Public data, AI Applications and the Transformation of the State: Contemporary Challenges to Democracy

Abstract

The use of AI applications and their abilities might have an unparallel transformative force on the state and the administration's relationship with citizens. Their application has the potential to usher in a new paradigm where alternative ways to perform administrative tasks may emerge.

The deployment of such technology in the private and the public sector signals that the time has come for their regulation. The current EU legal framework and proposed legislation for regulating AI is limited in critical ways, as demonstrated by the analysis of the AI Act and positive law in the Part A.

This article argues that AI applications employed by the public sector should be subject to a separate risk category for two reasons: first because specific safeguards are necessary in relation to the AI applications in the public sector in order to enhance the legitimacy and accountability of such applications, and second because AI applications in the public sector with access to the lake of data of the state create an unprecedented public resource, which must be safeguarded from malicious incumbents who would be keen to take advantage of such resource for self-entrenchment purposes.

Key Words

AI, AI ACT proposal, democracy, self-entrenchment, legitimacy, accountability

Introduction

Humanity always moves forward. From the agricultural revolution, we have progressed to the industrial revolution and nowadays another revolution is looming, the so-called information revolution. Such revolution is becoming tangible, based on the growing computational power and the rise of AI in combination with network connectivity. In practice, the benefits from such development were given the opportunity to be tested with the Covid-19 pandemic. As the measure of social distancing was implemented across the world, the public and the private sector were required to adapt to a new reality; services and the relationship between citizen and the administration moved online.

It is believed that AI and algorithms[1] (alternatively fully autonomous systems[2] or AI applications) can transform and revolutionize every aspect of daily life, e.g. work, mobility, communication, and the economy. The dominance of companies such as Google and Meta indicate that business models based on computational power, algorithms, and the collection and processing of personal data can thrive in the market economy. The promise is that

* Dr. Antonios Kouroutakis, Associate Professor, IE University, akouroutakis@faculty.ie.edu.

I would like to thank the participants of the 13th Constitutional Law Colloquium in Loyola School of Law for their useful comments. I would also like to thank my research assistant, Mr Miles Deichler for his support. Research Reported in this paper was partially funded by Agencia Estatal de Investigación (AEI) -10.13039/501100011033 Grant No. PID2020-115834RA-C33.

[1] Algorithms are a set of instruction rules based on mathematical formulas. Such formulas have a different level of sophistication depending on their use. According to the current level of technology, algorithms are a necessary component to operationalize AI. For more details about algorithms, see Buiten, 2019, pp 41 - 49.

[2] Autonomous systems and AI systems are not coterminous since only fully autonomous systems are operated by AI, without the control of the assistance of the human operator.

harvesting, and processing data would allow such companies to see the underline trends in the market and to dominate the supply side.

According to some more futurist scenarios, the collection of big data and behavioural and predictive analytics may allow planned economies to see the invisible hand of the market and make the allocation of resources; this would enable an unprecedented, accurate coordination of supply and demand.[3]

In like manner within the sphere of the administration, 'Artificial intelligence (AI) promises to transform how government agencies do their work. Rapid developments in AI have the potential to reduce the cost of core governance functions, improve the quality of decisions, and unleash the power of administrative data, thereby making government performance more efficient and effective.'[4] Specifically within public administration, the promise is that if AI and algorithms undertake any data-driven decision making, the outcome will be more accurate and fairer, while the procedure will be more efficient and possibly more transparent.[5] While, as it is accurately pointed out, the adoption of AI in governance has been notably slower when compared to the private sector[6], AI applications in the public sector have the potential to thrive. As AI's success depends on the amounts of data (in terms of quality and quantity) and on big data-supporting technologies to advance decision-making capabilities,[7] the state is the ideal environment. The state is an unparallel lake of data with information about the citizens on every aspect, like work status, income status, healthcare, and even religious beliefs. Such a quantity of data is the fuel for AI applications and their potential is maximized.

To exemplify how AI applications in the public sector might offer better solutions, the case of traffic lights is indicative. Traffic lights are an indispensable feature for city functionality. Such traffic lights are usually timed based on a statistical formula. This inevitably means that each direction is allocated a timed period of 'green' or 'red' time, regardless of the traffic congestion. With the use of an AI systems based on deep reinforcement learning, such systems read live camera footage and coordinate the lights to improve traffic.[8]

However, the application of such technology by the administration does not come without its risks or downsides. The early application of algorithms by governments in Europe and the US has brought challenges before Courts. In the US, the Wisconsin Supreme Court in the well cited COMPAS case held in its obiter dictum that automated systems calculating risk scores of

[3] The idea that computational power might be a very useful tool in planned economies appears with the Project Cybersyn in Chile. For more details on the program, see Medina, 2006, pp 571 – 601.
[4] Engstrom et al 2020
[5] Al-Mushayt argues that AI applications such as chatbots have the potential to improve the citizen government communication; see Al-Mushayt 2014. Ben Rijab and Mellouli (2018) analyse the potential of AI applications to the development of smart cities; see Mellouli and Rjab 2018. Bullock argues that AI applications will assist the administration in the exercise of its discretionary powers; see Bullock 2019. Gomes de Sousa et al examine the potential benefits generated for the administration based on the area of competence of each agency; see De Souza Bermejo et al 2019. In addition, it is argued that AI applications might enhance the democratic legitimacy of governments by producing better results; see Cavaliere and Graziella 2022, pp 571 – 601
[6] Chenok et al 2020, p 205. This possibly explains the 'paucity' of research in relation to AI applications employed by the public sector. For an account of literature in relation to AI in the public sector see Chen et al 2021.
[7] Is it an axiom in computer science and in mathematics that the quality of output is determined by the quality of the input.
[8] Chli et al 2022.

recidivisms may not be used by judges as the determinative factor.[9] In Idaho, the federal Ninth Circuit Court of Appeals in the K.W. v. Armstrong ruled that an automation system deciding on the individual budgets of participants (applicants) in Idaho's Developmental Disabilities Waiver program without adequate notice was a violation of the due process.[10] In the Netherlands, SyRI was an algorithm employed by the government to identify various forms of fraud, in relation to social benefits, allowances, and taxes; the District Court of The Hague ruled that such application was violating the right to privacy.[11]

If the use of algorithms is problematic when humans design them and feed the algorithm with data, the concerns multiply when AI perform these functions.[12] In other words, if algorithms are considered as a black box,[13] the mystery and the opacity intensify when AI designs and operates such black box.[14] On the top of that, the use of AI applications (which are characterized as black box) in the public sector (which bureaucracy is also characterized as a black box[15]) can be seen as a black box within a black box, creating a prima facie alarming combination.

AI applications in combination with digitalization and the internet of things have already shown an unparalleled potential in massive surveillance and the control of information. Around the world, such applications have been used by repressive regimes to control in absolute terms the life of citizens.[16] Dissenters and people who wish regime change would have nowhere to hide.

In liberal democracies, criticism is voiced about the negative impact of AI and algorithms from multiple fronts, such as privacy concerns, discrimination, etc.[17] Based on these concerns, the White House has published examples of AI automated systems already applied and their potential correlation to human rights;[18] examples include content moderation on social media platforms, automation systems in detecting tax frauds, and voters' signature validation.

---

[9] Supreme Court of Wisconsin, State v. Loomis, judgement of 13 July 2016, 2015AP157–CR. For criticism on that decision see, Freeman 2016, p 75

[10] See United States Court of Appeals for the 9th Circuit, K.W. v. Armstrong, judgement of 5 June 2015, 14-35296. In like manner, the Federal Court in Texas ruled that a program (EVAAS System) to evaluate teachers' performance was a violation of procedural due process as the teachers were denied access to the algorithm and the data. See United States District Court, S.D. Texas, Houston Division, Hous. Fed'n of Teachers v. Hous. Indep. Sch. Dist., judgement of 4 May 2017, CIVIL ACTION H-14-1189.

[11] District Court of First Instance of The Hague, C/09/550982 / HA ZA 18-388, judgement of 5 February 2020, C/09/550982.

[12] Alexopoulos et al have examined the benefits and the obstacles of machine learning in the public law sector. See Alexopoulos et al 2019, p 354. Chen et al analyse the risks using AI applications from governments. See Chen et al 2019, p 122

[13] For more analysis on the issue of opacity of algorithms see O'Neil 2016, pp 28 – 31, Barocas 2018, p 1085, and Pasquale 2015.

[14] Interestingly, DeepMind has already developed an AI application AlhpaTensor that can create its own algorithms. See Huston M (2022) DeepMind AI invents faster algorithms to solve tough maths puzzles. Nature https://www.nature.com/articles/d41586-022-03166-w Accessed on 29 November 2022

[15] Kegan wrote in 2002 'Bureaucracy is the ultimate black box of government - the place where exercises of coercive power are most unfathomable and thus most threatening.' See Kegan 2000-2001, p 2246

[16] For more analysis and for examples of AI applications already used in repressive regimes around the world, see Feldstein 2019, p 40.

[17] See for instance, Kitchin 2014; O'Neil 2016; Citron 2014, p 1.

[18] Office of Science and Technology Policy, Blueprint for an AI Bill of Rights; Examples of Automated Systems available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/examples-of-automated-systems/

The deployment of AI applications indicate that the time has come for their regulation.[19] A handful of draft laws regulating AI have been proposed, and some laws regulating different aspects of AI have been passed. Suffice to mention here the AI ACT,[20] which is a draft bill in EU, two Executive Orders 13859 and 13960[21], the National Defence Authorization Acts[22], and the AI training Act[23] in the US. In the US, further regulation is expected as a Bill of Rights for an Automated Society is in the early stages of drafting by the White House.[24]

In this article, I first analyze the proposed bill to regulate AI in the EU in order to examine how policy makers address AI applications used in the public sector. The examination of those laws reveal that lawmakers are concerned with the deployment of such technology and its impact on human rights, rule of law, and democracy.[25]

Despite this, the aforementioned law does not classify AI applications used in the public sector as a distinct category of risk with a separate set of conditions and safeguards. That said, I argue that a separate risk category in relation to the AI applications used by the public sector[26] could

[19] In general, the use of automation procedures (including algorithms) is regulated by a number of laws. For instance, the GDPR and the CCPA regulate the use of personal data by automation systems. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016 and California Consumer Protection Act of 2018 section 1798.100. Recently in EU the Digital Service Act was enacted and provisions regulated the use of algorithms for instance for content moderation. see Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1 OJ L 277, 27.10.2022 Art 14. In addition, the Digital Market Act imposes obligations to gatekeepers in the market who use algorithms to see provide information to the Commission upon its request. See Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1 OJ L 265, 12.10.2022, Art 21.

[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021.

[21] See Executive Order 13859, Maintaining American Leadership in Artificial Intelligence, February 11, 2019 and Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, December 3, 2020.

[22] See for instance, The National Defense Authorization Act for Fiscal Year 2022 S. 1605; NDAA 2022, Pub.L. No 117-81; John S. McCain National Defense Authorization Act for Fiscal Year 2019, Section 238(g), Pub. L. No. 115- 232, 132 Stat. 1636, 1695 (codified at 10 U.S.C. § 2358).

[23] Artificial Intelligence Training for the Acquisition Workforce Act or the AI Training Act, Pub L. No 117-207.

[24] See Join the Effort to Create a Bill of Rights for an Automated Society available at https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/

[25] See the reports On Artificial Intelligence – A European Approach to Excellence and Trust, COM(2020) 65 final; Communication on Building Trust in Human-Centric AI, COM(2019) 168.

[26] However, even in the public sector some areas shall be subject to different level of scrutiny, namely, AI application in the defence sector. National security concerns permit to the defence sector to remain secretive and evade transparency and accountability. For more analysis on AI application in relation to defence and national security, see Greg Allen and Taniel Chan, *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, July 2017, Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies*, Center for Naval Analysis, January 2017; Kelley Sayler. Artificial Intelligence and National Security: November 10, 2020 Washington, DC. Interestingly, the close examination of the laws in the US and EU shows that policy makers have already drawn a distinction between AI applications in the military sector. For instance, the AI Act draft of the EU states that 'This Regulation shall not apply to AI systems developed or used exclusively for military purposes.' See European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 2 para 3.

possibly have been more efficient for two reasons: firstly, because specific safeguards are necessary in relation to the AI applications in the public sector in order to enhance the legitimacy[27] and accountability[28] of such applications, and secondly, because public sector AI applications with access to the state's lake of data create an unprecedented public resource which must be safeguarded from malicious incumbents who would be keen to take advantage of such a resource for self-entrenchment purposes.[29]

To justify this argument, I explore the impact of AI applications from the administration on democracy and the democratic process. I approach this issue from two essential features of democracy: legitimacy and accountability of public authorities. I explore how the opacity and complexity of AI applications in administrative procedures breaks the invisible threads of legitimacy, which are necessary in every democratic system, and how AI applications distort the chain of accountability.

In doing so, I highlight the differences between private and public sector AI applications, focusing on their structural difference. Unlike private sector AI applications, which are subject to the forces of the market economy, AI applications in the public sector fit within the monopoly of administrative power to exercise coercion. I then argue that in public sector an AI applications' legitimacy resembles the legitimacy of technocrats, and for people to accept the outcomes from such applications, their deployment should be subject to certain preparatory acts with a regulatory impact analysis, risk assessment analysis and public consultation. Within this framework, citizens would be able to understand the use of AI in the public sector, trust it, and legitimize it.

In relation to the accountability of AI applications in the public sector, I argue that their deployment should be subject to the external scrutiny from courts. And the justiciability of AI

[27] For the purpose of the paper democratic legitimacy is defined as the faith of the people in the exercise of public authority by state officials. Weber prescribes that faith to the political authorities can be based on three sources: charisma of the leaders, tradition and rule of law. See Weber (1964), pp 124-128 and 382. Rawls on the issue of legitimacy stresses that the exercise of coercive political authority is 'fully proper' when it is exercised according to the constitution ('a constitution the essential of which all citizens as free and equal may reasonably be expected to endorse in the light of principles and ideals acceptable to their common human reason'). See Rawls (1996), p 137. For Buchanan, legitimacy is justified only if a minimum standard of justice exist, and therefore legitimacy is subject to three conditions: when political power does a credible goal to protect most basic human rights, provides procedural and substantive protections and does not depose a 'legitimate wielder of political power'. See Buchanan 2002, p 703. Scharpf argued that democratic legitimacy is based on the will of the people who decide who governs them (input) and on the results of that government for the people (output). See Scharpf 1998. See also, Scharpf 1999, pp 11–12. Finally Tyler focuses on the importance of rule of law as a source of legitimacy see Tyler 1990, pp 96, 137–38.

[28] Accountability might mean different things, such as the professional and personal accountability of public servants, accountaibility as a feature of checks and balances, accountability as responsiveness to the wishes of the citizens and finally accountability as the dialogue between citizens and democratic institutions. See Mulgan, 2000, p 556. For the purpose of this paper accountability means 'the obligation to be called 'to account', is a method of keeping the public informed and the powerful in check. It implies a world which is at once complex, where experts are needed to perform specialized tasks, but still fundamental democratic in aspiration in that members of the public assert their right to question the experts and the exercise ultimate control over them. See Mulgan, 2003, p 1.

[29] We define political self-entrenchment, as the use of legitimate or illegitimate tools by which political actors insulate themselves from political change. Political self- entrenchment is a subsection of political entrenchment. For more details on political self- entrenchment see Klarman 1997; Pildes 2004; Levinson, Sachs 2015; Kouroutakis 2021.

applications should not be barred based on the non-regulatory nature of the administrative process in civil law systems,[30] or the ripeness doctrine in common law systems.[31]

Finally, in the last part, I discuss the risks of public sectors' AI applications in relation to the democratic process. I argue that these application's access to the amount of state-controlled data creates a new category of public resource. Given that it has not been uncommon for political actors in power (ruling political parties and incumbents) to take advantage of public resources for self-entrenchment purposes throughout history, all AI applications in the public sector should be considered as high-risk subjects to enhanced levels of transparency[32] and explainability.[33]

In such manner, the democratic process would be better protected even from AI Systems deployed in various low risk areas but with the potential to gain insights into populations giving a comparative advantage to the incumbent or the ruling political party. Two reasons support this argument: firstly, the information asymmetry[34] between the designer of AI applications with the third parties in relation to the utility and outcomes of such applications, and secondly, the lack of a sanctions framework against the state for AI applications used in the public sector.

A. The regulatory framework: Building public trust with the AI Act

a. The EU regulatory approach on AI: a thematic approach based on risk assessment

As Artificial Intelligence has been increasingly deployed across various industries, reports from national and international institutions have been published urging the need for the regulation of AI, examples of such reports include a 2016 report from the White House,[35] a report from the House of Lords[36] in the UK and a report from the EU Parliament.[37]

To begin with the EU, AI-related regulations can be found in the General Data Protection Regulation (GDPR). Specifically, Article 22 regulates automated individual decision making without the intervention of a human and profiling based on such automated process and prescribes that individual's explicit consent is required unless such processes are necessary for the performance or entry into a contract, or unless such automated individual decision making without the intervention of a human and profiling is authorised by law.[38]

[30] About the non-regulatory acts in Germany, see Singh 1985, p 57.
[31] About the ripeness doctrine in the US, see Reno v. Catholic Soc. Servs., Inc., 509 U.S. 43, 57 n.18 (1993).
[32] About the level of transparency in relation to AI applications see Brauneis, Goodman 2018, p 118.
[33] About the problem of explainability of AI applications see Maclure 2021, p 421.
[34] Information asymmetry for the purpose of this papers is defined as the greater material knowledge possessed by the designer of the AI application than third parties.
[35] National Science and Technology Council Networking and Information Technology. Networking and Information Technology Research and Development Subcommittee, The national artificial intelligence research and development strategic plan (2016)
[36] UK House of Lords Artificial Intelligence Committee, AI in the UK: ready, willing and able? (HL Paper 100 2018)
[37] European Parliament Committee on Legal Affairs, Civil law rules on robotics (2015/2103 (INL))
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, Article 22.

As the GDPR applies equally to private and public entities, Article 22's requirement for explicit consent also regulates AI applications employed by the public sector.[39] However, when law enforcement authorities utilize automated systems, a separate regulatory framework outlined in Directive 2016/680 applies [40] Article 11 of the Directive, entitled 'Automated individual decision-making', prohibits the profiling and any decision with adverse legal effect on data subjects by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties 'unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller'[41]

In addition, Article 25 of the Directive creates an obligation for the competent authorities that use automated systems to create and save logs for such automated procedures which shall be sufficient to 'establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.'[42]

Finally, Article 29 of the Directive requires a set of additional security configurations to ensure that unauthorized persons do not have access or the power to use automation systems, and that authorized persons can verify which personal data have been input in such automated systems.[43]

A more comprehensive law to regulate AI, the AI Act, has been proposed by the European Commission. Article 3 of this proposed AI Act defines an 'artificial intelligence system' (AI system) as 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

[39] In relation to public authorities as controllers or processors of personal data see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, Article 4.

[40] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89 Articles 1 and 2.

[41] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89 Article 11.

[42] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89, Article 25.

[43] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89 Article 29.

with.'[44] In Annex I, the draft regulation includes, for instance, techniques such as supervised or unsupervised machine learning, reinforcement learning, deep learning, inference and deductive engines etc.[45]

The primary objective of the AI Act is to mitigate potential risks of AI systems. The proposed bill lists a series of AI applications that should be forbidden such as social scoring by governments, the exploitation of vulnerabilities of children, the use of subliminal techniques, and live remote biometric identification systems in publicly accessible spaces used for law enforcement purposes (subject to specific exceptions).[46]

In addition, the AI Act introduces a second category of AI systems, which are framed as 'high risk', and the AI act sets a series of procedurals requirements for these high-risk systems.[47] For instance, AI application in critical infrastructures such as in transports, education, employment, law enforcement, administration of justice and democratic procedures[48] would be subject to strict conditions. Accordingly, the provider would be expected to guarantee that AI applications in the aforementioned fields are subject to 'adequate risk assessment and mitigation systems, high quality of the datasets feeding the system to minimise risks and discriminatory outcomes, and logging of activity to ensure traceability of results.'[49]

Interestingly, the AI Act specifically mentions that 'This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a provider or user of an AI system.'[50] Moreover, Article 56 of the AI Act establishes the European Artificial Intelligence Board, a new regulatory authority with the competence to issue opinions and guidance on the implementation of the Act.

[44] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 3.

[45] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021 [Annex I]. Interestingly, the AI Act proposal in article 4 delegates the power to the EU Commission to update the techniques of AI applications in the definition in order to cover new techniques not currently listed. See European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 4.

[46] See European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, [Title II].

[47] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, [Title III].

[48] For a complete list of high-risk areas, see European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, [Annex III].

[49] See European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Articles 10 – 15.

[50] See European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021 [Preamble 12].

b. A critical review and the regulatory approach between AI applications in the public and private sector

Upon analyzing the architecture of the law, the EU's approach intends to enact a more comprehensive legislation. The EU approach is more hands on, with more specific content, focused on risk that some AI applications may pose. Accordingly, some AI applications are explicitly prohibited, and others are subject to specific conditions. Moreover, hefty fines are imposed in case there is a failure to comply with the AI ACT.

Without doubt, the framework in the EU is inspired by significant legal principles and concerns, first and foremost being the compatibility of AI application with the human rights; it is apparent that privacy, equality, and non-discrimination are of imperative concern. In addition, the need to deploy AI applications within the framework of constitutional guarantees, such as transparency and due process, is also clear.

A critical issue on the regulation of AI is its definition.[51] AI applications vary in terms of autonomy and in terms of their way of deployment. Most importantly, the technology around AI is evolving at such a rapid pace, making the task of lawmakers difficult to offer precision and legal certainty in their definitions. Interestingly, the definitions present in the AI Act reference precise applications of AI, which makes the definitions concrete. In addition, the definition focuses on the version of the AI which is currently deployed, the so-called weak version, without any reference to cognitive abilities.[52]

Most importantly, the door is left open for constant update of the term AI. In the AI Act, the Commission is entrusted with the power to update Annex I which includes the list of AI techniques and approaches.[53]

In the EU, despite the fact that an omnibus bill is proposed to regulate AI, several provisions of the AI Act create diverging obligations for AI applications employed by the public sector and private sector. For instance, social scoring is explicitly prohibited by public authorities,[54] in addition to real time biometric facial recognition by law enforcement authorities[55], all the while public actors can utilize biometric categorisation systems (BCS) and emotion recognition systems (ERS) without having to comply with transparency requirements.[56] In essence, the AI Act's all-encompassing nature complicates the distinction between public and private sector AI application regulation. As it currently stands, frameworks set out in the AI Act for public and private sectors AI application classifications overlap.

---

[51] About the definition of AI see Buiten 2019, pp 43-47.

[52] Alternatively, weak AI is termed as narrow Ai and is opposed to General AI or strong AI.

[53] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 4.

[54] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 5 para 1 (c)

[55] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 5 para 1 (d)

[56] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 52 para 2

It is because of this overlap that AI applications employed by the public sector must be subject to an altogether different legal framework, one that specifies such AI utilization as a special category of high risk. The following part will analyse why this would be necessary for democracy and the democratic process.

B. AI in government; justifications for a specific legal framework

a. AI applications in the public sector and their impact on democratic values

The administrative state is a complex organism, delivering a multitude of goods and performing a vast array of services each day. To better understand the implementation of AI applications within the administration, it is necessary to systematize the diversity and specificity of the administrative activity within the legal framework and in practice.

To begin with, an administration may act with its state capacity or as a private entity.[57] Within its state capacity, administrative actions might be contractual or unilateral.[58] The administrative unilateral actions might be among other 'regulations', 'decisions', 'orders', 'warrants', 'bylaws' 'approvals', 'bans', 'permits', 'certificates', 'recommendations', 'announcements', 'warnings', 'plans', 'summons' etc. In civil law jurisprudence, administrative unilateral acts are also distinguished from a legal point of view either as regulatory or non-regulatory.[59] Such distinction is significant as only regulatory acts are subject to judicial review, while non regulatory acts might be challenged via the state liability procedures. In Common law countries, although all administrative acts are considered to have regulatory force, the ripeness doctrine of justiciability has a similar effect as courts are prevented from the adjudication of premature or not fully formalized administrative decisions.[60]

In general, the administration may use AI applications to enhance or replace existing actions. For instance, such applications might be used for planning purposes such as budgeting, or even for strategic planning to predict wildfires, extreme weather conditions, or for the protection of wildlife.[61] In addition, AI might be of good use in relation to more material actions, as it was mentioned above with the control of the traffic lights. AI applications have found application in regulatory actions as well, such as child welfare assessments, predictive policing[62], and

[57] In civil law jurisprudence, the state acts as a private entity in its commercial and fiscal activities. For more details see Singh (1985), p 56. At the same time, with the waves of privatization and the outsourcing, even private entities, it is possible to exercise public law authority. Accordingly, the distinction between private and state actions is not always very clear. In relation to the US, the distinction between public and private actors is commonly known as the 'state action doctrine'. For more details see Brown 2008; Strickland 1991, p 591; Black, 1967, p 95.

[58] About the administrative contracts and the different approach between common law countries like UK and India, and civil law countries like Germany, see Singh 1985, p 50. See also about the UK, Craig 2010, p 173, and for France, see Bell, Lichere 2022, p 270.

[59] A prime example of non-regulatory acts is the German theory of administrative real acts. Such acts are also unilateral but their aim is the production of factual results, and they don't have legal consequences. For instance, an administrative real act is the cleaning of the streets, reporting, and the maintenance of the transpiration system. Such acts might be explanatory of administrative acts or they might materialize existing administrative acts and regulations. see Singh 1985.

[60] See Reno v. Catholic Soc. Servs., Inc., 509 U.S. 43, 57 n.18 (1993).

[61] Smith A et al 2012, p 1.

[62] Brauneis, Goodman 2018, pp 103- 105.

public-school teachers' evaluations.[63] All in all, AI applications in the public sector are found both in the procedures and the actual decisions of the administration.

Due to the inherent opacity and complexity of AI applications, the most immediate effect of such applications in the public sector is the de-legitimisation of the administration's decision-making process and the fracturing of the chain of accountability.

Prima facie, the legitimacy of AI in the public sector may resemble the legitimacy of technocrats in government. The source of legitimacy for technocrats is not, for instance, their charisma as leaders, or the tradition. On the contrary, the source of legitimacy for technocrats is based on 'reason' because they administer things better without representation of political interests or their influence. [64]

In like manner, it can be argued that the source of legitimacy for AI applications in the public sector is 'reason'. However, for people to understand the benefits from AI applications in the public sector, their deployment should be subject to certain preparatory acts with a regulatory impact analysis, risk assessment analysis, and public consultation. The regulatory impact analysis must a) address that AI applications are employed to solve a fundamental problem, b) demonstrate that the solution offered by such applications is the optimum, c) ensure that the deployment of AI solutions is coupled with explanatory notes that justify why such solution is the optimum, and d) must provide a risk assessment analysis. Then, public consultation would be of paramount importance for people to increase transparency and public engagement. Within this framework, citizens can understand the use of AI in the public sector, trust its deployment, and legitimize its usage.

Furthermore, such regulatory impact and risk assessment analyses enhance the role of the courts to review AI application legality; that way, accountability will be also established between citizens and holders of public offices who decide and employ AI applications.[65] Unlike AI applications in the private sector, which are subject to competition and the forces of the market economy, AI applications in the public sector are more challenging because the administration exercises a monopolistic authority.

The administration and its agencies have the monopoly of power to exercise state authority. Such exercise of power shapes public law relationships between citizens and the administration and is subject to strong accountability mechanisms. The failure of public law AI applications falls within the objective responsibility of the executive to administer public matters. Citizens do not have alternative options, as is the case with private AI applications in the market economy, and the only way to express their dissatisfaction is via judicial review and their votes during elections.

Therefore, emphasis must be placed on the external scrutiny from courts or independent authorities on the deployment of AI applications. In other words, the justiciability of AI

[63] O'Neil 2016.

[64] For more discussion on the antithesis between the administration of things and the representation of interest see Armytage (1965); and Kumar (1978). Such legitimacy alternatively is based on the outcomes that were achieved. For more analysis about the legitimacy based on the 'telos' see Weiler 1991.

[65] As Mulgan states 'In the context of a democratic state, the key accountability relationships in this core sense are those between the citizens and the holders of public office and, within the ranks of office holders, between elected politicians and bureaucrats.' Mulgan 2000, p 556.

applications must not be barred based on the non-regulatory nature of the administrative process in civil law systems, or the ripeness doctrine in common law systems.

To exemplify this, the Armstrong case serves as a strong example. In this case, the Idaho Department of Health and Welfare employed algorithms to design the budget for Idaho's Developmental Disabilities Waiver program.[66] It argued that 'this dispute is not ripe for resolution because the mere preparation of a budget does not entitle a participant to notice under either the Due Process Clause or the Medicaid Act. The Department contends that the Plaintiffs will not suffer a deprivation of property under the Fourteenth Amendment until services are actually denied.'[67] The court rejected the ripeness argument on the ground that 'Postponing adjudication of this dispute would not bring greater clarity to whether the Department's 2011 Budget Notices were adequate.'[68]

b. AI applications in the democratic process

AI applications of the public sector are already employed in relation to the democratic process. like algorithmic design of electoral districts and verification of voter signatures.[69] Ab initio, the AI ACT proposal classifies as high risk any AI systems employed in relation to the democratic process and imposes technical and regulatory requirements.[70] Obviously, such applications are expected to be subject to extensive scrutiny from political actors and media.

However, the democratic process might be threatened from AI applications that are both non-political in nature and possibly classified as low risk. From the outset, AI applications employed by the state have the potential to access such sources of data. As it has been previously stated,[71] the potential of all AI applications depends on the quality and quantity of data. In other words, the intelligence of an algorithm depends heavily on the input, which heavily influences the output. Therefore, AI applications embedded in different agencies, for instance in tax authorities or social security agencies, might be programmed by malicious incumbents and ruling parties to offer them useful information and insights about the electorate giving them an advantage vis as vis their political opponents.

To what extent is such a scenario science fiction? This is the first critical question, and if the answer to this question is that democracy might be threatened from such abuse of power, then the second critical question is whether the AI Act has sufficient safeguards to protect the democratic process.

Two points are relevant to the former question. First, on several occasions, incumbents (political actors holding office) have misused the state resources[72] for self-entrenchment

[66] See K.W. v. Armstrong, No. 14-35296 (9th Cir. 2015).
[67] See K.W. v. Armstrong, No. 14-35296 (9th Cir. 2015) p 13.
[68] See K.W. v. Armstrong, No. 14-35296 (9th Cir. 2015) p 14.
[69] See Office of Science and Technology Policy, Blueprint for an AI Bill of Rights; Examples of Automated Systems available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/examples-of-automated-systems/
[70] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, [Title III].
[71] See in the introduction.
[72] The OSCE/ODIHR Handbook for the Observation of Campaign Finance stresses that 'the abuse of state resources can be defined as undue advantage obtained by certain parties or candidates, through use of their official

purposes distorting the level playing field in the political process. Suffice to mention here that with the introduction of television and the establishment of public broadcasting services, incumbents around the world took advantage of their power to nominate directors in order to transform the public broadcasting into means to advertise government's work and therefore setting an uneven playing field for the opposition.[73]

Possibly the most emblematic moment of abuse of power and misuse of technological recourses for self-entrenchment purposes is when President Nixon orchestrated the wiretapping of the telephones in the Watergate Hotel, where the democratic party was holding its convention. Therefore, the realization that states are lakes of data in combination with the possibility to employ AI applications raises questions about abuse of power and maladministration of such resources for self-entrenchment purposes.[74]

In relation to the second question, whether the AI Act proposal has sufficient safeguards to protect the democratic process, two issues are relevant: the first is the presence of 'information asymmetries' due to the complexity of AI applications, and the second issue concerns the sanctions against AI applications employed by the state. In relation to the information asymmetry of AI and algorithms, an illustrative case is the Cambridge Analytica scandal.

The Cambridge Analytica scandal was a critical event that turn the focus of policy makers on the role of private entities in the democratic process and on how AI applications, in combination with quality of data, may influence voters. Policy makers realised the potential and the impact of the information technology ecosystem without necessary checks. Social media platforms having access to users' important and sensitive personal data became a fertile ground for disinformation and voters' manipulation. However, the practices of Cambridge Analytica were revealed only when a worker disclosed in detail their practices. The parties involved, including Meta (at that time Facebook) as the controller of the data and voters as data subjects, had no material knowledge of the data breach and the manipulation.

Eventually, the EU enacted comprehensive regulation to protect users and to shield the democratic process. The GDPR plays a key role to protect users' personal data in automated processes, and it will be complemented by the AI ACT which prohibits AI systems with the potential to manipulate users through subliminal techniques. However, effective protections were enhanced with the Digital Service Act, which provides better protections to users by establishing a powerful transparency and accountability framework for online platforms. Additionally, the Digital Service Act grants EU authorities the power to access and receive

positions or connections to governmental institutions, in order to influence the outcome of elections.' See Handbook for the Observation of Campaign Finance, Published by the OSCE's Office for Democratic Institutions and Human Rights (OSCE/ODIHR 2015) p 22.

[73] 'Public subsidies to political parties can take a variety of forms, including tax breaks, free access to public services including airtime, access to public buildings, provision of goods and allocation of financial resources. Considering the impact of resources on political competition the two most important forms of public subsidies are financial support and free airtime.' See Money in Politics: Sound Political Competition and Trust in Government (OECD Paris 14-15 November 2013) para 20.

[74] About the importance of the level playing field in the political process see Antonios Kouroutakis, 'How liberal is a democracy without a level playing field in the political process?', U.K. Const. L. Blog (21st May 2020) (available at https://ukconstitutionallaw.org/).

information about automation systems,[75] therefore mitigating risks for the democratic process such as disinformation and election manipulation.

The AI Act has provisions requiring transparency and explainability for AI applications classified as high risk. Moreover, any AI application with intent to manipulate persons is prohibited. However, by default all AI applications employed by the public sector should be characterized as risky subject to special safeguards guaranteeing that abuse of power won't take place. In such manner, the democratic process will be better protected even from AI systems deployed successfully in various low risk areas but misused by the incumbents or the ruling political party in order to gain insights into populations giving them a comparative advantage in the political process.

Finally, it is worth stressing that the AI Act provides for hefty administrative fines in case private entities or EU agencies violate the AI Act.[76] However, in case the national governments violate the EU AI Act, the sanctions' framework is not clear. In particular, the sanctions in case illegal AI applications are employed by the national government is subject to an opening clause that allows the EU Member States to decide the fines imposed on public authorities. In particular, Article 71 para 7 states that 'Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.'[77] Instead, the criminalization of the misuse of AI applications would have a stronger deterrence effect and would protect the democratic process to a greater extent.

Conclusions

In essence, the use of AI applications and their abilities might have an unparallel transformative force on the state and the administration's relationship with citizens. Their application has the potential to usher in a new paradigm where alternative ways to perform administrative tasks may emerge.

The deployment of such technology in the private and the public sector signals that the time has come for their regulation. The current EU legal framework and proposed legislation for regulating AI is limited in critical ways, as demonstrated by the analysis of the AI Act and positive law in Part A.

This article argued that AI applications employed by the public sector should be subject to a separate risk category for two reasons: first because specific safeguards are necessary in relation to the AI applications in the public sector in order to enhance the legitimacy and

[75] see Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1 OJ L 277, 27.10.2022 Article 40.

[76] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 71.

[77] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final 21.04.2021, Article 71 para 7.

accountability of such applications, and second because AI applications in the public sector with access to the lake of data of the state create an unprecedented public resource which must be safeguarded from malicious incumbents who would be keen to take advantage of such resource for self-entrenchment purposes.

Reference Lists

Al-Mushayt O S (2014) Automating E-government services with artificial intelligence. IEEE Access 7

Alexopoulos C, Androutsopoulou A, Charalabidis Y, Diamantopoulou V, Lachana Z, Loutsaris M A (2019) How machine learning is changing e-government. Association for Computing Machinery: 354

Armytage W H G (1965) The Rise of the Technocrats. Routledge

Barocas S, Selbst A D (2018) The Intuitive Appeal of Explainable Machines. Fordham Law Review 87: 1085

Bell J, Lichere F (2022) Contemporary French Administrative Law. Cambridge University Press

Black, Jr C L (1967) Foreword:"State Action", Equal Protection, and California's Proposition 14. Harvard Law Review 81: 69

Brauneis R, Goodman EP (2018) Algorithmic Transparency for the Smart City' Yale Journal of Law & Technology 20: 103

Julie K. Brown J K (2008) Less is More: Decluttering the State Action Doctrine. Missouri Law Review 73: 561

Bullock J B (2019) Artificial intelligence, Discretion, and Bureaucracy. The American Review of Public Administration 49: 751

Buchanan A (2002) Political Legitimacy and Democracy, Ethics 112: 689

Buiten M C (2019) Towards Intelligent Regulation of Artificial Intelligence. European Journal of Risk Regulation 10: 41-49

Cavaliere P, Graziella R (2022) From Poisons to Antidotes: Algorithms as Democracy Boosters. European Journal of Risk Regulation 13: 421

Chen Y, Salem F, Zuiderwijk A (2021) Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. Government Information Quarterly 38

Chen Y, Lin C, Liu H (2019) Beyond State v. Loomis: Artificial Intelligence, Government Algorithmization, and Accountability. International Journal of Law and Information Technology 27: 122

Chenok D, Dawson G S., Desouza K C. (2020) Designing, developing, and deploying artificial intelligence systems: Lessons from and for the public sector. Business Horizons 63: 205

Chli M, Deepka G, Vogiatzis G (2022) Fully-Autonomous, Vision-based Traffic Signal Control: from Simulation to Reality. Association for Computing Machinery 1: 454-462

Citron D, Pasquale F (2014) The Scored Society: Due Process for Automated Predictions. Washington Law Review 89: 1

Craig P (2010) Specific Powers of Public Contractors. in Noguellou R, Stelkens U (eds), Droit compare´ des contrats publics/Comparative Law of Public Contracts. Bruylant

De Souza Bermejo P H, Gomes de Sousa W, Pereira de Melo E R, Sousa Farias R A, Oliveira Gomes A (2019) How and where is artificial intelligence in the public sector going? A literature review and research agenda. Government Information Quarterly 36

Engstrom D F, Ho D E, Sharkey C M, Cuéllar M (2020) Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies. Administrative Conference of the United States

Feldstein S (2019) How Artificial Intelligence is reshaping repression. Journal of Democracy 30: 40

Freeman K (2016) Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis. North Carolina Journal of Law and Technology 18: 75

Huston M (2022) DeepMind AI invents faster algorithms to solve tough maths puzzles. Nature https://www.nature.com/articles/d41586-022-03166-w Accessed on 29 November 2022

Kegan E (2000-2001) Presidential Administration. Harvard Law Review 114: 2246

Kitchen R (2014) The Data Revolution: Big Data, Open Data, Data Infrastructures and Three Consequences. SAGE Publications Ltd

Klarman K (1997) Majoritarian Judicial Review: The Entrenchment Problem. Georgetown Law Journal 85: 491

Kouroutakis A (2021) Legitimate and Illegitimate Political Self-entrenchment and Its Impact on Political Equality. ICL Journal 15: 1

Kumar K (1978) Prophecy and Progress. Penguin

Levinson D, Benjamin Sachs B (2015) Political Entrenchment and Public Law. Yale Law Journal 125: 400

Maclure J *(2021) AI, Explainability and Public Reason: The Argument from the Limitations of the Human Mind. Minds & Machines 31: 421–438*

Medina E (2014) Designing freedom, regulating a nation: socialist cybernetics in Allende's Chile. Journal of Latin American Studies 38: 571-601

Mellouli S, Rjab A B (2018) Smart cities in the era of artificial intelligence and internet of things: literature review from 1990 to 2017. Association for Computing Machinery Article No. 81: 1-10

Mulgan R (2000) Accountability: An Ever-Expanding Concept. Public Administration 555

Mulgan R (2003) Holding Power to Account: Accountability in Modern Democracies. Springer

O'Neil C (2016) Weapons of Math Destruction How Big Data Increases Inequality and Threatens Democracy. Penguin Books

Pasquale F (2015) The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press

Pildes R H (2004) The Constitutionalization of Democratic Politics. Harvard Law Review 118: 28

Rawls J (1996) Political Liberalism. Columbia University Press

Scharpf W (1998) : Interdependence and democratic legitimation, MPIfG Working Paper, No. 98/2, Max Planck Institute for the Study of Societies, Cologne, http://www.mpifg.de/pu/workpap/wp98-2/wp98-2.html

Scharpf W (1999) Governing Europe: Effective and Democratic. Oxford University Press

Singh MP (1985) German Administrative Law, in Common Law Perspective. Springer

Smith A et al (2012) Using Maximum Entropy modelling to predict the potential distributions of large trees for conservation planning. Ecosphere 6: 1

Strickland H C (1991) The State Action Doctrine and the Rehnquist Court. Hastings Constitutional Law Quarterly 18: 587

Tyler T (1990) Why People Obey the Law. Princeton University Press

Weiler J H H (1991) The Transformation of Europe Yale Law Journal 100: 2403

Weber M (1964) The Theory of Social and Economic Organization. Free Press