or more interests of an individual is wrongfully thwarted", traditionally the only risks envisaged by our legislations (e.g. da-

As previously said (supra, n° 16) of high-risk AI systems are subject to multiple duties (art. 16). The proposal intends to institute, for so-called high-risk systems, a risk management system (art. 9) which involves monitoring of good practices in terms of system evaluation (absence of bias, data quality, etc...). Article 10 mentions various duties related to data governance, as well as the testing and validation of design choices and the data taken into account, examination of possible biases, etc. We add the obligations of documentation (art. 11 and 18), of logging (art. 12 and 20) and, above all, of human oversight (human oversight). The draft mentions the duty of cooperation with the competent national authorities including providing access to all logs. In particular, Article 19 mentions the obligation of a preventive assessment of the system's conformity before any placing on the market. Other obligations may concern other actors: providers of high-risk systems, producers, distributors, importers, users using a high-risk system in the context of their "professional" activities (for example, a public administration using a AI system provided by a private company) and this according to their precise role during the various stages leading from the design to the operation of the AI system. Article 30 obliges member states to create a so-called notification authority, "responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring".

What must be added is that the text subjects certain AI systems to specific transparency obligations (article § 52), as well as the obligation to inform people interacting with an AI system of the presence of a robot as an interlocutor (e.g., the chatbots used by more and more administrations), of the use of systems for recognizing emotions (notably as regards the selection of civil agents or when questioning by law enforcement of people suspected of an offence) or profiling based on biometric data (e.g. in case of investigations by law enforcement authorities) or for manipulating images, sounds or videos relating to people (for instance, deepfakes). It is quite clear that these obligations might be added to the obligations related to high-risk systems.

According to the principle of accountability. It is for the controller(s) to show that they have complied with the obligations stemming from the use of AI systems, having due regard to risks associated with these operations. The quality of the data will need to be checked, therefore, to ensure not only that it is accurate and up to date, but also that there is no bias in the way it is used in a given application. The same caution extends to the algorithm(s) used, whether developed by the controller themselves or elsewhere. The next step will be to document the various operations involved in processing and keep logs of the decisions made. Clearly, all these obligations could be the subject of certification by the AI systems supervisory body mentioned above or by other bodies accredited by it.

This obligation, on the part of the data controller does not mean that the other players operating on a commercial basis and offering one or more components (datasets, algorithms) are absolved of their responsibilities. Accordingly, depending on the "foreseeable" risks associated with their operation, the algorithm provider will document the product they are marketing, describing the applications for which it is designed or, on the contrary, those for which it must not or should not be used, and the fact

ta protection Act does protect only individual harms). Collective risks: "one or more interests of a collective or group of individuals l is wrongfully thwarted" (e.g. Profiling concerns group of individuals as such and not only each individual of the group. In that sense, the concept of Group's Privacy developed by B. van der Sloot). Societal risks: "a range of societal interest is wrongfully thwarted" (e.g. Cambridge Analytica or disinformation as a way to put into question the functioning of our democratic institutions – see also the threats linked with the functioning of certain AI systems which deeply jeopardised as the equilibrium between powers. On this need to extend the risks to be taken into account in the evaluation of the AI systems' impacts: "Moreover, the societal dimension of AI's risks that surpasses the impact on individuals, such as the impact on the electoral process and the democratic institutions or the legal system, is not yet sufficiently considered. While a number of national and international mechanisms allow individuals to seek redress before a court when a human right is breached in the context of AI, this mechanism is currently underdeveloped as regards an interference with democracy or the rule of law, which concern broader societal issues. Their protection necessitates public oversight over the responsible design, development and use of AI systems whenever such risks exist, by setting out clear obligations or requirements to this end" (Ad Hoc Committee on Artificial Intelligence (CAHAI) of The Council of Europe*, Feasibility Study on a legal framework for the creation, development and application of AI based on Council of Europe standards*, Strasbourg, 2020.

that it has already been applied or tested, and will collaborate during the test period, etc. These subcontractors will have the obligation to cooperate with the administrations in case of malfunctioning of the systems. The public procurement launched by public agencies must contain different provisions ensuring the respect of the multiple provisions envisaged by the proposed regulation.

Let us conclude Chapter 3. All these obligations will lead to a profound transformation in the procedure followed by the public sector and oblige our administrations to set up new functions and offices. As regards the obligation to proceed to a conformity assessment, the setting up of independent and multidisciplinary bodies will be required. The Proposal gives an important place to the notion of human oversight (Article 14). The obligation to ensure this human oversight and the fact that high-risk AI systems have major impact on individuals, groups of individuals and even for society, impose real human centrality and should leverage on highly qualified human oversight. A public AI assessment body[70] or rather several AI assessment bodies will have to supervise their conception, development and deployment and monitor their functioning. These bodies will have to produce reports about their activities.

As far as such systems are based on the processing of personal data or process personal data to fulfil their task, the obligation of human oversight also requires a lawful processing implying a human intervention. The administration will stipulate the organisational procedures necessary to ensure that the right to have a human, competent and responsible, involved in the final decision is respected and that data subjects are genuinely able to express their views and, should they do so, to have them taken on board[71].

We pinpoint two other points: the first one definitively is, as confirmed by numerous authors, to impose the publication of the algorithms used by the public authorities following the obligation of transparency and motivation of the public decisions[72]. The second one requires, as the White Paper has already stated[73], the public participation: "The governance structure should guarantee maximum stakeholders participation. Stakeholders – consumer organisation and social partners, businesses, researchers, and civil society organisations – should be consulted on the implementation and the further development of the framework". Since AI systems might have a deep impact on the balance of powers between a more and more digitalized state and the citizen, a public debate notwithstanding the complexity of the topics is needed. The creation of Data Ethics Commissions in different countries aims to facilitate the understanding of that complexity and overall to clarify the different options

[70] See in UK, the recent setting up of the *Data Ethics and innovation Authority* (www.statisticsauthority.gov.uk/about-the-authority/committees/nsdec/data-ethics). This Authority created within the Ministry for Statistics precisely has as aim to assist the other administrations to evaluate the AI systems of the numerous UK administrations: "The UK Statistics Authority aims to mobilise the power of data to meet the greater demand from policy makers and users for more timely, frequent, accurate and relevant statistics for the public good to help Britain make better decisions. This involves making better use of pre-existing administrative, real time and big data using innovative methods, to produce more frequent, timely and accurate statistics for the public good accounting for a wide variety of user needs. To ensure that this work is completed to the highest ethical standards the UK Statistics Authority has established a robust ethical governance structure to provide transparent and timely ethical advice to the National Statistician that the access, use and sharing of public data for research and statistical purposes is ethical and for the public good".

[71] This requirement develops the already existing requests laid down by GDPR article 22, in order to ensure that the right not to be subject to a decision based solely on automated processing is respected. On that issue, about AI systems used for profiling see the drafted Recommendation on Profiling (article 9.9): "The individual decisions or draft decisions taken by public authorities and based on automated decision-making should be transparent. Individuals and legitimate associations should, notwithstanding any technical or legal arguments, have access to the reasoning of the processing or, in the case of the use of processing based on machine learning, an explanation in plain language of the decision taken by the model on which the system is based. Otherwise, effective legal protection against the decisions would not be guaranteed". See for the explanation of that drafted provision, Y. Poullet and B. Frenay, *Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling*, Strasbourg, Council of Europe, 2019, report of The Consultative Committee of The Convention for The Protection of Individuals with regard to Automatic Processing of Personal Data Convention 108, T PD (2019)07 Final. Available on https://rm.coe.int/t-pd-2019-7final-en-2757-5764-0706-1-2776-139.

[72] See notably, the excellent report *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems*, in *AI Now Institute,* 2018, available on https://ainowinstitute.org/litigatingalgorithms.pdf. See also, the UK report of the Select Committee on Communications, *Regulating in a digital world,* 2nd Report of Session 2017-19, House of Lords, 2019.

[73] See White Paper, 24.

available and the respective challenges. It is obvious that the respect of these obligations of transparency, motivation and public participation will increase the citizens' trust and contribute to a living democracy[74].

5. *Conclusions*

"Government is potentially the major 'client' and also 'public champion' for these new data technologies", asserted ENGIN and TRELEAVEN in a very convincing article[75]. We definitively agree. It is effectively quite clear that public sector reveals many opportunities of using AI for the "public good" at the service of citizens, socio-economic sectors and democracy. Therefore, we understand the major role assigned by the EU Commission to the public sector for achieving its "third way"? Notwithstanding that conviction, we would like to underline that the possibility of making this wish come true requires a profound modification of the traditional conception of the public sector. As demonstrated in the first chapter, more openness is expected from it. This "Open Data" policy needs to conceive the public sector as a vast platform able to offer new information services at the benefit of citizens and companies. That implies the abandonment of a philosophy and a culture of administrations isolated and operating in silos but on the contrary working together through networks. We add that it would be interesting to create at the administrations level even in the public sector (broadly defined) level, a governance in charge not only of defining standardization and metadata but also of implementing the requirements of the Open data legislations and the Privacy ones. The openness of our public sector also means a proactive attitude *vis-à-vis* the private sector. As shown, the Open Data directive and the future Data Governance Act are pleading for an extended cooperation between two sectors in a bilateral sense. Public sector must be aware of the informational needs but also about the informational resources of the private sector by setting-up interfaces, able not only to identify reciprocal needs but also to solve delicate problems notably of privacy and intellectual property protection.

Beyond that, we underline our fear of facing a tendency to disempower decision-makers and to delegate decision-making power to AI, which some qualify to reject as "technological solutionism". Upstream, it is also important to keep in mind that the programming of AI systems is done by human agents who therefore make choices, and that, moreover, as noted by Paula Boddington, philosopher and researcher at Oxford University, "it is always a human being who has decided to use AI to make decisions"[76]. Beyond that, the proportionality principle must be recalled. As expressed by the draft text of the UNESCO recommendations on the Ethics of Artificial Intelligence (Point 26), "It should be recognized that AI technologies do not necessarily, per se, ensure human and environmental and ecosystem flourishing. Furthermore, none of the processes related to the AI system life cycle shall exceed what is necessary to achieve legitimate aims or objectives and should be appropriate in the context. The choice to use AI systems and which AI method to use should be justified in

[74] See in that sense, the recent Belgian draft bill proposed to the Belgian Parliament: "La proposition de loi vise à modifier l'article 2 de la loi sur la publicité de l'administration, de manière 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)" (Proposal for a law amending the law on the publicity of the administration in order to introduce greater transparency in the use of algorithms by the administrations, 2021, DOC 55 1904/001).

[75] British Computer Society, *Algorithmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies*, in *The Computer Journal*, 2018, vol. 62, issue 3, 448, doi:10.1093/comjnl/bxy082.

[76] P. Boddington, *Does AI make better decisions than humans? Thinking Ethics of AI*, Unesco, 2020, available on: www.youtube.com/watch?v=2E7l1hdjHsg. See, on this matter, Point 36 of the draft text of the *UNESCO recommendations on the Ethics of Artificial Intelligence* (SHS/IGM AIETHICS/2021/JUN/3 Rev. 2nd Session of the Intergovernmental Meeting, 25 June 2021. The Draft likely will be approved at the next UNESCO General Assembly): "It may be the case that sometimes humans would choose to rely on AI systems for reasons of efficacy, but the decision to cede control in limited contexts remains that of humans, as humans can resort to AI systems in decision-making and acting, but an AI system can never replace ultimate human responsibility and accountability". This point translates the famous principle of "human oversight" developed *supra*.

the following ways. The AI method chosen should be appropriate and proportional to achieve a given legitimate aim…" Transparency of the decisions when setting up AI systems applications is fundamental. Multidisciplinary and multistakeholder evaluation and public participation are other prerequisites in order to gain the confidence of citizens. "Excellence and trust" are at this price as well understood by the EU Commission.

Definitively, we must build up Public AI applications for the public good. The assertion is easy, its achievement is far more complicated