6

Conclusions

In this book, I set out to examine how public authorities' growing reliance on algorithmic regulation, defined as the use of algorithmic systems to inform or adopt administrative acts, might adversely impact the rule of law and erode its protective role in liberal democracy. I conceptualised this threat as *algorithmic rule by law*, and analysed to which extent the EU legal framework provides adequate safeguards to counter it, focusing both on legal provisions aimed at protecting the rule of law, and legal provisions aimed at tackling the risks associated with algorithmic systems. In this final chapter, I summarise my findings for each of the previous chapters and conclude that the threat of algorithmic rule by law is insufficiently taken into account (Section 6.1). Subsequently, I provide a number of recommendations that build on my analysis (Section 6.2). Finally, I formulate some concluding remarks, and defend the need to (re)embrace normative complexity – in algorithmic regulation, in regulation about algorithmic regulation and in society at large (Section 6.3).

6.1 SUMMARY

In Chapter 1, I introduced this book with the hypothesis that, despite the benefits that algorithmic regulation might generate, the technology's implementation by public authorities also implies significant risks, which may turn the state into an unchecked Algorithmic Leviathan. I specifically expressed the concern that reliance on algorithmic regulation might not only exacerbate the asymmetry of power between the government and its citizens, but also between the executive on the one hand, and the judicial and legislative on the other hand, by strengthening the executive's power, diminishing public accountability and undermining constitutional checks and balances. Importantly, I underlined that this concern arises within a broader context of rule of law-backsliding in several EU Member States, and a more general rise of authoritarian and illiberal tendencies across the world, including in liberal democracies. This concern led to an overarching research question:

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

which legal safeguards does the EU have in place to avoid that reliance on algorithmic regulation by public authorities, amidst a rule of law crisis, undermines the rule of law and results in *algorithmic rule by law*?

To answer this research question and verify my hypothesis, I first took a closer look at the concept of 'algorithmic regulation' in Chapter 2, by examining its technical and societal aspects, and how its use fits within the bureaucratic organisation of public authorities. In Section 2.1, I offered a technical description of algorithmic systems (which are the building blocks of algorithmic regulation) and set out their main characteristics, considering knowledge-driven and data-driven approaches alike and emphasising that algorithmic systems can rely on a mix of approaches. I also examined the definitional conundrums that surround the term artificial intelligence, noting that it can be defined differently depending on the time, context and definer, and that experts reasonably disagree on the type of systems that are deemed sufficiently 'intelligent' to fall under the AI-umbrella. I therefore decided to focus my investigation on all algorithmic systems deployed by public authorities to inform or adopt administrative acts, regardless of their underlying technical approach, and regardless of whether they are called 'AI'.

In Section 2.2, I then complemented the technical description of algorithmic systems with one that emphasises their socio-technical nature, and analysed several consequences of their societal embeddedness. For instance, I pointed out that, being the product of human developers and users, algorithmic systems can reflect human errors or bias, which can have vast consequences given the fact that they enable mass decision-making at population level. I also discussed the fact that algorithmic systems can function or be used in an opaque manner, and that they can undermine human agency and a sense of responsibility for the system's outcomes. Finally, I noted their dependency on data and proxies, which only ever provide a *partial* reflection of reality. I therefore stressed that, regardless of the systems' computational abilities, one should not overlook that the social phenomena they analyse can never be fully reduced to quantitative datapoints and numerical functions, especially when they concern something as complex as human nature.

Bearing these technical and societal aspects in mind, in Section 2.3 I described the role that algorithmic systems play within public authorities that are part of the executive branch of power, which first led me to examine how these authorities are organised, and how administrative acts are taken. To this end, I discussed the main characteristics of their bureaucratic environment (including traits like impersonality, efficiency, rationality and hierarchy) and examined some of the pitfalls associated therewith. I especially emphasised the risk that 'procedural' rationality gets prioritised over 'substantive' rationality, as an excessive focus on routinised procedures in the name of efficiency and objectivity might make public officials lose sight of the substantive aims those procedures are meant to achieve in the first place. I also discussed the warnings that the paradigm of public administration might not always align with the paradigm of individual rights, and that it can lead to authoritarian

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

tendencies. The reason I elaborated on this topic is because it shows, regardless of any reliance on algorithmic systems, that the values of liberal democracy are fragile, especially when public authorities do not explicitly take them into consideration. At the same time, I pointed out the important role of discretion to counter-balance the rigidity of rules and procedures, as it allows public officials to contextualise laws of general applicability to particular cases in a way that preserves individualised justice, based on an appropriate trade-off of relevant interests. Moreover, the pitfalls of bureaucracy can also be countered by public authorities' 'internal morality' based on substantive values, as well as democratic oversight. Finally, I noted that public authorities' use of algorithmic systems is not a new development, though the systems' sophistication and their impact on the lives of individuals steadily increases over time. I also observed that the logic of algorithmic systems aligns rather well with the logic of bureaucracy, which, however, also foreshadowed that reliance thereon might reinforce the pitfalls of bureaucracy.

Having clarified the notion of algorithmic regulation, I then moved on to conceptualise, in Chapter 3, the rule of law. For this purpose, I started in Section 3.1 with a theoretical introduction to the concept, and I explained that it can be defined in various ways, from a list-based enumeration of the principles it entails, to a more succinct focus on the rule of law's overarching purpose and spirit, and particularly the role it plays in taming public power. I distinguished formal and substantive conceptions of the rule of law, linking these, respectively, to naturalistic and positivistic approaches to the law as such. Subsequently, I justified my reliance on a conception of the rule of law that combines both elements, given my focus on the role of the rule of law in liberal democracy, and its inherent entwinement with its values. Finally, I distinguished the rule *of* law from rule *by* law, describing the latter as a distortion of the former, whereby the law is merely used instrumentally as a tool of political power, regardless of the law's substantive aims and of the illiberal or authoritarian practices it might enable through the guise of legality.

As this book focuses on the EU legal order, in Section 3.2, I examined how the rule of law has been conceptualised in the EU, and explained that it heavily draws on the work of the Council of Europe, which lay the groundwork for a conception of the rule of law beyond the nation state. I observed that, in the EU legal order and the acquis of the Council of Europe alike, the rule of law encompasses both substantive and formal elements, which can be boiled down to six core principles, namely the principles of *legality*; *legal certainty*; *the prohibition of arbitrariness of the executive powers*; *equality before the law*; *effective judicial protection, with access to justice and review of government action by independent and impartial courts*; and *the separation of powers.*

These six principles constituted my starting point in Section 3.3, where I set out to concretise the requirements that the rule of law implies for public authorities of the executive branch of power more specifically. Drawing on legal sources that concretise these requirements, I developed a normative analytical framework that could

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

subsequently enable me to assess how algorithmic regulation can impact the fulfilment of the rule of law's principles. For each of the six principles, I not only analysed the requirements they imply for public authorities, but I also examined the challenges associated therewith, observing that, just like the rule of law itself, these principles represent ideals that should be striven towards, yet can never be fully achieved due to the tensions they inherently bear. Essentially, striving to the rule of law's attainment can be likened to walking a tight rope, as a balance must continuously be found between stability and flexibility, precision and openness, rules and discretion. Undoing these tensions, for instance by opting for one of the two extremes instead of carrying out a balancing exercise, undoes the protective power of the law (leading either to rule *by* law or to arbitrary rule), since it is precisely by virtue of these tensions that the law can keep on fulfilling its role in an ever-changing environment marked by a plurality of often conflicting norms and interests.

In Chapter 4, I made a comprehensive assessment of how reliance on algorithmic regulation can undermine the rule of law's principles. For each of the six principles, I discussed in Section 4.1 some concrete examples that illustrate how public authorities' deployment of algorithmic systems can erode the law's protective power and enable illiberal and authoritarian practises, whether purposely or inadvertently. Even though the inherent pitfalls of bureaucracy discussed in Section 2.3 and the inherent tensions of the rule of law discussed in Section 3.3 already pose a challenge to public authorities' fulfilment of the rule of law's principles, my evaluation revealed that reliance on algorithmic regulation can significantly exacerbate those challenges. Importantly, I emphasised that my analysis does not allow me to conclude that *all* uses of algorithmic regulation are harmful for the rule of law and the values it protects per se, but it does support the conclusion that they *can* be harmful, and that this threat needs to be taken seriously, especially against the background of the EU's broader 'rule of law crisis'.

Since several risks were recurrent across the six principles, in Section 4.2 I consolidated the findings of my analysis and conceptualised the adverse impact of algorithmic regulation on the rule of law as *algorithmic rule by law*. I outlined five problematic characteristics of this threat, namely the fact that the law's application is being reduced to a techno-rational exercise (*primacy of techno-rationality*); that its translation from text to code is centralised and delegated to coders who shape the technology's affordance in a largely invisible way (*supremacy of coders*); that discretion at the level of public officials is near eliminated, which undermines their agency to counter the problem of law's over-generality and leaves them technically constrained to uncritically defer to the system's outcomes (*automation of legalism*); that accountability mechanisms for the validity and legality of the law's application are eroded (*deficit of accountability*); and, finally, that the technical infrastructure enabling algorithmic regulation introduces a significant vulnerability in the legal

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

system which can lead to a systemic deficiency of the rule of law (*systemic vulnerability*).[1]

On that basis, and while acknowledging that legal solutions are a necessary but not a sufficient answer to these problems, I concluded that the legal framework needs to have adequate safeguards in place to counter the conceptualised threat. While a detailed account of how those safeguards should look like goes beyond the scope of this book, in Section 4.3 I nevertheless proposed that the legal framework should at least have meaningful and effective mechanisms that enable prior and continuous oversight and accountability over algorithmic regulation, also as regards the upstream choices; that it should enable mechanisms for public participation for questions around algorithmisation, with red lines to protect certain rights and values against a potential tyranny of the majority; that the enforcement mechanisms it offers should be both private and public, and both at national and EU level; that there should be strengthened constitutional checks and balances, including a role for public interest litigation; and that it should foster mechanisms for contestability, as well as the opportunity for internal critical reflection by the public officials who deploy the systems.

Keeping those broad safeguards in mind, in Chapter 5 I evaluated the adequacy of the current EU legal framework in countering the threat of algorithmic rule by law. After contextualising the EU's competences in this field in Section 5.1, in Section 5.2 I proceeded with an analysis of EU legislation that aims to protect the rule of (EU) law, by examining, respectively, the mechanism foreseen in Article 7 TEU, the Conditionality Regulation, and the judicial review enabled by Articles 258–260 TFEU and Article 267 TFEU. I concluded that, while these mechanisms (and especially the two latter) can contribute to the protection of the rule of law at Member State level, they are inadequate to effectively counter the risks associated with algorithmic regulation, which requires ex ante oversight. I also noted that EU rule of law monitoring mechanisms currently do not pay attention to the rule of law-risks associated with algorithmic regulation.

In Sections 5.3 and 5.4, I examined whether EU legislation that aims to protect individuals against the risks of algorithmic systems, whether in the context of automated personal data processing or reliance on 'AI' systems, offers better safeguards. I observed that the GDPR provides important protection mechanisms for individuals, yet concluded, along with the European Commission itself, that these are insufficient to protect them against the various risks of algorithmic systems. I subsequently assessed the AI Act and applauded its introduction of new requirements that must be implemented *before* a system's deployment. However, I concluded that the market-based and legalistic approach of this regulation left open significant legal gaps. It entirely ignores the particular risks posed by

[1] While my analysis focused on the use of algorithmic systems to inform and adopt administrative acts, these pathologies can also arise outside the context of the public sector, since they are to a large extent associated with the problems of automation more generally.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

algorithmic regulation to the rule of law, and does not adequately deal with the threat of algorithmic rule by law. This is not only a missed opportunity given that the AI Act is meant to tackle the risks of algorithmic systems for years to come, but the Act also seemingly prevents Member States from introducing stronger protection mechanisms in view of the maximum harmonisation it aspires to achieve. More generally, I concluded that the legal domains pertaining to the rule of law and algorithmic systems, much like legal scholarship about these topics, are currently working in parallel rather than acknowledging the influence they have on each other, thereby overlooking their mutual risks.

In sum, the EU's *rule of law agenda* and its *digital agenda* – both a priority – are not merely misaligned, but they seem to be pursuing fundamentally antagonistic ends. This can have significant consequences both in the short and in the long term, as the Commission continues its promotion of Member States' uptake of algorithmic regulation under the false assumption that the risks associated therewith are comprehensively addressed by the new legal framework. Meanwhile, under the guise of the 'efficient implementation of the law', the EU is financing Member States' technical infrastructure for scaled algorithmic regulation in all public sector domains, and opens the door for the erosion of the very rule of law it seeks to protect. As I cautioned in the Introduction, at least two scenarios are thinkable. A Member State with intentions that are contrary to the values of liberal democracy might exploit this infrastructure to augment its power and scale its illiberal and authoritarian practices, while diminishing public scrutiny and accountability. Yet even a Member State with 'good' intentions might overlook the fact that the rule of law can be systemically undermined, along with the protective role it plays in liberal democracies, and that the infrastructure it puts in place can easily be abused by a next, less well-intentioned government.

In light of the above, it is crucial that a connection be made between the concerns around the ongoing erosion of the rule of law, and the concerns around the increased reliance on algorithmic regulation. In this book, I sought to establish a bridge between both by arguing that the former concerns can exacerbate the latter, which I conceptualised as the threat of algorithmic rule by law. It is my hope that this examination might foster further research in the intersection of these fields, as well as more attention from policymakers both at the European and national level for the issues at stake. The fact that reliance on algorithmic regulation keeps on increasing makes it essential that effective measures to counter the identified threat are adopted *with urgency*, ideally *before* the technology's adoption becomes even more widespread and its problematic implementation turns out to be irreversible.

6.2 RECOMMENDATIONS

Based on these findings, a number of general recommendations can now be made. First, policymakers and scholars need to take the threat of the algorithmic rule by law more seriously and acknowledge its risks since, without such awareness, no

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

adequate counter-measures can be adopted (Section 6.2.1). Second, the current legal framework needs to be strengthened, which can be done in various ways (Section 6.2.2). Third, a number of neighbouring subjects are relevant for the identified threat and merit being the object of further research, which should hence be encouraged (Section 6.2.3). In what follows, I discuss each in turn.

6.2.1 *Acknowledging the Threat of Algorithmic Rule by Law*

A first recommendation that flows from this book concerns the need for EU institutions and Member States, as well as (legal) scholars focusing on these domains, to start interlinking the known rule of law problems with the known problems arising from algorithmic regulation. These two sets of problems, though being of mutual relevance, are currently insufficiently considered in combination. Yet by examining and addressing these problems in isolation, one fails to apprehend that they can reinforce each other and lead to an adverse impact that is greater than the mere sum of their risks.

The rule of law and the values of liberal democracy more generally are inherently fragile, and the European Commission's expanding rule of law initiatives over the past decade confirms its sensitivity for this fragility. However, the fact that the rule of law is not on the radar of the AI Act demonstrates that the EU may not be aware of the role that algorithmic regulation can play in its erosion, including in the erosion of the rule of *EU* law. After all, problematic translations from legal text to code might also have direct consequences for the law of the European Union, as such translations can occur in a way that erroneously or deliberately infringe or limit the rights that individuals derive from the EU legal order. Furthermore, the illustrations I provided in Section 4.1 are but a fraction of the many known uses of algorithmic regulation adopted by Member States where the rule of law's principles were breached – let alone the many unknown uses where this occurs. My analysis hence only revealed the tip of the iceberg, especially given the fact that many uses of algorithmic regulation by public authorities are simply not (yet) being communicated about.

Despite the higher level of transparency and accountability that one should expect when it comes to actions by public authorities, it is noteworthy that the AI Act to a large extent imposes a single set of obligations on AI providers from private and public organisations alike, seemingly downplaying the specific role of the rule of law in taming public power. It also overlooks the unique role that public authorities play in implementing and applying democratically adopted legislation, and that the application of laws to individuals *not* based on what they do, but based on what they *could* do – in light of predictions grounded in loose correlations with similar profiles – erodes the normative power of the law as such.[2] Since these

[2] This point is well made in Emre Bayamlıoğlu and Ronald Leenes, 'The "Rule of Law" Implications of Data-Driven Decision-Making: A Techno-Regulatory Perspective' (2018) 10 Law, Innovation and Technology 295. See also Mireille Hildebrandt, 'Algorithmic Regulation

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

concerns were not incorporated in the AI Act, it is unlikely that they will be dealt with at the EU level in the near future. Moreover, it is unlikely that Member States will individually be able to adopt stronger protection mechanisms in their national legal orders to anticipate and address these risks, given that the AI Act is meant to provide a ceiling rather than a floor of protection.

One particular difficulty that the EU might grapple with, and that also renders it more difficult for individuals to combat practices that adversely impact the rule of law, is that these practices typically occur under a veneer of legality. As discussed, the law itself is being used as a tool to erode the rule of law's protection of liberal democratic values. Furthermore, the adverse effects associated therewith tend to seep in incrementally and over the longer term, rather than instantaneously and easily discernibly. In contrast with, for instance, the harm caused by a massive oil leak, the harm caused by algorithmic rule by law is often not as tangible, visible, measurable or predictable,[3] which makes it more difficult to take decisive action. It is precisely the combination of the guise of legality and the incremental erosion of the rule of law that renders it so challenging to trigger a strong response. However, by acknowledging these risks and paying more attention to them in discussions on the rule of law and on algorithmic regulation alike, it is my hope that awareness on these issues will increase, and thereby also the possibility that stronger countermeasures will be adopted.

6.2.2 *Strengthening Legal Safeguards*

While this book does not seek to provide detailed recommendations as regards legal provisions that need to be amended or adopted to counter the threat of algorithmic rule by law, based on my analysis I can nevertheless mention some solutions that should be explored.

First of all, there are several ways in which EU legislation can be strengthened so as to provide better legal safeguards against the risks associated with algorithmic regulation. While the AI Act is now final, and it is too late to adapt its legalistic market-based approach, its provisions can still be interpreted in a way that maximises the protection it affords. This would be especially important as regards its transparency and accountability measures, where the need for more meaningful and effective mechanisms for public input and feedback should be considered, for instance as part of the mandatory fundamental rights impact assessments. This could help reveal risks that were overseen, and in some instances perhaps also lead to the

and the Rule of Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20170355; Laurence Diver, 'Interpreting the Rule(s) of Code: Performance, Performativity, and Production' [2021] MIT Computational Law Report 2 <https://law.mit.edu/pub/interpretingtherulesofcode/release/1>.

[3] I also provided this example in Nathalie A Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 Internet Policy Review 3, 10.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

conclusion that it may be better not to use algorithmic regulation in a certain domain, or to do so differently. More generally, citizens should have more say in the process of algorithmisation, including the decisions to implement algorithmic regulation in the first place, while at the same time safeguarding the rights of minorities.

Second, beyond the AI Act, better use can be made of other legislation. Granted, as the analysis in Chapter 5 has shown, the current legal framework provides insufficient protection against the threat of algorithmic rule by law, especially considering the ex post nature of its mechanisms. This, however, does not mean that existing laws should be dismissed. When deployed strategically, ex post safeguards can still serve to mitigate potential harms. While they cannot always undo harm that already occurred, they can nevertheless contribute to the prevention of similar future harms. Both the GDPR and the LED, for instance, provide important safeguards to counter some of the risks associated with algorithmic systems, which can indirectly also counter their adverse impact on the rule of law's principles. At the same time, it is well known that EU privacy legislation is under-enforced, and that national data protection authorities often lack the necessary resources to properly carry out their tasks.[4] Their capacity should hence be expanded, especially given the high likelihood that their workload will considerably increase in the years to come in light of the omnipresence of algorithmic systems.

In addition to strengthening the enforcement of privacy legislation, mechanisms that serve to protect the rule of law can also be deployed more optimally. As already noted, the Commission has been criticised for not deploying the tools it already has in its rule of law toolbox. It can increase its recourse to infringement actions against Member States that adopt illiberal and authoritarian practices, whether they do so with or without algorithmic regulation. It should also be explored whether the Conditionality Regulation can be used to prevent Member States from implementing, especially with EU money, algorithmic regulation that adversely affects the rule of law's principles. Moreover, as part of its rule of law monitoring initiatives, the Commission can explicitly include attention to the risks raised by algorithmic regulation, which will in turn also force Member States to take these risks into consideration. Once the AI Act is applicable, despite its deficiencies, not only the Commission but also private individuals can challenge Member States' non-compliance with their obligations under the Act in court, and they should be encouraged to do so.

This brings me to a third recommendation, namely increasing people's literacy of the risks associated with algorithmic systems, and making them more aware of the fact that the outcomes of these systems are neither infallible nor incontestable. Improved education about the way in which algorithmic systems work is

[4] See also European Digital Rights (EDRi), 'Civil Society Call and Recommendations for Concrete Solutions to GDPR Enforcement Shortcomings' (EDRi, 16 March 2022) <https://edri.org/wp-content/uploads/2022/03/EDRi-recommendations-for-better-GDPR-enforcement.pdf>.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

indispensable to enable critical reflection on their use and output. Member States should hence not proceed with a wide-scale adoption of algorithmic regulation without priorly, or at the very least simultaneously, ensuring that public officials are trained to rely on them in a responsible manner and to ask critical questions about their functioning. It should, however, be noted that mere training and education is not enough to ensure public officials maintain their agency and sense of responsibility when deploying algorithmic systems. As already stressed, if the organisational environment in which the system is used excessively focuses on efficiency goals and KPIs, without facilitating the space, time and especially resources for reflection, procedural rationality will continue to be prioritised over substantive rationality. The protection of the rule of law, and of human rights and democracy more generally, hence needs to become part and parcel of the internal morality of public authorities, which can also imply that more resources need to be allocated for *human* decision-making to preserve the role of administrative discretion at the level of public officials.

Fourth, constitutional checks and balances need to be fortified. Legislators must become more familiar with the intricacies that accompany the implementation of algorithmic regulation and the translation choices this entails, and must take up their role of ensuring democratic oversight over its implementation and use. They, too, would hence benefit from better education about the opportunities and risks of algorithmic regulation, and particularly its impact on the rule of law. Similarly, judges that are tasked with carrying out judicial review of administrative acts that are informed or taken by algorithmic systems must have a better understanding of how these systems work, and be given the opportunity to review also the various upstream decisions that underlie the system's design, in order to tackle potential problems at the root. They should be able to conduct a systemic review rather than only focus their attention on the adverse impact on a single individual, given that the system's use can affect societal rather than mere individual interests. Simultaneously, it should be explored how individuals and civil society organisations can make use of strategic litigation in the public interest against the problematic deployment of algorithmic regulation, without the need to demonstrate individual harm to have standing.

Finally, it must also be acknowledged that legal safeguards to ensure accountability and oversight, even if strengthened, will always leave open the possibility that algorithmic regulation is inadvertently or deliberately used in a way that fosters illiberal and authoritarian practices. There are inherent limitations to what the law can do, and it would be a mistake to think that 'perfect' legislation exists or that it could solve the complex problems raised in this book. This means that reflection is also needed on whether, for some type of administrative acts, or in some public sector domains, the use of algorithmic regulation may need to be excluded altogether, given that it can exacerbate and scale the risks that are already inherent whenever public power is deployed.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

6.2.3 *Promoting Further Research*

This book focused on the use of algorithmic regulation by national public authorities that are part of the executive branch of power. Given this scope limitation, there are several subjects that were not examined, even if they are relevant for the analysis of the impact of algorithmic systems on the rule of law. These subjects hence merit further examination in order to gain a deeper understanding of this impact, and their research should be promoted. In this section, I provide a brief description of some of those areas, which can also be read as a future research agenda.

A first area that requires further examination, concerns the deployment of algorithmic systems in the judiciary. While I noted that algorithmic systems are currently primarily used within the executive branch of power, there are also increasing uses of such systems to assist judges, for instance to make predictions about the risk of recidivism, or to peruse and compare past case law that can be of relevance for a judicial decision.[5] This raises important questions not only for the individuals that may be subjected to a biased or faulty algorithmic system, but also for the rule of law and particularly the principle of judicial independence and impartiality, a prerequisite for the judicial review of government action. It should also be noted that the introduction of such systems in the judiciary can be the result of a government decision to make the judicial system 'more efficient', with potential adverse effects on the principle of the separation of powers.[6] Considering that the independence of the judiciary is already being eroded in several EU Member States, it is important to conduct further research on the use of algorithmic systems in this domain, not only in terms of how individual interests can be affected, but also how it may affect the rule of law.

Second, closer attention should be paid to the potential adverse effects on the rule of law when the European Union itself relies on algorithmic systems.

[5] See, for instance, Julia Dressel and Hany Farid, 'The Accuracy, Fairness, and Limits of Predicting Recidivism' (2018) 4 Science Advances 1; Tania Sourdin, 'Judge v Robot? Artificial Intelligence and Judicial Decision-Making' (2018) 41 University of New South Wales Law Journal 1114; Carolyn McKay, 'Predicting Risk in Criminal Procedure: Actuarial Tools, Algorithms, AI and Judicial Decision-Making' (2020) 32 Current Issues in Criminal Justice 22; Jasper Ulenaers, 'The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge?' (2020) 11 Asian Journal of Law and Economics 1; Vilte Kristina Steponenaite and Peggy Valcke, 'Judicial Analytics on Trial: An Assessment of Legal Analytics in Judicial Systems in Light of the Right to a Fair Trial' (2020) 27 Maastricht Journal of European and Comparative Law 759.

[6] Consider in this regard the example Polish Ministry of Justice's introduction of the Random Allocation of Cases (RAC) System in the Polish judiciary as discussed in Bartosz Wilk, 'Mysterious Random Judge Allocation Algorithm' (*Sieć Obywatelska Watchdog*, 29 January 2019) <https://siecobywatelska.pl/mysterious-random-judge-allocation-algorithm/?lang=en>; Joanna Mazur, 'Automated Decision-Making Systems as a Challenge for Effective Legal Protection in European Union Law' (2021) 46 European Law Review 194; Fundacja Moje Państwo, 'Algorithm of the System of Random Allocation of Cases Finally Disclosed!' (22 September 2021) <https://mojepanstwo.pl/aktualnosci/773>.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

As noted,[7] the Union, too, is subjected to the rule of law and must comply with its principles. In line with the general trend, EU institutions, bodies and agencies are increasingly adopting algorithmic systems to facilitate their tasks and enhance the efficiency of their decision-making processes.[8] Consider, for instance, the European Travel Information and Authorisation System (ETIAS).[9] This system is aimed at automating risk assessments regarding non-EU citizens who wish to enter the EU, and to make recommendations as to whether they should be allowed to enter.[10] According to Frontex' website, ETIAS will "*carry out pre-travel screening of travellers who enjoy from visa-free access to the Schengen Area, and thus allow Member States to deny authorisation to travellers considered to pose a security threat, a risk in terms of irregular migration or public health*".[11] Accordingly, the use of algorithmic regulation not only poses risks at the *national* level, but also at the *EU* level, and its impact on the EU rule of law should be further examined – ideally *before* its widespread adoption.

Third, while my investigation only focused on the robustness of the EU legal order, I noted that legislation at national level can also offer solace against the risk of algorithmic rule by law. In most Member States, provisions of constitutional and administrative law could, even if general in nature, potentially be applied to the use of algorithmic regulation, and be interpreted in a manner that provides stronger legal safeguards against the identified risks. A thorough examination of how individual Member States are currently dealing with those risks might not only reveal further gaps in protection, but could also lead to the identification of best practices that can be adopted by other jurisdictions.

A final area that merits closer attention is one that I mentioned only sporadically in this book, namely the reliance of public authorities on private companies to design and develop algorithmic systems. The focus of my analysis lay on how the dependency on such systems can increase the executive's power. However, when the executive outsources the upstream design and translation choices of algorithmic systems to a private company, or is otherwise dependent on a private company for its data or technical infrastructure, this can also significantly increase the power of that private company, as the latter can shape how public power is exercised by shaping the technology's affordances.[12] The Algorithmic Leviathan – mighty as it may be –

[7] See *supra*, Section 3.2.3.

[8] Note that the AI Act also applies to AI systems used by EU entities.

[9] See also Regulation 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations no. 1077/2011, no. 515/2014, no. 2016/399, no. 2016/1624 and no. 2017/2226 2018.

[10] Pedro Rubim Borges Fortes, Pablo Marcello Baquero and David Restrepo Amariles, 'Artificial Intelligence Risks and Algorithmic Regulation' [2022] European Journal of Risk Regulation 1, 2.

[11] Frontex, 'ETIAS' (2024) <www.frontex.europa.eu/what-we-do/etias/about-etias/>. At the moment of this book's finalisation, the system is not yet operational, though its launch is expected for mid-2025.

[12] See also Linnet Taylor, 'Public Actors without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector' (2021) 34 Philosophy & Technology 897.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

might hence in turn be dependent on an even mightier private company, which likewise raises important rule of law-concerns that require further scrutiny.

6.3 EMBRACING NORMATIVE COMPLEXITY

Let me conclude this book by taking a step back, and sharing a few broader reflections. Essentially, my analysis exposed that reliance on algorithmic regulation can disguise or obliterate the normative tensions that are inherent to the very concept of the rule of law and its principles, and thereby undermine the protective power of the law.[13] It might lead to an automated form of legalism – or the uncritical adherence to and execution of rules – by skewing the balance in favour of rules instead of discretion, resulting in their divorce rather than their marriage.

However, when examining the EU legal framework's aptness to counter the identified risks, I also recalled that a legalistic approach can arise in contexts outside algorithmic regulation, given the techno-rational features that underlie the AI Act. Its list-based methodology, along with its aspiration to reduce the protection of human rights (and the intricate trade-offs of interests this entails) to technical standards, may likewise result in a legalistic solution which fails to do justice to the complexity of the problem. Accordingly, on a meta level, even the rules that are supposed to counter the risks associated with algorithmic rule by law might show the same deficiency, whereby protecting human rights, democracy and the rule of law can turn into a technical checklist rather than being seen as a normative endeavour.[14]

Consequently, and rather ironically, one can observe the same deficiency both in the identified problem and in its proposed solutions. This deficiency comes down to the apparent need to eliminate normative tensions by settling down on a set of technical rules, whether algorithmically codified or part of a legalistic text, which allow us to forget about the complex normative questions that underlay those rules, and to just focus on their execution instead. In a way, this is not surprising. It is, after all, much easier to execute a set of pre-determined rules, than to be constantly faced with (the responsibility to make) difficult normative trade-offs, which requires confronting different interests, understanding various points of view and trying to balance them out on a continuous basis. However, that is precisely what the rule of law, along with its intrinsic tensions, is about, and what enables it to fulfil its protective role in a heterogenous society with inevitably conflicting norms.

[13] See *supra*, Sections 3.4 and 4.2 in particular.

[14] In the same vein, scholars have also remarked that, when public authorities are spurred to implement ethical guidelines when they develop and deploy algorithmic systems, there is a "*dangerous tendency where ethical deliberation is sometimes seen as an obnoxious bureaucratic box ticking exercise, instead of being considered as a vital part of the design and build-up of a data project*". See Lotje Siffels and others, 'Public Values and Technological Change: Mapping How Municipalities Grapple with Data Ethics' in Andreas Hepp, Juliane Jarke and Leif Kramp (eds), *New Perspectives in Critical Data Studies: The Ambivalences of Data Power* (Springer International Publishing 2022).

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009

As discussed in Chapter 3, the rule of law requires a balance between stability and flexibility, vagueness and precision, generality and particularity, rules and discretion. This also means that the law will never be *perfectly* predictable, but that the navigation of these tensions can nevertheless allow it to provide *reasonable* predictability.

However, as the analysis of this book has shown, we are at risk precisely because we no longer seem to find a way to deal with these normative tensions, and instead prefer to search for an optimal solution that can be codified into an algorithmic system, and subsequently scaled with the click of a button. Algorithmic regulation promises simplicity, and a route to avoid the complex tensions of legal rules which are continuously open to multiple interpretations. Crucially, this same promise is also what is threatening the very foundations of liberal democracy today, as illiberal and authoritarian tendencies – along with populism – embody the very elimination of plurality in favour of simplicity. Autocratic leaders are hence exploiting this very feature of the law and, through a rule *by* law approach, seek to put forward *their* interpretation above others. And algorithmic regulation provides them with a tool to systematise and scale that interpretation, in the name of efficiency.

In sum, the threat encountered at the level of the rule of law, of which algorithmic regulation in public administration is an illustration, is the same one that threatens the very preservation of liberal democracy as a political system, namely the elimination of conflicting normative tensions in favour of essentialising a single view. Accordingly, the most important antidote to this threat is to (re)learn to embrace not only the normative tensions that are inherent to the law, but also the tensions that are inherent in a democratic society, which is marked by a plurality of views rather than by a single ideology. As long as we believe that there are multiple ways of living a 'good life' and that no one political view should oppress all others, the law's interpretation should not be essentialised and systematised. Any attempts to do so would undermine not only the rule of law, but also liberal democracy.

Yet if the law's normative tensions are to be maintained, along with the intricate balancing exercise this entails, it is even more important that this exercise is not simply outsourced to a handful of coders. Regardless of any future political developments, algorithmic regulation will inevitably play an ever bigger role in our society. It is therefore our collective responsibility to ensure that its adoption involves public participation, transparency, oversight and democratic accountability, and that it occurs in line with the trinity of human rights, democracy and the rule of law.

Downloaded from https://www.cambridge.org/core. IP address: 13.201.136.108, on 05 Oct 2025 at 00:42:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009427500.009