19

The Use of Algorithmic Systems by Public Administrations

Practices, Challenges and Governance Frameworks

Nathalie A. Smuha

19.1 INTRODUCTION

Public administrations play a unique role in our societies. As an instrument of the state, they are responsible for the execution of laws, the implementation of public policies, and the management of public programs – both at the national and the local level. A large part of their tasks consists of taking administrative acts, which can have an individual or a general scope.[1] These decisions affect individual, collective and societal interests, and can have a significant impact on the everyday lives of natural and legal persons.[2] Increasingly, public administrations rely on algorithmic systems – including artificial intelligence (AI) systems – in their decision-making processes.[3] This practice has also been referred to as "algorithmic regulation," since it essentially comes down to regulating[4] natural and legal persons through algorithmic applications.[5] Today, most of these applications are still primarily used to *inform*

[1] The Council of Europe's Committee of Ministers has defined administrative acts as comprising (a) legal acts, of both individual and general application, (b) physical acts of the administration taken in the exercise of public authority which may affect the rights or interests of natural or legal persons; and (c) situations of refusal to act or an omission to do so in cases where a public authority is under an obligation to act. See Committee of Ministers, "Recommendation Rec (2004) 20 of the Committee of Ministers to Member States on Judicial Review of Administrative Acts."

[2] See Nathalie A. Smuha, "Beyond the individual: Governing AI's societal harm" (2021) *Internet Policy Review*, 10(3): 1–33. See also Karen Yeung, "Why worry about decision-making by machine?" in Karen Yeung and Martin Lodge (eds), Algorithmic Regulation (Oxford University Press, 2019), 21–48.

[3] See also Weslei Gomes de Sousa, Elis Regina Pereira de Melo, Paulo Henrique De Souza Bermejo, Rafael Araújo Sousa Farias, and Adalmir Oliveira Gomes, "How and where is artificial intelligence in the public sector going? A literature review and research agenda" (2019) *Government Information Quarterly*, 36(4): 101392; Jamie Berryhill, Kévin Kok Heang, Rob Clogher, and Keegan McBride, "Hello, World: Artificial intelligence and its use in the public sector," *OECD Working Papers on Public Governance*, No. 36, OECD Publishing, Paris, 2019.

[4] Drawing on Julia Black, regulation is broadly understood as a means of managing risk or influencing behaviour in order to achieve a pre-specified goal. See Julia Black, "Learning from regulatory disasters," *24 LSE Law, Society and Economy Working Papers* 3, 2014.

[5] See Nathalie A. Smuha, *Algorithmic Rule by Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law* (Cambridge University Press, 2025), 4. This term has also been used in a broader sense. For a useful overview, see Lena Ulbricht and Karen Yeung, "Algorithmic regulation:

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

rather than to *adopt* administrative acts. This is, however, rapidly changing, as ever more acts – as well as sub-decisions that underpin those acts – are being outsourced to algorithmic systems.

Algorithmic regulation can offer numerous advantages to public administrations,[6] many of which center around faster information retrieval and data processing, which in turn can lead to efficiency gains and better service provision. For this reason, algorithmic regulation is sometimes also heralded as a tool to enhance human rights, democracy and the rule of law, as it could help ensure that the execution and implementation of legal rules occurs in a more efficient manner, and that the rights of natural and legal persons are better protected. At the same time, the proclaimed benefits of algorithmic regulation do not always materialize in practice, and even when they do, they are rarely evenly distributed. Numerous examples exist of algorithmic regulation deployed by public administrations in a way that – often unintendedly – ran counter to the values of liberal democracy.[7] These values should however also be protected when the state decides to rely on algorithmic systems. In this chapter, I will therefore focus on the deployment of algorithmic regulation by public administrations, and explore some of the ethical and legal challenges that may arise in this context.

I start by setting out a brief history of public administrations' reliance on automation and algorithmic systems (Section 19.2). Subsequently, I explore some applications of algorithmic regulation that have been implemented by public administrations across several public sector domains (Section 19.3). I then respectively discuss some of the horizontal and sectoral challenges that reliance on algorithmic regulation brings forth, which require being addressed to ensure that core liberal democratic values remain protected (Section 19.4). Finally, I move toward an analysis of the legal framework that governs the use algorithmic regulation by public administrations, with a particular focus on the European Union (Section 19.5), before concluding (Section 19.6).

19.2 ALGORITHMIC REGULATION IN CONTEXT

Public administrations have existed since antiquity, yet in many jurisdictions, the nineteenth century brought a significant transformation both in terms of their size and their professionalization. The expansion of their competences and tasks – which

A maturing concept for investigating regulation of and through algorithms" (2022) *Regulation & Governance*, 16(1): 3–22.

6 See Chapter 1 of this Handbook for an extensive discussion of artificial intelligence as a research domain.

7 See for example, Virginia Eubanks, *Automating Inequality – How High-Tech Tools Profile, Police and Punish the Poor* (New York, Picador, 2019); Fabio Chiusi, Sarah Fischer, Nicolas Kayser-Bril and Matthias Spielkamp (eds), Automating Society Report 2020, AlgorithmWatch and Bertelsmann Stiftung, 2020, https://automatingsociety.algorithmwatch.org; Calo, Ryan, and Danielle Keats Citron, "The automated administrative state: A crisis of legitimacy" (2021) *Emory Law Journal* 70(4): 797–845.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

was also propelled by the growth of welfare programs – was accompanied by a demand for more specialized expertise, as well as a process of rationalization and streamlining of public decision-making processes. This, in turn, also required more data collection and analysis based on which administrative acts could subsequently be taken.[8] In this regard, Peeters and Widlak pointed out that: "*as state tasks expanded, especially in welfare states, so did the number of registrations and their importance. Knowing your citizens has never been more important as when you try to decide who is eligible to student grants, social security, health care, social housing, or pensions.*"[9] The increase in the number of decisions to be taken also necessitated a rethinking of organizational information processes in order to secure the continued efficiency of public administrations. Unsurprisingly, the adoption of modern information and communication technologies (ICT) was strongly aligned with this purpose.[10]

Public administrations' embrace of ICT technologies is hence nothing new, and algorithmic regulation is an inherent part of this development. From the 1980s onwards, the uptake of such tools was further spurred by the New Public Management (NPM) movement, "*a collection of ideas that have as their main focus the importation of private sector tools, such as efficiency, private sector approaches, privatization and outsourcing, market-based mechanisms, and performance indicator into the public service.*"[11] While these ideas have not been immune from criticism and were found outdated already by the early 2000s,[12] they were quite influential and further entrenched the belief that public administrations could rely on (commercial) digital applications to attain their goals more efficiently – thereby, however, problematically elevating "efficiency" to a prime consideration, sometimes to the detriment of other important (public) interests and values.[13] Gradually, the uptake of ICT technologies also transformed the administrative

[8] See in this regard also Smuha, n (5), 83.

[9] Rik Peeters and Arjan Widlak, "The digital cage: Administrative exclusion through information architecture – The case of the Dutch civil registry's master data management system" (2018) *Government Information Quarterly*, 35(2): 175–183.

[10] Arre Zuurmond therefore points out that "*bureaucracy and informatisation seem to go hand in hand.*" See Arre Zuurmond, *De Infocratie: Een Theoretische En Empirische Heroriëntatie Op Weber's Idealtype in Het Informatietijdperk* (Phaedrus, 1994), 2.

[11] Rónán Kennedy, "The Rule of Law and Algorithmic Governance" in Woodrow Barfield (ed), *The Cambridge Handbook of the Law of Algorithms* (Cambridge University Press, 2020), 211. See also E. H. Klijn, New Public Management and Governance: A Comparison, in D. Levi-Faur (ed.), *The Oxford Handbook of Governance* (Oxford University Press, 2012) 209.

[12] See in this regard Karen Yeung, "The new public analytics as an emerging paradigm in public sector administration" (2022) *Tilburg Law Review* 27(2): 4. In this regard, she also refers to Christopher Hood, "Public Management, New" in N. J Smeltser and P. B Bates (eds) *International Encyclopedia of the Social & Behavioral Sciences*, Volume 12 (Oxford: Elsevier, 2001), 12553–12556.

[13] See also Patrick Dunleavy, Helen Margetts, Simon Bastow, Jane Tinkler, "New public management is dead-long live digital-era governance" (2005) *Journal of Public Administration Research and Theory*, 16(3): 467–494.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

apparatus from "street-level" to "system-level" bureaucracies, as pointed out by Bovens and Zouridis.[14] They note that:

> Insofar as the implementing officials are directly in contact with citizens, these contacts always run through or in the presence of a computer screen. Public servants can no longer freely take to the streets, they are always connected to the organization by the computer. Client data must be filled in with the help of fixed templates in electronic forms. Knowledge-management systems and digital decision trees have strongly reduced the scope of administrative discretion. Many decisions are no longer made at the street level by the worker handling the case; rather, they have been programmed into the computer in the design of the software.[15]

Over time, the trend of informatization and automatization persisted, while the technologies used for this purpose became ever more sophisticated. Rather than relying primarily on rule-based systems and decision-trees, in the last few years, public administrations also increasingly started turning to data-driven automated analysis, often in a way that likewise seems to "*mimic or borrow from the success of commercial techniques*," a trend that Karen Yeung conceptualized as New Public Analytics (NPA), to highlight its (dis)continuity with NPM.[16] These data-driven technologies are typically based on advanced statistics and machine learning, and can be used to make probabilistic inferences and predictions.

Today, a large number of countries in the world adopted an "AI strategy," which virtually always includes a section with policy initiatives to bolster the uptake of AI systems in the public sector. Often, these strategies focus on maximizing AI's benefits, which in public administrations translates to a more efficient provision of citizen services, a speedier allocation of rights and benefits, and a reduction of backlogs and waiting times – or more generally: doing more with less.

This aspiration should not be seen separate from the difficult economic situation in which many countries found themselves after respectively the global financial crisis of 2008 and the COVID-19 pandemic which broke out in 2020. These developments, along with a more political tendency to limit public spending, forced many public administrations to cut costs. Indeed, as noted by Yeung, "*the pursuit of austerity policies that have seriously reduced public sector budgets has prompted*

[14] See Mark Bovens and Stavros Zouridis, "From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control" (2002) *Public Administration Review*, 62(2): 174–184. They rely on Lipsky's conceptualization of public-service workers as "street-level bureaucrats," by virtue of the fact that they interact directly with individual citizens (hence "street-level"), and have considerable discretion when taking decisions. See Michael Lipsky, *Street-level Bureaucracy: Dilemmas of the Individual in Public Service* (New York, NY: Russell Sage Foundation, 1980).

[15] Bovens and Zouridis, n (14), 177. See in this regard also Justin B. Bullock, "Artificial intelligence, discretion, and bureaucracy" (2019) *The American Review of Public Administration*, 49(7): 751–761.

[16] See Yeung, n (12), 7.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

growing interest in automation to reduce labour costs while increasing efficiency and productivity."[17] Unfortunately, as the next section will show, this eagerness has sometimes also led to problematic implementations of algorithmic regulation, with significant adverse consequences to those who were subjected to such systems, and without generating the benefits that were promised by the system's developers.

19.3 ALGORITHMIC REGULATION IN PRACTICE

Public administrations take a wide array of administrative acts on a daily basis. These acts or decisions are as diverse as allocating social welfare benefits, identifying tax fraud, imposing administrative fines, collecting taxes, granting travel visas, procuring goods and services, and handing out licenses and permits. Algorithmic regulation is gradually being deployed in all of these areas, in ever more creative and far-reaching ways. Evidently, the uptake of such applications significantly differs from one country to the other, and even from one ministry or municipality to the other – also in the European Union. While some are rolling out fancy facial recognition systems, others are still struggling with putting in place basic infrastructures that will enable digital technologies to operate in the first place. To concretize the variety of applications for which algorithmic regulation is deployed, and especially some of the risks they entail, let me offer a few examples.

Under French tax laws, properties with a pool must be declared to the government, as they increase a property's value and are hence subjected to higher taxes.[18] Many property owners however do not declare their pools, in contravention with the law. Therefore, in October 2021, nine French regions trialed an AI application developed by Capgemini (a French IT and consulting company) and Google, which analyzes areal images of properties and applies object recognition technology to assess whether the properties showcase non-declared pools.[19] The application's development was said to cost around €26 million.[20] According to several media outlets in 2022, more than 20,000 "hidden pools" were discovered by the tax authorities, contributing to about €10 million in revenues.[21] Later that year, the French authorities decided to roll out the application across the country, hoping this would lead to

[17] See Yeung, n (12), 6.

[18] Environmental considerations play a role here too, as many French regions adopted policies to reduce water consumption given its scarcity, while private swimming pools require considerable water.

[19] James Vincent, "French government uses AI to spot undeclared swimming pools – and tax them," *The Verge*, August 30, 2022, www.theverge.com/2022/8/30/23328442/france-ai-swimming-pool-tax-aerial-photos.

[20] Hannah Thompson, "France's way of tracking undeclared pools is unfair, says report," *The Connexion*, January 23, 2024, www.connexionfrance.com/article/Practical/Money/France-s-way-of-tracking-undeclared-pools-is-unfair-says-report.

[21] See for example, Kim Willsher, "French tax officials use AI to spot 20,000 undeclared pools," *The Guardian*, August 29, 2022, www.theguardian.com/world/2022/aug/29/french-tax-officials-use-ai-to-spot-20000-undeclared-pools; Undeclared pools in France uncovered by AI technology, *BBC News*, August 29, 2022, www.bbc.com/news/world-europe-62717599

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

€40 million additional tax earnings. By 2024, it was reported that more than 120,000 undeclared pools had been identified, thus allegedly reaching this target.[22]

That said, claims have also been made that the application has a margin of error of 30%, "*mistaking solar panels for swimming pools*" and "*failing to pick up taxable extensions hidden under trees or in the shadows of a property*."[23] Furthermore, in addition to questions that arose around the right to privacy, in November 2023, the French Court of Audit ("Cour des Comptes") published a report in which it found that the application's use constitutes a form of unequal treatment of French citizens, as it is not deployed in France's overseas territories and in Corsica, but only in the mainland. Accordingly, not all French taxpayers are subjected to the same scrutiny, which constitutes an inequality.[24] Interestingly, in the same report, the Court of Audit also questioned the deployment of automated tax evasion detection techniques more generally, stating that insufficient evidence of their effectiveness exists[25] – a recurring theme in the context of algorithmic regulation.

For another example, let me turn to the Netherlands, where the government was forced to resign in 2021 following the so-called "childcare benefits scandal."[26] Since the early 2010s, the Dutch tax authorities have been deploying an algorithmic system to help determine the risk of fraud by recipients of childcare benefits. Due to the unduly harsh legal rules of the Dutch system at the time, even a suspicion of fraud or involuntary error could lead to a penalty, whereby all the received benefits were retroactively claimed back by the government, leading thousands of families to accumulate (at times wrongfully attributed) debts they could not afford to pay off.[27] This not only caused depressions and suicides, but – due to ensuing poverty and a risk of neglect – some children were subsequently also taken away from their parents into foster care.[28] Only years later, the system was found to be in breach with privacy legislation, as well as reliant on discriminatory risk indicators.[29] People with

[22] Thompson, n (20).

[23] Willsher, n (21). At this stage, the application is hence merely used to suggest tax authorities which taxpayers must be further scrutinized.

[24] Cour des Comptes, "La Détection de la Fraude Fiscale des Particuliers – Une incontestable modernization des méthodes, des résultats encore insuffisants," November 2023, www.ccomptes.fr/sites/default/files/2023-11/20231115-Detection-fraude-fiscale-des-particuliers.pdf.

[25] Ibid., 42.

[26] John Henley, "Dutch government resigns over child benefits scandal," *The Guardian*, January 15, 2021, www.theguardian.com/world/2021/jan/15/dutch-government-resigns-over-child-benefits-scandal.

[27] Tweede Kamer der Staten-Generaal (Dutch Parliament), "Verslag – Parlementaire ondervragingscommissie Kinderopvangtoeslag: Ongekend onrecht," December 2020, www.tweedekamer.nl/sites/default/files/atoms/files/20201217_eindverslag_parlementaire_ondervragingscommissie_kinderopvangtoeslag.pdf.

[28] Melissa Heikkilä, "Dutch scandal serves as a warning for Europe over risks of using algorithms," *Politico*, March 29, 2022, www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.

[29] Autoriteit Persoonsgegevens (Dutch Data Protection Authority), Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, July 2020, 2018–22445, https://autoriteitpersoonsgegevens.nl/uploads/imported/onderzoek_belastingdienst_kinderopvangtoeslag.pdf.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

a second nationality and single mothers were, for instance, more likely to be identified as potential fraudsters, and hence subjected to higher scrutiny. However, by the time this breach was established, the damage was done, often irreparably so.[30]

Algorithmic regulation is also finding its way into other public sector domains. During the COVID-19 pandemic in 2020, the UK, for instance, decided to deploy an algorithmic system to allocate students' A-level grades after exams had been canceled in schools.[31] One potential solution was to rely on teachers' predictions of what the final grade would have been had the exam gone through. Yet given the observation that teachers tend to inflate grades and that this should hence not be the only factor to consider, the government suggested using an algorithmic system instead, claiming it would provide a "fairer" result. It decided to outsource students' grading to an algorithmic tool that determined its output not only based on teachers' predictions but also based on previous exam results and the overall grade distribution of a school over the last three years. When almost 40% of the students ultimately received lower grades than they anticipated, this led to a public outcry, as well as public scrutiny of the system.[32] In addition to concerns around the system's low accuracy and the way it penalized students in schools with a historically lower performance, the system was also deployed in a biased manner. If a school had fifteen students or less for a particular subject, more weight was given to the teacher's estimate – which the government already acknowledged was likely "too high." This policy choice ended up benefitting students attending private schools in particular, as they typically have fewer students per subject, thus also raising concerns of discrimination.

Finally, let me provide an example from the United States, where the Idaho Department of Health and Welfare decided to roll out an algorithmic system in 2011 in the context of a Medicaid program for persons with a disability. Such persons were eligible for a personalized benefits budget depending on their needs, and the system was used to calculate this budget with the aim of enhancing the program's efficiency. However, it turned out to have several flaws: Some people who had developed more substantial needs contradictorily saw their budget shrinking, without any sound explanation or justification.[33] As a consequence, highly vulnerable

[30] See also the Australian example discussed in Terry Carney Ao, "The new digital future for welfare: Debts without legal proofs or moral authority?" (2018) *UNSW Law Journal Forum*, 1: 1–16.

[31] Will Bedingfield, "Everything that went wrong with the botched A-levels algorithm," *Wired UK*, August 10, 2020, www.wired.co.uk/article/alevel-exam-algorithm.

[32] Daan Kolkman, "'F**k the algorithm'?: What the world can learn from the UK's A-level grading fiasco," *LSE Impact Blog*, August 26, 2020, https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/.

[33] See David Restrepo-Amariles, 'Algorithmic Decision Systems: Automation and Machine Learning in the Public Administration' in Woodrow Barfield (ed), *The Cambridge Handbook of the Law of Algorithms* (Cambridge University Press, 2020), 289.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

individuals were wrongfully denied the help they required. Similar systems were also deployed in other states, which in the worst case even led to the death of disabled persons who did not receive the care they depended on.[34] Since the problematic decisions of Idaho's algorithmic system were not reversed and the people concerned felt unheard, they were forced to span a class action before Idaho's District Court, thus bringing to the surface a number of the system's deficiencies, which were tied to its lack of transparency and model and data validation.[35] Ultimately, the Court found that the tool's use amounted to a breach of due process rights and was hence unconstitutional.[36]

These examples, while taken from various public sector areas, show at least two similarities. First, the implementation of algorithmic regulation in each of these cases started from the desire to enhance public services' efficiency, whether it concerns detecting tax evasion, uncovering benefits fraud, or allocating healthcare benefits. Second, they also showcase the adverse consequences that can ensue when such systems are used to implement (problematic) policies at scale, without consideration for the risks they entail when developed and deployed irresponsibly. In what follows, drawing on these examples, let me unpack in more detail some of the challenges that public administrations must consider when relying on algorithmic regulation.

19.4 CHALLENGES FOR THE RESPONSIBLE USE OF ALGORITHMIC REGULATION

Over the past decade, a rich academic literature developed around the ethical, legal and societal concerns associated with algorithmic systems, and particularly with AI. Many of AI's risks manifest themselves horizontally, in virtually all domains in which the technology is used. Others are more sector-specific and depend on the particular context or domain. As noted earlier, public authorities play a different role in society than private actors do, as they are tasked with upholding and promoting the *public* interest. Since public administrations are responsible for the fulfilment of numerous rights that are essential for people's well-being, the automation of problematic government policies can have vast adverse consequences. In what follows, I respectively discuss how algorithmic regulation can affect fundamental rights like privacy and non-discrimination (Section 19.4.1), the rule of law (Section 19.4.2), a sense of responsibility (Section 19.4.3), and the exercise of public power (Section 19.4.4).

[34] Erin McCormick, "What happened when a 'wildly irrational' algorithm made crucial healthcare decisions," *The Guardian*, July 2, 2021, www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions.

[35] See Restrepo-Amariles, n (33), 289. See also a discussion of this case in Smuha, n (5), 55.

[36] K.W. v. Armstrong, 180 F. Supp. 3d 703 (D. Idaho, 2016) (No. 1:12-cv-00022-BLW).

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

19.4.1 *Impacting Fundamental Rights*

One of the most common challenges arising from use of algorithmic regulation is its impact on fundamental rights, and most notably the right to privacy and data protection.[37] The performance of algorithmic systems hinges on the availability, collection and processing of high volumes of (personal) data, especially when used to enable scaled decision-making about individuals. Such data collection can have vastly intrusive effects on people's lives and can potentially be used in ways that undermine their agency.[38]

In the worst case, the irresponsible implementation of algorithmic regulation not only breaches privacy legislation (such as in the Dutch case discussed earlier), but can also lead to the mass-surveillance of citizens, in the name of efficiency. Unjustified intrusions into people's private lives can also affect the value of democracy, especially when data is gathered about potential individuals or groups that are not favored by the government. Moreover, privacy is often instrumental to secure other fundamental rights, such as the right to free speech and the right to human dignity, which are hence also at stake.[39] Yet given the financial investments that public administrations undertake when they decide to develop, procure or implement algorithmic regulation, and given the path dependencies this brings along, administrations are only incentivized to gather ever more data. A balance must hence be found between the government's desire to exercise its tasks with more efficiency, and the protection of people's private lives.

Another important concern relates to the way in which algorithmic systems can affect the right to non-discrimination.[40] Human beings have a range of biases and prejudices, which can at times be unjust or discriminatory, for instance when they echo societal stereotypes, historical inequalities, or other (often unconscious) problematic influences. Since algorithmic systems are designed and developed by human beings, their output can reproduce these unjust human biases, thus mirroring and potentially even exacerbating discriminatory practices.[41] The earlier

[37] See in this regard also Chapter 7 of this Book: Pierre Dewitte, 'AI meets the GDPR: Navigating the impact of data protection on AI systems' in Nathalie A. Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).

[38] See also Carissa Véliz, *Privacy is Power: Why and How You Should Take Back Control of Your Data* (Penguin, 2020).

[39] See also for example, Ruth Gavison, "Privacy and the limits of law" (1980) *Yale Law Journal*, 89(3): 421–471, 455; Bart van der Sloot, "Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 5(3), 2014, 230–244, 231; See also more generally Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015).

[40] See in this regard also Chapter 4 of this Book: Laurens Naudts and Anton Vedder, "Fairness and Artificial Intelligence" in Nathalie A. Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).

[41] See also Mireille Hildebrandt, "The Issue of Bias: The Framing Powers of Machine Learning," in Marcello Pelillo and Teresa Scantamburlo (eds), *Machines We Trust: Perspectives on Dependable AI* (The MIT Press, 2021).

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

illustrations of algorithmic regulation have shown that this risk is not hypothetical. In the Dutch example, inequalities found their way into the system's parameters and dataset during the development phase, thus adversely affecting certain groups of the population. In France and in the UK, the algorithmic system was deployed in an unequal manner and hence exposed individuals to its impact in an uneven way.

At a much more banal level, it is also possible that flaws or errors seep into the development and deployment process of algorithmic regulation – whether through erroneous human input or invalid correlations and inferences drawn by the system. This risk, and the problematic consequences ensuing therefrom, was illustrated by the benefits-allocation system deployed in the US, yet many other examples exist.[42] More generally, the fact that public administrations are responsible for the allocation of basic socio-economic rights also renders these rights vulnerable when their implementation is wholly or partly outsourced to a flawed or biased system.

Evidently, public administrations can also adversely affect people's rights without the use of algorithmic systems. Yet their reliance on powerful tools that enable data processing at a much wider scale and higher speed, coupled with the opacity of the internal processes of these systems and the recurrent lack of transparency about their deployment not only aggravate these risks, but also makes it more difficult to discover them. Adding a layer of digitalization to public services can certainly provide benefits of scale, but it is also precisely this scale-element that renders it so risky when implemented without considering these concerns.

19.4.2 *Eroding the Rule of Law*

Algorithmic regulation also raises a number of challenges to the rule of law. In essence, the rule of law comes down to the idea that nobody stands above the law, and that citizens and government officials alike are subjected to legal rules.[43] It embodies the notion that, rather than being governed by the arbitrary whims of "men" (who, as Aristotle already pointed out, are susceptible to arbitrary passions that undermine rational thinking),[44] people should be governed by "laws," which are based on reason and offer predictability. The rule of law is a broad term that has been defined

[42] See in this regard also the examples provided by Eubanks, n (7).

[43] See for example, AV Dicey, *Introduction to the Study of the Law of the Constitution [1885]*, 10e ed., (Macmillan, 1968); Friedrich A Hayek, *The Road to Serfdom [1944]* (Institute of Economic Affairs, 2005); Joseph Raz, "The Rule of Law and Its Virtue," *The Authority of Law: Essays on Law and Morality* (Oxford University Press, 1979).

[44] In Aristotle's words "*he who bids the law rule may be deemed to bid God and Reason alone rule, but he who bids man rule adds an element of the beast; for desire is a wild beast, and passion perverts the minds of rulers, even when they are the best of men*," see Aristotle, *Politics* (Benjamin Jowett tr, Batoche Books, 1999), 77.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

in countless ways,[45] yet the Council of Europe's Venice Commission[46] provided a helpful conceptualization for the European legal order by breaking it down into several principles (which were subsequently taken over by the European Union).[47] Under this conceptualization, the rule of law encompasses six principles: (1) the principle of legality; (2) the principle legal certainty; (3) the prohibition of arbitrariness of executive power; (4) equality before the law; (5) effective judicial protection, with access to justice and a review of government action by independent and impartial courts, also as regards human rights; and (6) the separation of powers.[48]

Under this conceptualization, the rule of law is hence understood not only as requiring *procedural* safeguards, but also *substantive* ones.[49] Indeed, it is not enough to merely apply the law in an efficient and procedurally agreed upon manner. Otherwise, the law could simply be used as a (powerful) instrument to enforce illiberal and authoritarian policies – a practice that has been denoted as rule *by* law instead.[50] Rather, the law and its application should also protect and comply with substantive values, and particularly respect for human rights and democracy. Accordingly, whenever public administrations want to exercise their powers, they are constrained by these rule of law-principles, which ensure that the law plays a protective role in society.[51]

At first glance, algorithmic regulation seems rather innocuous from a rule of law-perspective, and could even be seen as potentially advancing its principles to a greater extent. By eliminating civil servants' discretion from the picture, along with their potentially inconsistent or arbitrary decision-making, algorithmic regulation could arguably catalyze Aristotle's aspiration of being ruled by *law* instead of *men*. However, on closer inspection, this unqualified relationship between the rule of law and the rule of men is too simplistic: just like laws are created, applied and interpreted by human beings, so are algorithmic systems inherently dependent on

[45] For this reason, it has also been described as an "essentially contested concept," see Jeremy Waldron, "The Rule of Law as an Essentially Contested Concept," in Jens Meierhenrich and Martin Loughlin (eds), *The Cambridge Companion to the Rule of Law. Cambridge Companions to Law* (Cambridge University Press, 2021), 121–136.

[46] European Commission for democracy through law (Venice Commission), The Rule of Law Checklist, Venice, March 11–12, 2016, www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e.

[47] See, for example, the EU's Conditionality Regulation which establishes a mechanism to protect the EU's budget against rule of law-infringements by Member States: Regulation 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget 2020, OJ L 433I, 22.12.2020, 1–10.

[48] For an analysis of these principles in the context of the public sector, see Smuha n (5), chapter 3.2.

[49] See in this regard also Paul Craig, "Formal and substantive conceptions of the rule of law: An analytical framework" (1997) *Public Law*, 467–487.

[50] See for example, Brian Tamanaha, "*On the Rule of Law: History, Politics, Theory*" (Cambridge University Press, 2004); Jeremy Waldron, "The Rule of Law," *The Stanford Encyclopedia of Philosophy*, in Edward N. Zalta and Uri Nodelman (eds.) (Fall 2023), https://plato.stanford.edu/archives/fall2023/entries/rule-of-law/.

[51] See also, Geranne Lautenbach "The Rule of Law Concept" in *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press, 2013), 18–69.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

the human beings that design, develop and deploy them.[52] There are hence several distinctive challenges to the ideal of the rule of law when public administrations rely on algorithmic systems,[53] of which an important one relates to the very act of implementing the law in an automated manner.

Automating the law's application through algorithmic regulation requires a "translation process" from text-based laws and policies to digital code. To a greater or lesser extent, text-based provisions are inevitably open to different (and contestable) interpretations, sometimes inadvertently, sometimes purposely. It is often precisely this very openness of the law that enables it to play its protective role, by facilitating its tailored interpretation to the specific situation at hand. Indeed, laws typically consists of (overly) general rules set forth by the legislator, which must subsequently be interpreted and applied to concrete cases. However, once automated, the law becomes more rigid, as a particular interpretation must be codified or optimized for. There is thus a risk that this translation process changes the nature of the law in a problematic manner. The translation may, for instance, occur in a way that is too legalistic, that incorporates biases and inequalities, that deviates from the intent of the legislator and unwarrantedly bolsters the power of the executive, that undermines the predictability and congruence of the law's application, that erodes essential rights and liberties or limits their scope, or that leaves individuals unable to contest the chosen interpretation and subject it to judicial review.

This risk not only undermines the rule of law's principles, but also erodes the constraints they place on government power, to the detriment of other liberal democratic values. In other words, algorithmic regulation could turn into a powerful tool to enforce rule *by* law. While this risk is not limited to the algorithmic context, the automated application of the law could be a highly efficient tool to erode the very protection the law is meant to afford, on a broader scale than ever before – a threat I conceptualized as *algorithmic rule by law*.[54] Bearing in mind the inherent malleability of software, and the additional level of opacity it introduces, it is thus essential to remain vigilant and put the necessary safeguards in place to ensure public administrations do not sacrifice efficiency over human rights, democracy and the rule of law.

19.4.3 *Delegating Responsibility*

Despite the push of the NPM movement to reconceptualize public administrations as "service providers" toward "customers," citizens are more than just customers. A far more inherent power imbalance is at play between governments and individuals as, unlike in private settings, the latter cannot easily "shop" at another service provider when for example, their social welfare benefits are wrongfully denied. As Sofia

[52] See in this regard also *infra*, Sections 19.4.3 and 19.4.4.

[53] For an extensive overview, see Smuha n (5).

[54] Nathalie A. Smuha, *Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law* (Cambridge University Press, 2025).

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

Ranchordas and Luisa Scarcella pointed out, this power asymmetry can also exacerbate citizens vulnerabilities, and even instigate dehumanizing effects.[55] This risk can be spurred by the datafication process that accompanies the use of algorithmic regulation,[56] as it inevitably reduces individuals to numbers in a quite literal sense, thus diminishing their individuality and potentially even their human dignity. Yet it is far easier to overlook one's responsibility for the well-being of a number than for the well-being of an individual human being.

One of the distinctive elements of algorithmic regulation concerns the elimination of the need for direct personal interactions between individuals and civil servants, as such interactions can instead be mediated through algorithmic systems. At the same time, this time-saving feature can also make it more difficult for citizens to interact with another human being that understands their needs and concerns, and that can rectify any erroneous information that public administrations may have (which is a common difficulty with networked databases).[57] It can also render it more challenging for individuals to receive a clear explanation of the decisions affecting them, or to voice their concerns when problematic administrative acts are taken about them. In other words: it might be far more difficult for them to be heard, and to be acknowledged in their human individuality.[58]

In this regard, it is also important to consider the role of discretion, "*a power which leaves an administrative authority some degree of latitude as regards the decision to be taken, enabling it to choose from among several legally admissible decisions the one which it finds to be the most appropriate.*"[59] Civil servants use this discretion when they decide how to apply general rules to specific cases in the most appropriate way, in line with the rule of law. However, when public administrations rely on algorithmic regulation, this typically reduces discretion at the level of individual officials. Instead of officials exercising their judgment in specific cases, it is the *system* that will "apply" the law to a given case and take or suggest a decision.[60] Even

[55] Sofia Ranchordás and Luisa Scarcella, "Automated government for vulnerable citizens: intermediating rights" (2021) *William & Mary Bill of Rights Journal*, 30(2): 371–418.

[56] See also Heather Broomfield and Lisa Reutter, "In search of the citizen in the datafication of public administration" (2022) *Big Data & Society* 9(1): 3.

[57] As thoroughly explored by Marlies van Eck in her dissertation, this can be especially problematic when erroneous data from one administration is used to inform the decision of another administration – see *Geautomatiseerde ketenbesluiten & rechtsbescherming: Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*, Tilburg Law School, 2021, https://pure.uvt.nl/ws/portalfiles/portal/20399771/Van_Eck_Geautomatiseerde_ketenbesluiten.pdf.

[58] See in this regard also Nathalie A. Smuha, 'The Human Condition in An Algorithmized World: A Critique through the Lens of twentieth-Century Jewish Thinkers and the Concepts of Rationality, Alterity and History', KU Leuven Institute of Philosophy, *SSRN*, 2021, http://dx.doi.org/10.2139/ssrn.4093683.

[59] See Committee of Ministers of the Council of Europe, "Recommendation No. R (80) 2 of the Committee of Ministers Concerning the Exercise of Discretionary Powers by Administrative Authorities," Strasbourg, 1980.

[60] See also Justin B Bullock, "Artificial intelligence, discretion, and bureaucracy" (2019) *The American Review of Public Administration* 49(7): 751–761; David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey, and Mariano-Florentino Cuéllar. "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies" *Administrative Conference of the United States*, 2020,

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

when the system merely offers a suggestion, officials will often be strongly incentivized to follow it for reasons of efficiency and the system's perceived authority. Indeed, if they would want to deviate from the system's suggestion, they typically need to provide a justification for this deviation, which not only requires time but also space for critical judgment to go against the system's centralized and allegedly more commanding suggestion.[61]

Civil servants might also feel that, by relying on the system's outcomes, they can delegate or at least share responsibility for the decision they take.[62] Especially when they do not see or talk with the individual concerned, the distance often renders it easier and more convenient to delegate a decision to an algorithmic system, though that could also lead to an (at least psychological) delegation of responsibility for that decision, and thus for the potential adverse consequences in case it is wrong or unjust. This can, in turn, increase the likelihood of negligence, nurture a lack of concern for citizens' interests and how they are impacted, and more generally diminish the procedural legitimacy of decisions taken by public administrations. Prior to the implementation of algorithmic regulation, it is hence important to anticipate and mitigate this challenge.

19.4.4 *Delegating Public Power*

At the same time, it must be pointed out that administrative discretion does not disappear when algorithmic regulation is deployed. While it is significantly reduced at the level of individual civil servants, it is instead transferred to the level of the designers and developers of the algorithmic systems, who through their seemingly technical choices in fact shape the system's highly normative outcomes.[63] A related problem is the fact that these designers and developers are typically *not* the civil servants who have the necessary experience and training to adopt administrative acts, who have expertise on how a specific law should be applied, and who must abide by the public sector's deontological standards. Rather, these algorithmic systems are often developed by data scientists and engineers working for private companies. This

[61] For a more nuanced perspective of an empirical study aiming to mimic automated decision-making in bureaucratic context, see Saar Alon-Barkat and Madalina Busuioc, "Human–AI Interactions in Public Sector Decision Making: 'Automation Bias' and 'Selective Adherence' to Algorithmic Advice" (2023) *Journal of Public Administration Research and Theory* 33(1), 153–169. See however also Albert Meijer, Lukas Lorenz, Martijn Wessels, "Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems" (2021) *Public Administration Review*, 81(5): 837–846.

[62] See in this regard Albert Meijer, Lukas Lorenz, Martijn Wessels, n (56), See also Matthew M. Young, Justin B. Bullock, and Jesse D. Lecy, "Artificial discretion as a tool of governance: A framework for understanding the impact of artificial intelligence on public administration" (2019) *Perspectives on Public Management and Governance*, 2(4): 301–313.

[63] See in this regard Smuha n (5), 211–212. See also Reuben Binns, "Human judgment in algorithmic loops: Individual justice and automated decision-making" (2022) *Regulation & Governance*, 16: 197.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

raises questions about the influence of the private sector on public decision-making, given the normative relevance of the systems they develop for this purpose. The less a public administration can count on in-house infrastructure and knowledge about how algorithmic systems work and what their capabilities and limitations are, the more this can lead to a problematic dependency on actors that are driven by non-public values.[64] The use of algorithmic regulation should however never lead to the unwarranted delegation of public powers to private actors.

The COVID-19 pandemic, for instance, made many public administrations aware of the fact that they were utterly dependent on private actors to set up and use digital infrastructures for their day-to-day operations (many of which had to move entirely to the digital realm) and for their management of the pandemic itself (for instance through contact tracing apps).[65] This also contributed to concerns around "digital sovereignty," or a nation's ability to autonomously decide on its relationship with (providers of) digital technology.[66] As discussed elsewhere, digital sovereignty implies the exercise of control over two entwined elements, namely: (1) the normative values that underly the technology, and (2) the physical and socio-technical digital infrastructure that enables the technology.[67] Sovereignty over both of these elements is essential to ensure that the core values which public administrations ought to protect – including human rights, democracy and the rule of law – are safeguarded also when they deploy algorithmic regulation.

19.5 GOVERNING ALGORITHMIC REGULATION

This brings me to the penultimate section of this chapter: how is algorithmic regulation governed to ensure that these challenges are tackled and that the necessary safeguards are in place? Let me start by jettisoning the misconception that no regulation currently applies to the use of these new technologies. Over the centuries, a rich body of law was developed to oblige public administrations and civil servants to act in line with a set of rules that limit their power, thus seeking to rebalance the inherent power asymmetry between governments and individuals. These rules did not seize applying once public administrations started relying on algorithmic regulation. Rather, they offer protection independently of how governments take administrative decisions, and thus play an important role in digital contexts too.

[64] See in this regard also Linnet Taylor, "Public actors without public values: Legitimacy, domination and the regulation of the technology sector" (2021) *Philosophy & Technology*, 34: 897–922.

[65] See for example, Luciano Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU" (2020) *Philosophy & Technology* 33: 369–378.

[66] See also Julia Pohle and Thorsten Thiel, "Digital sovereignty" (2020) *Internet Policy Review*, 9; Benjamin Cedric Larsen, "The Geopolitics of AI and the Rise of Digital Sovereignty," *Brookings*, December 8, 2022, www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.

[67] Nathalie A. Smuha, "*Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective*" (SSRN 2023), http://dx.doi.org/10.2139/ssrn.4501591.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

19.5.1 *Constitutional Law and Administrative Law*

The most primary of these rules are enshrined in national constitutions and set out the competences that governments have when exercising their powers, as well as the limitations of such powers. Fundamental rights and freedoms – such as the right to equality and nondiscrimination, freedom of speech and association, the right to privacy, and the right to a fair trial – are typically part of constitution-level norms, either directly or through (international) human rights treaties. This enables (constitutional) courts to review public administrations' actions in light of these limitations and safeguards. To carry out judicial review, it should not matter whether the administration's actions were taken solely by human civil servants or with the help of algorithmic systems.

A more detailed set of rules can be found in the realm of administrative law. While this area of law emerged as a scientific study in Europe around the nineteenth century, as a body of law its was already established prior to that time in several countries.[68] In essence, administrative law sets out the contours of the space of action of public administrations, drawing on constitutional norms and principles. It can thus be seen as limiting but also legitimizing and empowering administrations and the discretion they exercise when implementing the rules established by the legislative branch of power.[69] While each country has its own administrative law rules, some commonalities can be identified, as these rules are closely associated with the rule of law principles mentioned earlier.[70] They have sometimes also been conceptualized under the concept of "good governance" or "good administration."[71] In what follows, let me discuss some of the principles that the Council of Europe's Committee of Ministers laid down in its "Code of Good Administration" ("the Code").[72]

The first concerns the *principle of lawfulness*, which broadly corresponds to the concept of "legality."[73] It states that public authorities must act in accordance with the law (including domestic, supranational and international law), and cannot take any arbitrary measures, also when exercising discretion. This means they must have a legal basis to act, in accordance with the rules that define their powers and

[68] See Giacinto della Cananea, *The Common Core of European Administrative Laws* (Brill Nijhoff, 2023), 2.

[69] Christine B. Harrington and Lief H. Carter, *Administrative Law and Politics: Cases and Comments* (Sage, 2014), 25.

[70] See Section 19.4.2 above.

[71] See, for instance, Henk Addink, *Good Governance: Concept and Context* (Oxford University Press, 2019).

[72] The Code was an appendix to Recommendation CM/Rec(2007)7 of the Council of Europe's Committee of Ministers to member states on good administration, adopted by the Committee of Ministers on June 20, 2007 at the 999bis meeting of the Ministers' Deputies.

[73] Article 2 of the Code. See also Franz Merli, "Principle of Legality and the Hierarchy of Norms," in Werner Schroeder (ed), *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation* (Oxford: Hart Publishing, 2016), 37–45.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

procedures, and they can only use the powers conferred upon them for the purpose delimited in those rules. The interpretation of how this principle must be complied with in practice differs from state to state, but given the intrusiveness of algorithmic systems, many countries in Europe provide that outsourcing certain tasks to such systems requires a specific legal basis. Accordingly, the legislative branch will typically need to set out the conditions under which public administrations can rely on algorithmic regulation. Additionally, public administrations have the obligations to ensure that – when they deploy algorithmic regulation – this occurs in full compliance with existing legislation, including the protection of human rights.

The *principle of equality* is likewise mentioned in the Code and provides that public administrations must treat persons who are in the same situation in the same way.[74] Any difference in treatment must be objectively justified – and merely claiming that an algorithmic system makes unintended discriminatory distinctions would not be a sufficient justification. Linked thereto is the *principle of impartiality*, which the Code conceptualizes as ensuring that public administrations act objectively, having regard only to "relevant matters" when they adopt administrative acts, and that they should not act in a "biased manner."[75] Individual public officials, too, must carry out their duties in an impartial manner, irrespective of their personal beliefs and interests. Applied to the context of algorithmic regulation, these principles hence require public administrations to ensure preemptively that the tools they deploy do not provide biased outcomes, and do not take into account elements that are not relevant for the administrative act in question. The latter point is especially interesting, since data-driven systems typically function by correlating different information points that may not necessarily have a causal link with the matter at hand. Importantly, respect for these principles must also be ensured when administrations *procure* algorithmic applications; they cannot escape this obligation by outsourcing the system's development, but remain responsible to respect these principles also when they make use of (privately developed) systems.[76] Public administrations must hence exercise a certain standard of care before they take specific actions, which arguably also extends to the action of implementing algorithmic regulation.

The Code's *principle of proportionality* is also of relevance: measures affecting the rights or interests of individuals should only be taken where necessary "*and to the extent required to achieve the aim pursued.*"[77] This principle is particularly

[74] See Article 3 of the Code.

[75] See Article 4 of the Code.

[76] The *principle of due diligence*, acknowledged in many administrative law systems, plays an important role in this regard too. Under Belgian law, public administrations must for instance abide by the due diligence principle pursuant to the (binding) "general principles of good administration." See for example, Kaat Leus, "Het Zorgvuldigheidsbeginsel" in Ingrid Opdebeek and Marnix Vandamme (eds), *Beginselen van Behoorlijk Bestuur* (Die Keure, 2006).

[77] See Article 5 of the Code.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

important whenever civil servants exercise discretion, as it also states they must maintain "*a proper balance between any adverse effects which their decision has on the rights or interests of private persons and the purpose they pursue*," without these measures being excessive.[78] Given the problematic examples of algorithmic regulation discussed earlier, the proportionality principle plays an important role in the algorithmic context, especially when discretion is shifted away from individual civil servants who are able to balance different rights and interests, toward (designers of) algorithmic systems that rely primarily on pre-codified rules or optimization functions.

The Code also includes the *principle of participation*, which emerged more recently.[79] This principle is closely connected to the notion of (deliberative) democracy and embodies the idea that public administrations should offer individuals the opportunity to participate in the preparation and implementation of administrative decisions which affect their rights or interests. As I argued elsewhere, one could claim that participation should not only extend to administrations' decision-making processes based on algorithmic regulation, but also to the very choice taken by public administrations to implement algorithmic regulation in the first place.[80]

Finally, I should point out the *principle of transparency*, which states that public administrations must ensure that individuals are informed, by appropriate means, of their actions and decisions.[81] This may also include the publication of official documents and should in any case encompass respect for the rights of access to official documents according to the rules relating to personal data protection. A debate exists about the extent to which this principle applies to algorithmic systems used by public administrations, in so far as the source code of these algorithms (or at least their parameters) can be said to constitute information that falls under such access rights.[82]

This brings me to the observation that existing administrative law rules undoubtedly apply when public administrations use algorithmic systems, yet the enforcement of such rules is often rendered more difficult in this context precisely due to the nature and features of such systems, and civil servants' unfamiliarity with the particular challenges they pose. Partly for this reason, more specific legal rules have been developed to protect individuals when their personal data is processed in an automated way, and when they are subjected to AI systems – two domains I will discuss next.

[78] Ibid.
[79] See Article 8 of the Code.
[80] See also Smuha, n (5), 228.
[81] See Article 10 of the Code.
[82] See, for example, Henrik Palmer Olsen, Thomas Troels Hildebrandt, Cornelius Wiesener, Matthias Smed Larsen, and Asbjørn William Ammitzbøll Flügge, "The right to transparency in public governance: Freedom of information and the use of artificial intelligence by public agencies," *Digital Government: Research and Practice*, 5(1): 2024, 1–15.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

19.5.2 *Data Protection Law*

In the EU legal order, the right to privacy and personal data protection is enshrined respectively in Articles 7 and 8 of the Charter of Fundamental Rights of the EU (CFR) and in Article 8 of the European Convention on Human Rights. These fundamental rights were further concretized in other legal instruments. At the level of the Council of Europe, Convention 108 for the protection of individuals with regard to the processing of personal data was already opened for signatures in 1981, being the first legally binding international instrument in the field of data protection (later modernized through Convention 108+ in 2018).[83] Unsurprisingly, the Council of Europe's 2007 Code of Good Administration also included the *principle of respect for privacy*.[84] At the level of the European Union, the most well-known legal instrument in this field is the General Data Protection Regulation or GDPR,[85] which was largely inspired by Convention 108 and on which I will focus in what follows in a very succinct way, as it establishes directly invokable rights and obligations in EU Member States.[86]

The GDPR imposes obligations on private and public entities alike, and hence also applies to all personal data processing activities of public administrations (though a separate regime exists for the processing of data by law enforcement authorities in the context of criminal investigations).[87] Its protective provisions are especially relevant in the context of algorithmic regulation, which almost by definition implies the *processing* of *personal data*.[88] Public administrations must, pursuant

[83] This Convention was ratified by fifty-five states, including also non-member States of the Council of Europe.

[84] See Article 9 of the Code of Good Administration.

[85] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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, OJ L 119, 4.5.2016*, 1–88.

[86] The GDPR is a revision of an earlier EU directive dating from 1995, which already contained several safeguards against the processing of individuals' personal data. See Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281, 23.11.1995*, 31–50.

[87] This is known as the Law Enforcement Directive or LDR. See Directive 2016/680 of the European Parliament and of the Council of April 27, 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 offenses 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, 89–131.

[88] Article 4(1) of the GDPR defines personal data as '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'. Processing is also broadly defined (in Article 4(2)), as '*any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means*' (which, to illustrate, can include the collection, recording,

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

to Article 6 of the GDPR, be able to justify each data processing activity through a legal basis that confers them such power, whether this be the data subject's consent, the protection of the vital interests of a person, or the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.[89] In case a public administration seeks to rely on the latter ground, the legal basis must be laid down further in Union law or in domestic law which sets out the processing's purpose, meets an objective of public interest and is proportionate to the legitimate aim pursued.[90]

The GDPR also mandates that administrations processing personal data do so in line with several principles, including the need to process data in a lawful, fair and transparent manner; to ensure it is collected only for specified, explicit and legitimate purposes, in a way that is adequate, relevant and limited to what is necessary in relation to such purposes; to ensure the data is accurate, kept up to date, and not stored for longer than necessary; and to ensure the data is processed with appropriate security measures, including protection against unlawful processing, accidental loss or damage.[91] Finally, administrations are not only responsible to make sure these principles are respected, but they must also be able to *demonstrate* compliance with them to foster accountability.[92]

In addition to these obligations, data subjects also have certain rights regarding their personal data, including the right to information about which data is being processed and in what way, as well as the right to rectify or erase such data.[93] Moreover, at any time, Article 21 of the GDPR grants data subjects a right to object to the automated processing of their personal data based on "*the performance of a task carried out in the public interest or in the exercise of official authority*" on grounds relating to their particular situation. Administrations must demonstrate compelling legitimate grounds for the data processing which override the interests, rights and freedoms of the data subject (or for the establishment, exercise or defense of legal claims). Pursuant to Article 22 of the GDPR, data subjects also have a right not to be subject to a decision based solely on automated processing if it produces legal effects concerning them or similarly significantly affects them – which comes down to a general prohibition on such decision-making, subject to the exceptions listed in the article.[94]

organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data). See in this regard also Chapter 7 of this Book.

[89] Article 6 GDPR also refers to a number of other potential legal bases, yet public administrations would need to be able to provide a justification for their applicability.

[90] See Article 6(3) GDPR.

[91] See Article 5(1) GDPR.

[92] See Article 5(2) GDPR.

[93] See in particular Articles 12 to 22 GDPR.

[94] See Article 22 GDPR.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

The question of how much human intervention is needed to disqualify as "solely" automated processing is still not satisfactorily answered, though the European Data Protection Board (formerly the "Article 29 Data Protection Working Party")[95] issued interpretative guidelines in this respect.[96] The Guidelines for instance clarify that this provision cannot be avoided "*by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing.*"[97] Indeed, to qualify as human involvement, the public administration should ensure that "*any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.*"[98] Of course, to meaningfully exercise their right to object to automated decision-making, individuals must first be made aware of the fact that a public administration is taking an automated decision which concerns them (though administrations would have an information obligation in this respect under the GDPR).[99]

19.5.3 *AI Law*

While data protection law provides important safeguards to counter the risks of algorithmic regulation,[100] the GDPR's entry into force also revealed that many legal gaps still remain. From 2020 onwards, these gaps were also more explicitly recognized by policymakers in Europe,[101] such as the Council of Europe's Ad Hoc Committee

[95] This organization was set up under Article 29 of Directive 95/46/EC, the predecessor of the GDPR, and is now called the European Data Protection Board. It is an independent European advisory body on data protection and privacy.

[96] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,' October 3, 2017 (revised and adopted on February 6, 2018), WP251rev.01. See in this regard also Lorenzo Gugliotta, "Towards a right to explanation for automated (and AI-based) decisions? Anticipating the upcoming judgment in C-634/21 OQ v SCHUFA," *The Law, Ethics and Policy of AI Blog*, November 28, 2023, www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/SCHUFA-right-to-explanation.

[97] Article 29 Working Party, n (99), 21.

[98] Ibid.

[99] See in this regard chapter 3 of the GDPR, which sets out the rights of data subjects, and particularly articles 13(2)(f) and 14(2)(f).

[100] For a discussion of the interaction between the data protection framework and the AI Act, and the remaining importance of the former, see also Nathalie A. Smuha, "The paramountcy of data protection law in the age of AI (Acts)," *Two decades of personal data protectin. What's next? EDPS 20th Anniversary*, Luxembourg: Publications Office of the European Union, 2024.

[101] Also in other parts of the world, legislators started considering the adoption of new legislation to counter AI's risks. Consider, in this regard, Canada's proposed Artificial Intelligence and Data Act (tabled in June 2022), the US' Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI (issued in October 2023), and China's regulation of inter alia recommendation algorithms and generative AI systems (adopted in March 2022 and May 2023, respectively).

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

on AI (in its Feasibility Study on a legal framework on AI),[102] and the European Commission (in its White Paper on Artificial Intelligence[103] and the work of its High-Level Expert Group on Artificial Intelligence[104]). The realization that existing legal rules were insufficient to protect people's rights against AI's risks, and that the promulgation of nonbinding AI ethics guidelines did not provide a satisfactory solution either, prompted new legislative initiatives. At the level of the Council of Europe, in Spring 2022, negotiations were launched to adopt a new international "Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law," finalized in Spring 2024.[105] At the level of the EU, the Commission proposed a new regulation laying down harmonized rules on AI in Spring 2021 – referred to as "the AI Act" – which after lengthy negotiations was adopted by the European Parliament and the Council in Spring 2024 as well.[106] Since the former is very succinct and abstract, and still needs to be converted into national legislation by the States who wish to sign it, I will briefly focus on the latter.

As discussed more extensively in Chapter 12 of this book, the AI Act establishes mandatory requirements for AI systems that pose risks to people's "health, safety and fundamental rights" and introduces prohibitions for several AI practices that are deemed incompatible with EU values.[107] Being a regulation rather than a directive, the AI Act has binding legal force in every EU Member State without the need for any national transposition rules. Yet a first question to ask is whether algorithmic regulation by public administration falls under the scope of the AI Act. Rather

[102] See Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), "Feasibility Study," Council of Europe, CAHAI(2020)23, https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da, 21–25. This formed the basis of the subsequent negotiations by the CAHAI's successor (the CAI or Committee on AI) for a new Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.

[103] European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, Brussels, February 19, 2020.

[104] Before proposing the AI Act, the European Commission set up a High-Level Expert Group on AI with the task of drafting '*Ethics Guidelines for Trustworthy AI*' (published in April 2019), which later inspired the Act's proposal. The non-binding nature of this initiative was however criticized, and also the Expert Group itself noted in its '*Policy Recommendations for Trustworthy AI*' (published in June 2019) that binding rules were needed for AI systems that can adversely affect fundamental rights. See in this regard also Nathalie A. Smuha, "The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence: A continuous journey towards an appropriate governance framework for AI," *Computer Law Review International* 4 (2019), 97–106.

[105] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law [Vilnius, 5.IX.2024], https://rm.coe.int/1680afae3c.

[106] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[107] Since the AI Act is extensively discussed in Chapter 12 of this book, the discussion in this section focuses primarily on its applicability in the context of public administrations. See Nathalie A. Smuha and Karen Yeung, "The European Union's AI Act: Beyond Motherhood and Apple Pie?" in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

than focusing on algorithmic systems, the AI Act applies to "AI," which it defines as a "*machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*."[108] In the recitals, the EU legislator made it clear that this does not encompass "simpler traditional software systems or programming approaches" or "systems that are based on the rules defined solely by natural persons to automatically execute operations." This means that some applications of algorithmic regulation might not be captured by the AI Act, despite their potentially harmful consequences, merely because they are considered too "traditional" – which would be an unfortunate gap.[109] That said, public administrations are increasingly jumping on the machine learning hype (often without a proper assessment of whether this is also more useful for the purpose they envisage), so it can be expected that ever more applications of algorithmic regulation will fall under the AI Act's scope.

It is, however, not enough to merely fall under the scope of the regulation to also be subjected to its restrictive provisions. Taking a risk-based approach, the AI Act sets out five categories: (1) prohibited systems; (2) high-risk systems; (3) general purpose AI models; (4) systems requiring transparency measures; and (5) low-risk systems. The most relevant categories for the purpose of this chapter are the first two, since they pertain most frequently to the public sector.

The first category contains a list of several AI practices that are considered to pose an unacceptable level of risk to fundamental rights, and that are hence prohibited. For instance, AI systems cannot be used to deduce or infer people's race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation based on their biometric data (so-called biometric categorization).[110] Public and private organizations are also banned from engaging in social scoring of individuals or groups based on their social behavior or based on known, inferred or predicted personality characteristics, if this scoring leads to their unfavorable treatment in unrelated contexts, or to a disproportionate detrimental treatment.[111] Fully automated risk assessments of natural persons to predict the risk they commit a

[108] See Article 3(1) of the AI Act.

[109] See Recital 12 of the AI Act, which focuses particularly on the capability of making "inferences." According to this recital, the relevant techniques that enable this include machine learning approaches that learn from data how to achieve certain objectives; and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. Yet the capacity of an AI system to infer goes "beyond basic data processing, enable learning, reasoning or modeling." It remains to be seen how a distinction will be drawn between "basic" modeling and more advanced applications.

[110] See Article 5(1)(g) of the AI Act. An exception is foreseen for the labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement, which does not fall under this prohibition.

[111] See Article 5(1)(c) of the AI Act.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

criminal offence based solely on their profiling is also prohibited,[112] as is law enforcement's use of real time facial recognition in public places, unless one of three exceptions apply and safeguards are foreseen.[113]

The second category encompasses AI systems that are considered to pose a high risk to the health, safety and fundamental rights of individuals. Either they are already covered by existing product safety legislation (listed in Annex I) or they fall under the list of stand-alone high-risk systems (listed in Annex III). Many algorithmic regulation applications used by public administrations (to the extent they fall under the regulation's "AI" definition) are included in Annex III, such as the use of AI systems to "*evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services.*"[114] Annex III also lists several applications used by law enforcement and by migration and border control administrations, including the use of AI to assist in asylum application decisions, to profile individuals in the detection of criminal offenses, or to serve as a polygraph.

Before being put into service, high-risk systems must undergo a conformity assessment to ensure they respect the requirements listed in Articles 9–15 of the AI Act, taking into account the systems' "*intended purpose*" and the "*generally acknowledged state of the art on AI.*"[115] That said, for virtually all high-risk AI systems public administrations can carry out this assessment themselves,[116] meaning there is no prior licensing or approval scheme before these systems are used.[117] Concretely, high-risk systems must be subjected to a risk-management process ("*understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system*") that allows the identification of reasonably foreseeable risks the system can pose to "*health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose*," on the basis of which "*appropriate and targeted risk management measures*" must be taken.[118] High-risk systems are

[112] See Article 5(1)(d) of the AI Act.

[113] See Article 5(1)(h) of the AI Act These exceptions pertain to the search for victims of a crime, the prevention of an imminent threat to the life or safety of individuals, and the localization or suspects of specific crimes.

[114] Annex III, point 5(a) of the AI Act.

[115] Article 8(1) of the AI Act.

[116] The only exception to this self-assessment are high-risk AI systems listed under point 1 of Annex III (biometrics), for which the conformity assessment must be undertaken by a notified authority. The systems currently falling under this exception are: (a) remote biometric identification systems (unless it concerns biometric verification the sole purpose of which is to confirm that a natural person is who they claim to be); (b) AI systems used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics; and (c) AI systems used for emotion recognition.

[117] They can also rely on technical specifications and standards which are being developed to facilitate compliance with the requirements (see Article 40 and following of the AI Act). Compliance with harmonized standards offers a presumption of conformity with the high-risk requirements.

[118] Article 9 of the AI Act.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

also subject to data governance obligations for the training, validation and testing of systems, which include considerations regarding the relevant design choices of the model, the formulation of assumptions with respect to the information the data are supposed to represent, an assessment of the data availability and suitability and potential gaps, as well as the examination and mitigation of possible biases.[119]

Besides obligations that pertain to their accuracy, robustness and cybersecurity,[120] high-risk systems must also technically allow for the automatic recording of events for recordkeeping purposes[121] and set up a technical documentation of their compliance with those requirements, which national supervisory authorities can inspect if need be.[122] They must additionally be designed in a way that enables them to be overseen by natural persons. Such human oversight is meant to act as a supplementary safeguard to prevent or minimize risks (all the while taking into account the risk of so-called automation bias)[123] and to enable the system's user to decide *not* to use the system or to reverse its output.[124] In the context of public administrations, civil servants should hence always have the possibility to deviate from the system's suggested decision – though, as discussed earlier, this not only depends on a legal provision, but also requires an organizational environment that enables them to do so in practice.

As to the systems' transparency, providers of high-risk systems must present deployers of their systems with the necessary information to "*interpret the system's output and use it appropriately*."[125] This means that civil servants who procure AI systems should in principle receive information about the system's "*characteristics, capabilities and limitations of performance*."[126] Note, however, that this information need not be shared with those who are subjected to (and potentially negatively affected by) the system, but only to the system's users. The only information about high-risk systems that must be made publicly available is enumerated in Annex VIII of the AI Act and must be registered in the new "EU database for high-risk systems listed in Annex III," which the European Commission must set up as per Article 71 of the AI Act. The most useful information that AI providers must register is "*a description of the intended purpose of the AI system and of the components and functions supported through this AI system*," as well as "*a basic and concise description of the information used by the system (data, inputs) and its operating logic*." Whenever a high-risk system is used by a public sector deployer, the system's use must also be registered in the database, including a summary of "*the findings of the fundamental rights impact*

[119] Article 10 of the AI Act.
[120] Article 15 of the AI Act.
[121] Article 12 of the AI Act.
[122] Article 11 of the AI Act.
[123] See, for example, Linda J. Skitka, Kathleen Mosier, and Mark D. Burdick, "Accountability and automation bias," *International Journal of Human-Computer Studies*, 52(4), 2000, 701–717.
[124] Article 14 of the AI Act.
[125] Article 13 of the AI Act.
[126] Article 13(3)(b) of the AI Act.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

assessment" which such deployers must conduct pursuant to Article 27 of the AI Act, and a summary of the data protection impact assessment they must carry out pursuant to Article 35 of the GDPR or Article 27 LED. The new EU database might hence become a valuable source for individuals seeking more information about public administrations' use of algorithmic regulation, especially with a view of challenging it in case there are concerns about breaches of their rights.

At the same time, there are many shortcomings in the protection the AI Act intends to afford, which are discussed in more detail in Chapter 12 of this book.[127] Particularly in the context of algorithmic regulation, many concerns remain unaddressed. The AI Act barely mentions the rule of law and has nothing to say about the normative influence that private actors can have on the public sphere through the procurement of algorithmic regulation tools. It also does not ensure that citizens get a say about whether certain algorithmic regulation applications should be used by public administrations in the first place, and its overly restrictive scope means it does not cover many harmful applications of algorithmic regulation, especially when based on more traditional systems. The AI Act also has many carve-outs which undermine its protection: AI systems deployed for research or for national security fall outside its scope, which risks constituting a significant gap. In addition, the safeguards against the use of live facial recognition (or biometric identification more generally) in public places only apply in the context of law enforcement and do not include borders, which leaves migrants – who already find themselves in a very vulnerable position – even more vulnerable.[128]

One could also argue that, by virtue of AI Act, the use of certain problematic applications is actually legitimized, since they can now be rubberstamped by claiming conformity with the AI Act's rules. This also led some people to criticize the AI Act an instrument of "deregulation," by potentially undermining safeguards drawn from other legal domains.[129] Finally, the AI Act's list-based approach – which exhaustively lists the systems that fall within its different categories – also means that some important applications are not covered, as the lists are underinclusive.[130] Combined with the fact that providers of high-risk systems can largely self-assess their system's

[127] See Chapter 12 of this Book: Nathalie A. Smuha and Karen Yeung, "The European Union's AI Act: beyond motherhood and apple pie?" in Nathalie A. Smuha (ed.), *The Cambridge Handbook on the Law, Ethics and Policy of AI* (Cambridge University Press, 2025).

[128] See also Petra Molnar, "EU's AI Act Falls Short on Protecting Rights at Borders," *Just Security*, December 20, 2023, www.justsecurity.org/90763/eus-ai-act-falls-short-on-protecting-rights-at-borders/.

[129] See for example, Aída Ponce Del Castillo, "The AI Act: Deregulation in Disguise," *Social Europe*, December 11, 2023, www.socialeurope.eu/the-ai-act-deregulation-in-disguise. See also Michael Veale and Frederik Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach," *Computer Law Review International*, 22(4), 2021, 97–112.

[130] The Annexes of the AI Act can however be updated over time through the procedures laid down therein. As regards the high-risk systems listed in Annex III, Article 7 for instance sets out the conditions under which the European Commission can adopt a delegated act to add, modify, or eliminate AI applications from the list.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

conformity with the requirements, and the fact that they can even self-assess whether their system is truly high-risk,[131] the regulation leaves a lot of leeway to the very actors against which it allegedly seeks to protect individuals.[132]

That said, the AI Act does provide a number of new safeguards that can be invoked to counter some risks posed by public administrations' use of AI. Moreover, the fact that it establishes a novel public enforcement mechanism both at the national and the European level also provides a strong signal that the EU takes AI's challenges seriously. The AI Act should hence be seen as part of a broader legal framework that also includes other protective provisions, and that is complementary to the legal domains set out above. Its relationship with existing legislation is also clarified in the AI Act itself, which for instance states that it "*does not seek to affect the application of existing Union law governing the processing of personal data*,"[133] and that "*where an AI practice infringes other Union law*" it can still be prohibited regardless of its inclusion in the exhaustive list of prohibitions of Article 5.[134] Accordingly, one should look beyond the AI Act's provisions to hold public administrations to account when they choose to rely on algorithmic regulation. Rather, the AI Act should be invoked along with provisions of constitutional law, administrative law and data protection law (as well as other relevant legal domains) to provide stronger protection against the challenges discussed in this chapter.

19.6 CONCLUSIONS

Algorithmic regulation has found its way to virtually all areas of the public sector. While the level of its uptake strongly varies from one country to another, and from one administration to another, it is being used for ever more impactful decisions – a trend that will undoubtedly continue. In the previous sections, along with setting out the reasons for this uptake, I also discussed some of the challenges that public administrations must consider when fully or partly delegating their tasks – and especially administrative acts – to algorithmic systems.

Drawing on existing practices from France, the UK, the Netherlands and the US, I showed that algorithmic regulation can raise legitimate concerns around the risk of biased decision-making, unwarranted privacy intrusions, and errors that can lead

[131] See Article 6(3) of the AI Act, which states that "*an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*." Accordingly, even if an AI system is specifically listed in the Annex of high-risk systems, the requirements attached thereto can still be avoided if the system's provider believes it does not pose a significant risk of harm. In that case, the provider must however still register the system, and be ready to provide a justification for the exclusion.

[132] See Chapter 12 of this Book, n (132). See also Smuha n (5), 291.

[133] Recital 10 of the AI Act.

[134] Article 5(8) of the AI Act. One could however question what such "other Union law" refers to, given that the AI Act supposedly already includes protective provisions for health, safety and fundamental rights.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023

to wide-scaled harm given the essential role that public administrations fulfil in society. Whether through traditional techniques or advanced machine learning applications, the automated execution and implementation of laws and policies implies a transformation from natural language to code, which has normative implications that can also affect the rule of law. As the earlier illustrations have shown, these risks also exist in countries that are committed to protect human rights, democracy and the rule of law, which makes it even more important for them to ensure they maintain sovereignty over the way in which (algorithmically driven) public decision-making occurs. Furthermore, we must stay vigilant that the delegation of administrative decision-making to algorithmic systems does not simultaneously lead to a delegation of responsibility and a neglect of citizens' rights and interests, in the name of efficiency.

Public administrations are already bound by an array of legal norms that can contribute to countering those risks, including safeguards from constitutional law, administrative law, data protection law, or AI-specific law. Yet even when invoked in a strategic and complementary way, these legal protection mechanisms will never be perfect. And while it is sensible to strive for their improvement and to develop further guidance for practitioners on how existing legal norms should be applied to the algorithmic context, one should also be careful not to treat the law as a panacea for all the challenges raised by technology. Beyond legal compliance, it is essential that public administrations also invest in education and literacy efforts among their civil servants, that they provide them with the necessary conditions to exercise their critical judgment, and that they prevent the delegation of public power – especially when this happens without democratic deliberation and accountability. It is only by taking these considerations seriously and adopting adequate measures prior to the implementation of algorithmic regulation that public administrations can continue fulfilling their vital role in liberal democracies with the help of algorithmic systems.

Downloaded from https://www.cambridge.org/core. IP address: 3.22.70.102, on 28 Apr 2025 at 13:29:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009367783.023