

1

Introduction

1.1 ALIGNING ALGORITHMIC REGULATION AND THE RULE OF LAW

1.1.1 *The Algorithmic Leviathan*

... why may we not say, that all Automata (Engines that move themselves by springs and wheelles as doth a watch) have an artificiall life? For what is the Heart, but a Spring; and the Nerves, but so many Strings; and the Joynts, but so many Wheelles, giving motion to the whole Body, such as was intended by the Artificer? Art goes yet further, imitating that Rationall and most excellent worke of Nature, Man. For by Art is created that great LEVIATHAN called a COMMON-WEALTH, or STATE, (in latine CIVITAS) which is but an Artificiall Man; though of greater stature and strength than the Naturall, for whose protection and defence it was intended;

Thomas Hobbes, Leviathan, 1651¹

In the seventeenth century, Thomas Hobbes famously argued in favour of a strong, undivided and absolute sovereign – poetically captured by a reference to the biblical Leviathan² – who would safeguard society against a war of all against all.³ Through the establishment of a social contract, citizens would agree to give up certain freedoms in exchange for the peace and security that the powerful sovereign would

¹ Thomas Hobbes, *Leviathan: Or the Matter, Forme and Power of a Commonwealth, Ecclesiasticall and Civil* (1651) (Project Gutenberg 2002) <www.gutenberg.org/files/3207/3207-h/3207-h.htm>, introduction.

² In Jewish theology, Leviathan is a powerful mastodontic creature, sometimes represented as a sea serpent or whale-like monster, mentioned inter alia in the Book of Job. Scholars have debated its meaning, yet it is often seen as “symbolizing God’s power and sovereignty over against Job’s impotence because he cannot restrain or catch them. Thus, Job has no right to challenge God concerning his justice in running the world”. See Mark R Sneed, *Taming the Beast: A Reception History of Behemoth and Leviathan* (De Gruyter 2021) 2. Following Hobbes’ work, the term has been used to refer to highly powerful entities or absolute states.

³ Hobbes (n 1).

provide. Following Hobbes' influential work, the term Leviathan – still conjuring up the image of an all-mighty state⁴ – has been used to refer to authoritarian regimes.⁵ However, it is increasingly also applied to liberal democracies of which it is argued that their executive branch of power (and public administration in particular) has become overly powerful.⁶ More recently, the term is also deployed in the context of public authorities' increased reliance on algorithmic systems, which have proven to be a highly potent and effective tool to exercise and amass power – giving rise to the so-called *Algorithmic Leviathan*.⁷ Today, a mounting number of states – regardless of their political form of organisation – are arguably starting to qualify for this appellation.

In essence, algorithmic systems enable the automation of tasks through various techniques, from simple rule-based algorithms to more complex knowledge-driven and data-driven methods, including artificial intelligence (AI).⁸ Such systems are increasingly used by public and private actors alike for a range of functions, from the recommendation of books that consumers might like to purchase online or the prediction of crime hotspots, to the approval of a loan. Given the impact they have on their environment and on people subjected to their outputs, algorithmic systems are hence tools through which one can wield power⁹ and through which one can

⁴ Merriam-Webster's online definition of 'leviathan' is: (1) (a) a sea monster defeated by God in various scriptural accounts, (b) a large sea animal; (2) the political state, especially a totalitarian state having a vast bureaucracy; and (3) something large or formidable. See www.merriam-webster.com/dictionary/leviathan. The online Cambridge Dictionary instead keeps it at: something or someone that is extremely large and powerful. See <https://dictionary.cambridge.org/dictionary/english/leviathan>. The online Oxford Advanced Learner's Dictionary refers to: (1) a very large sea monster and (2) a very large and powerful thing, complemented with the example of 'the leviathan of government bureaucracy'. See www.oxfordlearnersdictionaries.com/definition/english/leviathan_1?q=leviathan.

⁵ See, for instance, Ji Li, 'The Leviathan's Rule by Law' (2015) 12 *Journal of Empirical Legal Studies* 815.

⁶ See, for instance, Cass R Sunstein and Adrian Vermeule, *Law and Leviathan: Redeeming the Administrative State* (Harvard University Press 2020).

⁷ The algorithmic Leviathan is characterised by Köning as a "‘giant machine’ that operates in the background, that brings together and harnesses the combined power of a multitude of individuals, and that makes possible coordination outcomes which the individuals themselves could not attain without it" in 'Dissecting the Algorithmic Leviathan: On the Socio-Political Anatomy of Algorithmic Governance' (2020) 33 *Philosophy & Technology* 467. See also Malcolm Langford, 'Taming the Digital Leviathan: Automated Decision-Making and International Human Rights' (2020) 114 *AJIL Unbound* 141. The term has, however, also been used to denote private actors, e.g. in Kathleen Creel and Deborah Hellman, 'The Algorithmic Leviathan: Arbitrariness, Fairness, and Opportunity in Algorithmic Decision-Making Systems' (2022) 52 *Canadian Journal of Philosophy* 26.

⁸ I will provide an extensive description of these techniques in Section 2.1.

⁹ See also, e.g., Karen Yeung, 'Why Worry about Decision-Making by Machine?' in Karen Yeung and Martin Lodge (eds), *Algorithmic Regulation* (Oxford University Press 2019); Pratyusha Kalluri, 'Do Not Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power' (2020) 583 *Nature* 169; Gry Hasselbalch, *Data Ethics of Power* (Edward Elgar Publishing 2021).

1.1 Aligning Algorithmic Regulation and the Rule of Law

3

regulate – whereby regulation is understood, broadly, as a means to manage risk or influence behaviour to achieve a pre-specified goal.¹⁰

Regulation can, however, also be understood more narrowly: as a means *used by a public authority* to influence behaviour or to manage risk *through law*.¹¹ Public authorities¹² of the executive branch of power – tasked with the implementation, application and enforcement of law – increasingly deploy algorithmic systems to regulate in this narrower sense. Across the European Union (EU), Member States have, for instance, started deploying algorithmic systems to assist in decision-making regarding the initiation of tax fraud investigations, the allocation of social welfare

¹⁰ This definition is drawn from Julia Black in ‘Learning from Regulatory Disasters’ (2014) 24 LSE Law, Society and Economy Working Papers 3 <http://eprints.lse.ac.uk/60569/1/WPS2014-24_Black.pdf>, following its adoption by Karen Yeung in ‘Algorithmic Regulation: A Critical Interrogation’ (2018) 12 Regulation & Governance 505, 507.

¹¹ Lawrence Lessig famously identified four different modalities of regulation of which law – traditionally seen as *the* regulatory modality – is only one, the others being: social norms, the market and the architecture or design of technological applications. See Lawrence Lessig, ‘The Law of the Horse: What Cyberlaw Might Teach’ (1999) 113 Harvard Law Review 501. See also Roger Brownsword, ‘Technological Management and the Rule of Law’ (2016) 8 Law, Innovation and Technology 100; Mireille Hildebrandt, ‘Algorithmic Regulation and the Rule of Law’ (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20170355, 4; Nathalie A Smuha, ‘From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence’ (2021) 13 Law, Innovation and Technology 57, 60.

¹² Public authorities can be defined as bodies established by public law, whether at national, regional or local level, for the purpose of providing a public service or acting in the public interest, as well as any private law bodies vested with such powers. See, e.g., the Council of Europe, *The Administration and You – A Handbook* (Conseil de l’Europe 2018). This definition is also used in, e.g., ‘Recommendation CM/Rec(2007)7 of the Committee of Ministers to Member States on Good Administration 2007’ (CM/Rec(2007)7), Article 1. In EU legislation, the scope of ‘public authority’ typically depends on the particular context. For instance, in Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information, a ‘public authority’ is defined in Article 2(2) as (a) government or other public administration, including public advisory bodies, at national, regional or local level; (b) any natural or legal person performing public administrative functions under national law, including specific duties, activities or services in relation to the environment; and (c) any natural or legal person having public responsibilities or functions, or providing public services, relating to the environment under the control of a body or person falling within (a) or (b). The Directive explicitly enables Member States to exclude ‘bodies or institutions when acting in a judicial or legislative capacity’ and hence to render the Directive only applicable to public administrations. See in this regard also Case C-470/19, *Friends of the Irish Environment Limited v Commissioner for Environmental Information*, 15 April 2021. Compare this with the approach taken in the Data Governance Act, where instead the concept of ‘public sector body’ was used, defined as the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities, or one or more such bodies governed by public law. See Article 2(17) of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) 2022 (OJ L).

benefits, the risk assessment of children's well-being, the profiling of criminals, and a range of other administrative acts.¹³

While reliance on algorithmic systems raises intricate ethical and legal questions in private and public contexts alike, in this book, I will be focusing on this narrower type of regulation, and particularly on how public authorities rely on such systems to inform or take administrative acts. Drawing on a definition from the Council of Europe, administrative acts comprise (1) legal acts, of both individual and general application, (2) 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 (3) situations of refusal to act or an omission to do so in cases where a public authority is under an obligation to act.¹⁴ It is through these acts that the executive branch of power regulates individuals, and directly and significantly impacts their lives. As this book will demonstrate, by increasingly outsourcing the adoption of administrative acts to algorithmic systems, the executive can not only act more efficiently but also more powerfully, hence transforming into an *Algorithmic Leviathan*. Given this specific focus – and being well aware that other scholars have used the term more broadly¹⁵ – in this book I will reserve the term *algorithmic regulation* to denote public authorities' use of algorithmic systems to inform or take administrative acts.

The benefits of algorithmic systems are well known. Their use to automate administrative acts can improve productivity, lead to cost savings, and generate

¹³ Maciej Kuziemski and Gianluca Misuraca, 'AI Governance in the Public Sector: Three Tales from the Frontiers of Automated Decision-Making in Democratic Settings' (2020) 44 *Telecommunications Policy* 101976.

¹⁴ See Committee of Ministers of the Council of Europe, 'Recommendation Rec(2004)20 of the Committee of Ministers to Member States on Judicial Review of Administrative Acts' 2. Since the EU lacks a harmonised definition of administrative acts at the level of Member States, I opted to draw on this well-established definition by the Council of Europe. Note, however, that, under EU law, administrative acts taken by EU authorities are typically denoted as 'regulatory acts of individual or general application' (as opposed to 'legislative acts' which in principle only refers to acts adopted through the ordinary or special legislative procedure). See, e.g., Camilla Buchanan, 'Long Awaited Guidance on the Meaning of "Regulatory Act" for Locus Standi under the Lisbon Treaty' (2012) 3 *European Journal of Risk Regulation* 115.

¹⁵ See, e.g., the definition by Mireille Hildebrandt as "*standard-setting, monitoring and behaviour modification by means of computational algorithms*", in Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (n 11) 2. Consider also Karen Yeung's conceptualisation of algorithmic regulation as

decisionmaking systems that regulate a domain of activity in order to manage risk or alter behavior through continual computational generation of knowledge from data emitted and directly collected (in real time on a continuous basis) from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine (or prompt refinement of) the system's operations to attain a prespecified goal

in Yeung, 'Algorithmic Regulation' (n 10) 507. Yeung's conceptualisation is not only broader (since it also encompasses regulation by private actors) but also narrower (as it does not include regulation through basic knowledge-driven algorithmic systems).

1.1 Aligning Algorithmic Regulation and the Rule of Law

5

efficiency gains, particularly by operating at scale.¹⁶ Against the background of an aging civil servants' population, an increasing workload and widespread budget cuts, it is thus no wonder that public authorities are strongly incentivised to adopt this technology on a large scale, as part of the EU's digital agenda¹⁷ and the broader impetus to digitalise the public sector.¹⁸ The European Union's recovery plan – the “*largest stimulus package ever*”, aiming to “*rebuild a post-COVID-19 Europe*”¹⁹ – even explicitly includes a pillar on ‘digital transformation’ that Member States need to integrate in their recovery plans to receive a financial contribution.²⁰ Reference is thereby made to investments in “*government ICT solutions, e-services, applications*”, including the “*use of advanced technologies (such as high performance computing, cybersecurity or artificial intelligence) for public services and decision making*”.²¹

While the potential of algorithmic regulation is clear, the technology can also cause significant harm.²² This risk is inherent to the use of *any* technology, yet the features of algorithmic regulation – and the exercise of power that they enable, along with the delegation of human authority and control over impactful decisions – raises particular threats.²³ First of all, algorithmic systems are shaped by human programmers, and they can hence reflect the prejudices and biases of these programmers, or of the data selected by these programmers to train them on, which can lead to

¹⁶ See, e.g., OECD, *The Path to Becoming a Data-Driven Public Sector* (OECD 2019) <www.oecd-ilibrary.org/governance/the-path-to-becoming-a-data-driven-public-sector_059814a7-en>.

¹⁷ European Commission, ‘A Digital Agenda for Europe’ (2010) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM/2010/0245 final; European Commission, ‘2030 Digital Compass: The European Way for the Digital Decade’ (2021) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions COM/2021/118 final.

¹⁸ The Commission's Coordinated Plan on AI of 2021, for instance, explicitly seeks to “*make the public sector a trailblazer for using AI*”. European Commission, ‘Coordinated Plan on Artificial Intelligence: 2021 Review. Fostering a European Approach to Artificial Intelligence’ (2021) Annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2021) 205 final 46.

¹⁹ See the European Commission's website, detailing the recovery plan: https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

²⁰ See Article 3(b) of Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 Establishing the Recovery and Resilience Facility 2021, OJ L 57.

²¹ *Ibid.*, Annex VII.

²² Drawing on Feinberg, in this book I conceptualise harm as a wrongful setback to or thwarting of an interest, which can also include harm in the non-physical sense, such as the breach of a right. See Joel Feinberg, ‘Harm to Others – Introduction’, in his *The Moral Limits of the Criminal Law – Volume 1: Harm to Others* (Oxford University Press 1984).

²³ See, e.g., Cathy O’Neil, *Weapons of Math Destruction* (Penguin Books Ltd 2017); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (Picador 2019); Timnit Gebru, ‘Race and Gender’ in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford University Press 2020); Smuha, ‘From a “Race to AI” to a “Race to AI Regulation”’ n 11.

discriminatory outcomes.²⁴ Algorithmic systems also process vast amounts of (personal) data, based on which they can instantly categorise and profile individuals, infer new (sensitive) information about them, and intrude their personal sphere.²⁵ Furthermore, algorithmic systems can be used in an opaque manner, which might make it more difficult to identify and address potential unintended errors or prejudices. More importantly, such opacity can also conceal the possible risk that they are *deliberately* designed in a biased, intrusive or erroneous way.²⁶ Due to the scale and speed at which these systems can be used, the consequences when something goes wrong can be enormous.²⁷

Unsurprisingly then, the increased adoption of algorithmic systems is met with increased concern. As a growing body of scholarship has analysed, the use of such systems can adversely impact the rights and interests of individuals subjected to their output, for instance by breaching their right to privacy and their right to non-discrimination.²⁸ When considering the context of the public sector in particular, the use of algorithmic systems also gives rise to domain-specific challenges. Public authorities that rely on such systems to inform or take administrative acts might hamper individuals' social, economic and cultural rights (e.g. by wrongly denying social welfare benefits), their right to asylum (e.g. by wrongly denying an asylum application), their right to liberty and due process (e.g. by wrongly arresting them) and other rights and freedoms that should be protected and respected by the state.

1.1.2 Algorithmic Regulation and the Rule of Law

Reliance on algorithmic regulation can also affect broader societal interests which do not necessarily correspond to, or which go well beyond, individual harm. This can be clarified by distinguishing three types of harm – whereby harm is defined

²⁴ See, e.g., Gabrielle M Johnson, 'Algorithmic Bias: On the Implicit Biases of Social Technology' (2021) 198 *Synthese* 9941; Frederik J Zuiderveen Borgesius, 'Discrimination, Artificial Intelligence, and Algorithmic Decision-Making' (Council of Europe – Directorate General of Democracy 2018).

²⁵ See, e.g., Paul De Hert and others, 'Legal Safeguards for Privacy and Data Protection in Ambient Intelligence' (2009) 13 *Personal and Ubiquitous Computing* 435.

²⁶ See, e.g., Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society* 205395171562251.

²⁷ See, e.g., Karen Yeung, 'Responsibility and AI: A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework', Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), DGI(2019)05, 2019.

²⁸ See, e.g., Max Vetzo, JH Gerards and Remco Neumelman, *Algoritmes en grondrechten* (Boom juridisch 2018); Council of Europe Ad Hoc Committee on Artificial Intelligence – CAHAI, 'Feasibility Study' (Council of Europe 2020) CAHAI(2020)23; European Union Agency for Fundamental Rights, 'Getting the Future Right – Artificial Intelligence and Fundamental Rights in the EU' (European Union Agency for Fundamental Rights 2020) <<https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>>.

broadly as the thwarting of an interest²⁹ – namely individual, collective and societal harm.³⁰

Individual harm occurs when one or more interests of an individual are thwarted. When public services, for instance, seek to detect tax fraud and rely on a biased algorithmic system, which disproportionally flags people with a migration background as risky and leads to biased output, this can hamper the interest of the individual who is subjected to the system, and her right not to be unjustly discriminated against.

Collective harm occurs when one or more interests of a collective or group of individuals are thwarted. Just as a collective consists of the sum of individuals, so too might this harm consist of the sum of harms suffered by members of the collective. The use of the biased fraud detection system can, for instance, give rise to collective harm where it thwarts the interest of a collective of people (in this case, those with a migration background who are subjected to the system) not to be unjustly discriminated against.

Societal harm occurs when one or more interests of society are thwarted. It is hence not concerned with the interests of a particular individual or an interest shared by a collective of individuals. Instead, it concerns harm to an interest held by society at large, going over and above the sum or accumulation of individual interests.³¹ In the above example, a third type of harm is in fact at play. Whether individuals have a migration background or not, and whether they are subjected to this particular algorithmic system or not, they share an interest to live in a society in which the state treats people equally and exercises its power non-arbitrarily. Otherwise, they would live in fear that the state might treat *them* unequally next. That interest is different from the interest not to be unjustly discriminated against, and can hence be distinguished from the individual or collective harm done to those directly subjected to the system. Societal harm may well include instances of individual and collective harm, yet it has an impact beyond it and can hence be assessed as a *sui generis* type of harm.³² The distinction between these types of harm matters, since legal mechanisms that are tailored to protect against individual and collective harm may not necessarily be apt to also protect us against forms of societal harm.³³

²⁹ I made this distinction previously in Nathalie A. Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 Internet Policy Review 3.

³⁰ As mentioned *supra* in note 22, I draw on the conceptualisation of harm by Joel Feinberg, whereby 'interests' include rights but are not limited thereto. Some, but not all, wrongful setbacks to interests are protected by law. It should also be noted that the concept of harm is not static. It changes over time, along with the normative framework of a given society. See, e.g., Joanne Conaghan, 'Law, Harm and Redress: A Feminist Perspective' (2002) 22 Legal Studies 319.

³¹ See in this regard also Yeung, 'Responsibility and AI' (n 27).

³² This is inspired by Émile Durkheim's conceptualisation of society as a *sui generis* entity. See Émile Durkheim, *L'éducation morale* (Alcan 1925).

³³ The importance of considering the societal adverse impact of the use of AI and other digital technologies was already stressed by other scholars. See, e.g., Mireille Hildebrandt, *Smart*

In liberal democracies, the executive branch of power is responsible for implementing and enforcing laws that are, in principle, adopted by the legislative branch through a pluralistic democratic process. Depending on the policy area, public authorities will have a margin of discretion when implementing those laws, and they may have delegated powers to enact laws themselves, yet whenever they exercise public power, they remain bound by the rule of law.³⁴ However, as this book will demonstrate, when public authorities implement and enforce the law through algorithmic regulation, this may – inadvertently or deliberately – undermine the rule of law. The rule of law is a core societal interest in constitutional liberal democracies, and any adverse impact thereon can be conceptualised as a *societal harm*, as it goes beyond the harm to an individual right.

So what is the rule of law? The rule of law implies that government officials and citizens alike are bound by legal rules, and that nobody stands above the law. In the context of the public sector, it requires public authorities to adopt administrative acts based on established rules rather than arbitrary whims.³⁵ The rule of law thus tames public power, as it sets the legal boundaries within which public authorities can legitimately exercise their power.³⁶ Let me, however, stress that, beyond this general description, there is no universal agreement on what this concept precisely entails.³⁷ Drawing on legal sources and scholarship, in this book I will propose a more detailed account of the rule of law in the specific context of *liberal democracies*³⁸ –

Technologies and the End(s) of Law (Edward Elgar Publishing 2015); Yeung, 'Responsibility and AI' (n 27); Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Carissa Véliz, *Privacy Is Power* (Bantam Press 2020); Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) 131 *The Yale Law Journal* 573; Bart van der Sloot and Sascha van Schendel, 'Procedural Law for the Data-Driven Society' (2021) *Information & Communications Technology Law* 1. Reference can also be made to the work of Omri Ben-Shahar, who conceptualised the notion of 'data pollution' as one that goes beyond individual interests, and hence requires different legal mechanisms to tackle its risks. See Omri Ben-Shahar, 'Data Pollution' (2019), 11 *Journal of Legal Analysis* 104.

³⁴ Denis James Galligan, 'Discretionary Powers in the Legal Order', in his *Discretionary Powers: A Legal Study of Official Discretion* (Oxford University Press 1990). See also more generally Bart Raymaekers, *Ethiek, recht en samenleving*. (LannooCampus 2013).

³⁵ See e.g. Brian Z. Tamanaha, *On the Rule of Law: History, Politics, Theory* (Cambridge University Press 2004); David Dyzenhaus, 'Preventive Justice and the Rule-of-Law Project' in Andrew Ashworth, Lucia Zedner and Patrick Tomlin (eds), *Prevention and the Limits of the Criminal Law* (Oxford University Press 2013).

³⁶ Martin Krygier, 'The Rule of Law: Pasts, Presents, and Two Possible Futures' (2016) 12 *Annual Review of Law and Social Science* 199; Wojciech Sadurski, 'Rule of Law v. the Rule of Men and Women: What's in the Distinction?: A Short Essay for Martin Krygier' (2019) 11 *Hague Journal on the Rule of Law* 377.

³⁷ Joseph Raz, 'The Law's Own Virtue' (2019) 39 *Oxford Journal of Legal Studies* 1, 1.

³⁸ It is important to emphasise this context here since – as I will discuss *infra*, in Section 3.1 – the conceptualisation of the rule of law in liberal democracies does not fully align with its conceptualisation in authoritarian regimes.

given that my analysis is concerned with the EU in particular – and I will emphasise its close alignment with human rights and democracy.

Crucially, by virtue of the legal boundaries it establishes, the rule of law enables the protection of human rights and safeguards human liberty and dignity. Moreover, by enabling legislative and judicial oversight over executive action, the rule of law also counters authoritarian tendencies and ensures that governments respect the democratic process. Accordingly, in constitutional liberal democracies, the law plays a *protective* role, which public authorities must safeguard when carrying out their tasks.³⁹ In the EU legal order, the rule of law consists of a number of principles that public authorities must respect, including the principles of legality and legal certainty, the prohibition of the arbitrary use of executive power, the principle of equality before the law, effective judicial review of executive action, and the separation of powers.⁴⁰ As I will argue in this book, the fulfilment of these principles can be undermined when public authorities rely on algorithmic regulation.

Algorithmic regulation requires a translation from legal text-based rules to machine-readable code to enable the automation of the law's application. This translation process encompasses important normative and political decisions of legal interpretation, rather than mere technical actions. When this process contains errors or mistranslations, encompasses prejudices, occurs arbitrarily, encroaches on people's rights, or infringes hierarchically higher legal norms, this dilutes the protective function of the law. Given the scale at which algorithmic regulation is deployed, such dilution can be *systemic* rather than exceptional. That is because the infrastructure put in place for the implementation of algorithmic systems allows for instantaneous mass-decision-making, without the need for human intervention. This also means that, overnight, the parameters of algorithmic systems can be technically adapted by the executive authority that uses them, at the push of a button, thereby immediately affecting all people that are subjected thereto, without the need to inform or to convince (potentially critical) public officials of the changes made. Moreover, the opacity of algorithmic systems can make legislative, judicial and public oversight over how the law is applied through these systems highly difficult.

Over the longer term, this may therefore not only exacerbate the asymmetry of power between the government and its citizens, but also between the executive branch, on the one hand, and the judicial and legislative branch, on the other hand. The latter may no longer be able to ensure that constitutional checks and balances are in place. Both of these asymmetries open the door to the risk that algorithmic

³⁹ See also Werner Schroeder, 'The European Union and the Rule of Law – State of Affairs and Ways of Strengthening', in Werner Schroeder (ed.), *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation* (Hart Publishing 2016).

⁴⁰ I will discuss these principles extensively in Section 3.3, where I will examine the conceptualisation of the rule of law in the EU legal order to build the normative analytical framework of this book.

regulation incrementally increases executive power, diminishes public accountability, and erodes the rule of law. At worst, algorithmic regulation can in this way become a tool that enables authoritarian and illiberal practices,⁴¹ thereby furthering the power of the Algorithmic Leviathan.

At least two scenarios are thinkable. Under a first scenario, a state may resort to the implementation of algorithmic regulation with ill intentions, at scale, to augment its power under the guise of enhancing the efficiency of the public sector, all the while avoiding public scrutiny. It can, for instance, creatively translate law to code and program algorithms in a manner favourable to government supporters, yet unfavourable to dissidents, minority groups or anyone the state considers falling outside the ‘norm’. Under a second scenario, a state may resort to algorithmic regulation with good intentions, yet without proper attention to the risks that can arise therefrom – out of ignorance, negligence, recklessness, or even plain delusion. While the current well-intentioned government may not seek to abuse the vulnerabilities it creates, in the meantime, individuals subjected to the system can nevertheless be harmed, the rule of law’s principles might be undermined, and – albeit inadvertently – an infrastructure is put in place that can easily be abused by a next, less well-intentioned government. Evidently, neither of those two scenarios are desirable, and a third one should be ensured: one in which appropriate safeguards exist to counter this threat.

1.1.3 *The EU’s Rule of Law Crisis and the Rule by Law*

Such safeguards are not only important for the citizens of individual Member States but for the European Union as a whole. After the disastrous occurrence of World War II – initiated by an authoritarian state – the Union was brought to life as a project of state cooperation with the aim of preventing future wars. Originally, this cooperation was primarily economic in nature, focusing on the establishment of a common market.⁴² Yet, over the years, the EU developed into an “*autonomous legal*

⁴¹ For a definition of illiberal and authoritarian practices, I draw on the conceptualisation proposed by Marlies Glasius. She defines authoritarian practices as “*patterns of action that sabotage accountability to people over whom a political actor exerts control, or their representatives, by means of secrecy, disinformation and disabling voice*” and distinguishes these from “*illiberal practices, which refer to patterned and organized infringements of individual autonomy and dignity*”. She notes that, “*although the two kinds of practice often go together in political life, the difference lies in the type of harm effected: authoritarian practices primarily constitute a threat to democratic processes, while illiberal practices are primarily a human rights problem*”. See Marlies Glasius, ‘What Authoritarianism Is ... and Is Not: A Practice Perspective’ (2018) 94 *International Affairs* 515, 517. See also Marlies Glasius and Marcus Michaelsen, ‘Illiberal and Authoritarian Practices in the Digital Sphere’ (2018) 12 *International Journal of Communication* 3795.

⁴² See in this regard e.g. Catherine Barnard, *The Substantive Law of the EU: The Four Freedoms* (6th edn, Oxford University Press 2019).