Introduction

Technologies have always challenged, if not disrupted, the social, economic legal, and to an extent, the ideological status quo. Such transformations impact constitutional law, as the State formulates its legal response to the new technologies being developed and applied by the market, and as it considers its own use of the technologies. The development of data collection, mining, and algorithmic analysis, resulting in predictive profiling – with or without the subsequent potential manipulation of attitudes and behaviors of users – presents unique challenges to constitutional law at the doctrinal as well as theoretical levels.

Historically, liberal constitutionalism has been built on a vertical dimension where the power to limit liberty is only the public one, only in given jurisdictional territory, and therefore should be constrained by the national constitution. Moreover, as of the rise of the bureaucratic state, the technologies for infringing liberty or equality were thought to be containable by the exercise of concrete judicial review (either constitutional or administrative), abstract judicial review, or a combination of the above. In recent years, however, the rise of the algorithmic society has led to a paradigmatic change where the public power is no longer the only source of concern for the respect of fundamental rights and the protection of democracy, where jurisdictional boundaries are in flux, and where doctrines and procedures developed in the pre-cybernetic age do not necessarily capture rights violations in a relevant time frame. This requires either the redrawing of constitutional boundaries so as to subject digital platforms to constitutional law or a revisiting of the relationship between constitutional law and private law, including the duties of the state to regulate the cybernetic complex, within or outside the jurisdictional boundaries of the state.

Within this framework, this book is the result of the biannual work of the IACL Research Group "Algorithmic State, Market and Society" after an inaugural conference at the University of Florence and European University Institute in 2019. This Research Group promotes the debate in the field of law and technology, and primarily regarding the new constitutional challenges raised by the development of algorithmic technologies which assist (if not control) decision-making processes by state agencies or corporations (often large and multinational) that provide key

services online. Based on this framework, this book tries to answer the following research questions: How has the relationship among powers changed in the algorithmic society? What are the new substantive and procedural rights protecting individuals and democratic values? How can we balance innovation (and the legal incentives for businesses to pursue innovation) with the need to ensure transparency and accountability? To what extent should new forms of public or private law tools be developed to address the challenges posed by the shift to the algorithmic society?

The answers to these questions have likely changed in the last years due to the evolving landscape of algorithmic technologies and policy. The increasing implementation of algorithmic technologies in the public and private sectors promotes an intertwined framework. The launch of the European proposal for the Artificial Intelligence Act is just an example of the need to provide a framework for mitigating risks while promoting innovation. This book does not aim just to address recent developments and provide answers to evolving dynamics. The goal is to provide a taxonomy of the constitutional challenges of the algorithmic society, with some focuses on specific challenges.

This goal is reflected in the book's structure, which is articulated in three parts. The first part aims to underline the challenges for fundamental rights and democratic values in the algorithmic society. In particular, this part underlines how the fast-growing use of algorithms in various fields like justice, policing, and public welfare could end in biased and erroneous decisions, boosting inequality, discrimination, unfair consequences, and undermining constitutional rights, such as privacy, freedom of expression, and equality. The second part addresses the regulation and policy of the algorithmic society. There are multiple challenges here due to opacity and biases of algorithmic systems, as well as the actors involved in the regulation of these technologies. The third part examines the role and responsibilities of private actors, underlining various constitutional opportunities and threats. In this case, the book aims to underline how the private sector is a relevant player, pursuing functions that reflect public powers.

1

Constitutional Law in the Algorithmic Society

Oreste Pollicino and Giovanni De Gregorio [*]

1.1 INTRODUCTION

Technologies have always led to turning points in society.[1] In the past, technological developments have opened the door to new phases of growth and change, while influencing social values and principles. Algorithmic technologies fit within this framework. These technologies have contributed to introducing new ways to process vast amounts of data.[2] In the digital economy, data and information are fundamental assets which can be considered raw materials the processing of which can generate value.[3] Even simple pieces of data, when processed with a specific purpose and mixed with other information, can provide models and predictive answers. These opportunities have led to the rise of new applications and business models in a new phase of (digital) capitalism,[4] as more recently defined as information capitalism.[5]

Although these technologies have positive effects on the entire society since they increase the capacity of individuals to exercise rights and freedoms, they have also led to new constitutional challenges. The opportunities afforded by algorithmic technologies clash with their troubling opacity and lack of accountability, in what

[*] Oreste Pollicino is a Full Professor of Constitutional Law at Bocconi University. He authored Sections 1.2, 1.5, and 1.6. Giovanni De Gregorio is Postdoctoral Researcher, Centre for Socio-Legal Studies, University of Oxford. He authored Sections 1.1, 1.3, and 1.4.

[1] Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008).

[2] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 239; Sue Newell and Marco Marabelli, 'Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of "Datification"' (2015) 24 *Journal of Strategic Information Systems* 3.

[3] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Murray 2013).

[4] Daniel Schiller, *Digital Capitalism. Networking the Global Market System* (MIT Press 1999).

[5] Julie Cohen, *Between Truth and Power. The Legal Construction of Information Capitalism* (Oxford University Press 2020).

has been defined as an 'algocracy'.[6] It is no coincidence that transparency is at the core of the debate about algorithms.[7] There are risks to fundamental rights and democracy inherent in the lack of transparency about the functioning of automated decision-making processes.[8] The implications deriving from the use of algorithms may have consequences on individuals' fundamental rights, such as the right to self-determination, freedom of expression, and privacy. However, fundamental rights do not exhaust the threats which these technologies raise for constitutional democracies. The spread of automated decision-making also challenges democratic systems due to its impact on public discourse and the impossibility of understanding decisions that are made by automated systems affecting individual rights and freedoms.[9] This is evident when focusing on how information flows online and on the characteristics of the public sphere, which is increasingly personalised rather than plural.[10] Likewise, the field of data is even more compelling due to the ability of data controllers to affect users' rights to privacy and data protection by implementing technologies the transparency and accountability of which cannot be ensured.[11] The possibility to obtain financing and insurance or the likelihood of a potential crime are only some examples of the efficient answers which automated decision-making systems can provide and of how such technologies can affect individuals' autonomy.[12]

At a first glance, algorithms seem like neutral technologies processing information which can lead to a new understanding of reality and predict future dynamics. Technically, algorithms, including artificial intelligence technologies, are just methods to express results based on inputs made up of data.[13] This veil of neutrality

[6] John Danaher, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29 *Philosophy & Technology* 245.

[7] See, in particular, Daniel Neyland, 'Bearing Accountable Witness to the Ethical Algorithmic System' (2016) 41 *Science, Technology & Human Values* 50; Mariarosaria Taddeo, 'Modelling Trust in Artificial Agents, A First Step toward the Analysis of e-Trust' (2010) 20 *Minds and Machines* 243. Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) 11 *Ethics and Information Technology* 105.

[8] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3 *Big Data & Society*; Christopher Kuner et al., 'Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?' (2017) 6 *International Data Privacy Law* 167; Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in Jacques Bus et al. (eds), *Digital Enlightenment Yearbook* (IOS Press 2012); Meg L. Jones, 'Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 *Social Studies of Science* 216.

[9] Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) *Royal Society Philosophical Transactions* A.

[10] Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 *Social Media + Society* 3.

[11] Serge Gutwirth and Paul De Hert, 'Regulating Profiling in a Democratic Constitutional States', in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (2006), 271.

[12] Brent D. Mittlestadt et al., 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 *Big Data & Society*.

[13] Tarleton Gillespie, 'The Relevance of Algorithms' in Tarleton Gillespie et al. (eds), *Media Technologies: Essays on Communication, Materiality, and Society* (MIT Press 2014), 167.

falls before their human fallacy. Processes operated by algorithms are indeed value-laden, since technologies are the result of human activities and determinations.[14] The contribution of humans in the development of data processing standards causes the shift of personal interests and values from the human to the algorithmic realm. If, from a technical perspective, algorithms are instruments that extract value from data, then moving to the social perspective, such technologies constitute automated decision-making processes able to affect society and thus also impacting on constitutional values, precisely fundamental rights and democratic values.

Within this challenging framework between innovation and risk, it is worth wondering about the role of regulation and policy in this field. Leaving the development of algorithmic technologies without safeguards and democratic oversight could lead society towards techno-determinism and the marginalisation of public actors, which would lose their role in ensuring the protection of fundamental rights and democratic values. Technology should not order society but be a means of promoting the evolution of mankind. Otherwise, if the former will order the drive of the latter in the years to come, we could witness the gradual vanishing of democratic constitutional values in the name of innovation.

Since algorithms are becoming more and more pervasive in daily life, individuals will increasingly expect to be aware of the implications deriving from the use of these technologies. Individuals are increasingly surrounded by technical systems influencing their decisions without the possibility of understanding or controlling this phenomenon and, as a result, participating consciously in the democratic debate. This situation is not only the result of algorithmic opacity, but it is firmly linked to the private development of algorithmic technologies in constitutional democracies. Because of the impact of these technologies on our daily lives, the predominance of businesses and private entities in programming and in guiding innovation in the age of artificial intelligence leads one to consider the role and responsibilities of these actors in the algorithmic society. The rise of 'surveillance capitalism' is not only a new business framework but a new system to exercise (private) powers in the algorithmic society.[15]

We believe that constitutional law plays a critical role in addressing the challenges of the algorithmic society. New technologies have always challenged, if not disrupted, the social, economic, legal, and, to a certain extent, ideological *status quo*. Such transformations impact constitutional values, as the state formulates its legal response to new technologies based on constitutional principles which meet market dynamics, and as it considers its own use of technologies in light of the limitation imposed by constitutional safeguards. The development of data collection, mining,

[14] Philippe A. E. Brey and Johnny Soraker, *Philosophy of Computing and Information Technology* (Elsevier 2009); Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Da Capo Press 1988).

[15] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Political Affairs 2018).

and algorithmic analysis, resulting in predictive profiling – with or without the subsequent potential manipulation of the attitudes and behaviours of users – present unique challenges to constitutional law at the doctrinal as well as theoretical levels.

Constitutions have been designed to limit public (more precisely governmental) powers and protect individuals against any abuse from the state. The shift of power from public to private hands requires rethinking and, in case, revisiting some well-established assumptions. Moreover, during the rise of the bureaucratic state, the technologies for infringing liberty or equality were thought to be containable by the exercise of concrete judicial review (either constitutional or administrative), abstract judicial review, or a combination of the above. In recent years, however, the rise of the algorithmic society has led to a paradigmatic change where public power is no longer the only source of concern for the respect of fundamental rights and the protection of democracy, where jurisdictional boundaries are in flux, and where doctrines and procedures developed in the pre-cybernetic age do not necessarily capture rights violations in a relevant time frame. This requires either the redrawing of the constitutional boundaries so as to subject digital platforms to constitutional law or to revisit the relationship between constitutional law and private law, including the duties of the state to regulate the cybernetic complex, within or outside the jurisdictional boundaries of the state. Within this framework, the rise of digital private powers challenges the traditional characteristics of constitutional law, thus encouraging to wonder how the latter might evolve to face the challenges brought by the emergence of new forms of powers in the algorithmic society.

The primary goal of this chapter is to introduce the constitutional challenges coming from the rise of the algorithmic society. Section 1.2 examines the challenges for fundamental rights and democratic values, with a specific focus on the right to freedom of expression, privacy, and data protection. Section 1.3 looks at the role of constitutional law in relation to the regulation and policy of the algorithmic society. Section 1.4 examines the role and responsibilities of private actors underlining the role of constitutional law in this field. Section 1.5 deals with the potential remedies which constitutional law can provide to face the challenges of the information society.

1.2 FUNDAMENTAL RIGHTS AND DEMOCRATIC VALUES

Algorithmic technologies seem to promise new answers and an increase of accuracy of decision-making, thus offering new paths to enrich human knowledge.[16] Predictive models can help public administrations provide more efficient public services and spare resources. Likewise, citizens can rely on more sophisticated platforms allowing them to express their identity, build social relationships, and share ideas. Therefore, these technologies can be considered an enabler for the exercise of rights and

[16] Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (Public Affairs 2013).

freedoms. Nonetheless, artificial intelligence technologies are far from perfect. Predictive models have already produced biased results and inaccurate outputs, leading to discriminatory results.[17] The implications deriving from the implementation of automated technologies may have consequences for individual fundamental rights, such as the right to self-determination, freedom of expression, and privacy, even at a collective level. It is worth stressing that the relationship between fundamental rights and democracy is intimate, and the case of freedom of expression and data protection underlines this bundle. Without the possibility of expressing opinions and ideas freely, it is not possible to define society as democratic. Likewise, without rules governing the processing of personal data, individuals could be exposed to a regime of private surveillance without a set of accountability and transparency safeguards. Among different examples, the moderation of online information and users' profiling can be taken as two paradigmatic examples of the risks which these technologies raise for fundamental rights and democratic values.

The way in which we express opinions and ideas online has changed in the last twenty years. The Internet has contributed to shaping the public sphere. It would be a mistake to consider the new channels of communication just as threats. The digital environment has indeed been a crucial vehicle to foster democratic values like freedom of expression.[18] However, this does not imply that threats have not appeared on the horizon. Conversely, the implementation of automated decision-making systems is concerning for the protection of the right to freedom of expression online. To understand when automation meets (and influences) free speech, it would be enough to closely look at how information flows online under the moderation of online platforms. Indeed, to organise and moderate countless content each day, platforms also rely on artificial intelligence to decide whether to remove content or signal some expressions to human moderators.[19] The result of this environment is troubling for the rule of law from different perspectives. First, artificial intelligence systems contribute to interpreting legal protection of fundamental rights by de facto setting a private standard of protection in the digital environment.[20] Second, there is also an issue of predictability and legal certainty, since private determinations blur the lines between public and private standards. This leads us to the third point: the lack of transparency and accountability in the decision concerning freedom of expression online.[21] In other words, the challenge in this case is to measure compliance with the principle of the rule of law. Indeed, the implementation of machine

[17] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) (2) *Columbia Business Law Review*.

[18] Yochai Benkler, *The Wealth of Networks* (Yale University Press 2006).

[19] Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (Yale University Press 2018).

[20] Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598.

[21] Giovanni De Gregorio, 'Democratising Content Moderation. A Constitutional Framework' (2019) *Computer Law and Security Review*.

learning technologies does not allow to scrutinising decisions over expressions which are still private but involve the public at large. With the lack of regulation of legal safeguards, online platforms will continue to be free to assess and remove speech according to their business purposes.

Within this framework, disinformation deserves special attention.[22] Among the challenges amplified by technology, the spread of false content online has raised concerns for countries around the world. The Brexit referendum and the 'Pizzagate' during the last US elections are just two examples of the power of (false) information in shaping public opinion. The relevance of disinformation for constitutional democracies can be viewed from two angles: the constitutional limits to the regulatory countermeasures and the use of artificial intelligence systems in defining the boundaries of disinformation and moderating this content. While for public actors the decision to intervene to filter falsehood online requires questioning whether and to what extent it is acceptable for liberal democracies to enforce limitations to freedom of expression to falsehood, artificial intelligences catalogue vast amounts of content, deciding whether they deserve to be online according to the policies implemented by unaccountable private actors (i.e., online platforms). This is a multifaceted question since each constitutional system paradigm adopts different paradigms of protection, even when they share the common liberal matrix, like in the case of Europe and the United States. In other words, it is a matter of understanding the limits of freedom of speech to protect legitimate interests or safeguard other constitutional rights.

Besides, the challenges of disinformation are not just directly linked to the governance of online spaces but also to their exploitation. We have experienced in recent years the rise of new (digital) populist narratives manipulating information for political purposes.[23] Indeed, in the political context, technology has proven to be a channel for vehiculating disinformation citizenship, democracy, and democratic values. By exploiting the opportunities of the new social media, populist voices have become a relevant part of the public debate online, as the political situations in some Member States show. Indeed, extreme voices at the margins drive the political debate. It would be enough to mention the electoral successes of Alternative für Deutschland in Germany or the Five Star Movement in Italy to understand how populist narratives are widespread no longer as an answer to the economic crisis but as anti-establishment movements fighting globalised phenomena like migration and proposing a constitutional narrative unbuilding democratic values and the principle of the rule of law.[24]

The threats posed by artificial intelligence technologies to fundamental rights can also be examined by looking at the processing of personal data. Even more evidently,

[22] Giovanni Pitruzzella and Oreste Pollicino, *Disinformation and Hate Speech: A European Constitutional Perspective* (Bocconi University Press 2020).
[23] Maurizio Barberis, *Populismo digitale. Come internet sta uccidendo la democrazia* (Chiareletter 2020).
[24] Giacomo Delle Donne et al., *Italian Populism and Constitutional Law. Strategies, Conflicts and Dilemmas* (Palgrave Macmillan 2020).

automated decision-making systems raise comparable challenges in the field of data protection. The massive processing of personal data from public and private actors leads individuals to be subject to increasingly intrusive interferences in their private lives.[25] Smart applications at home or biometric recognition technologies in public spaces are just two examples of the extensive challenges for individual rights. The logics of digital capitalism and accumulation make surveillance technologies ubiquitous, without leaving any space for individuals to escape. In order to build such a surveillance and profiling framework, automated decision-making systems also rely on personal data to provide output. The use of personal information for this purpose leads one to wonder whether individuals should have the right not to be subjected to a decision based solely on automated processing, including profiling which produces legal effects concerning him or her or similarly significantly affects him or her.[26] These data subjects' rights have been primarily analysed from the perspective of the right to explanation. Scholars have pointed out possible bases for the right to explanation such as those provisions mandating that data subjects receive meaningful information concerning the logic involved, as well as the significance, and the envisaged consequences of the processing.[27]

These threats would suggest looking at these technologies with fear. Nonetheless, new technologies are playing a disruptive role. Society is increasingly digitised, and the way in which values are perceived and interpreted is inevitably shaped by this evolution. New technological development has always led to conflicts between the risks and the opportunities fostered by its newness.[28] Indeed, the uncertainty in the novel situations is a natural challenge for constitutional democracies, precisely for the principle of the rule of law.[29] The increasing degree of uncertainty concerning the applicable legal framework and the exercise of power which can exploit technologies based on legal loopholes also lead one to wonder how to ensure due process in the algorithmic society. Therefore, the challenges at stake broadly involve the principle of the rule of law not only for the troubling legal uncertainty relating to new technologies but also as a limit against the private determination of fundamental rights protection the boundaries of protection of which are increasingly shaped and determined by machines. The rule of law can be seen as an instrument to

[25] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001).
[26] Ibid., Art 22.
[27] Margot Kaminski, 'The Right to Explanation, Explained' (2019) 34(1) *Berkeley Technology Law Journal* 189; Antoni Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)' (2017) 8(3) *European Journal of Law and Technology* 1; Sandra Wachter et al., 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 243; Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38(3) *AI Magazine* 50.
[28] Monroe E. Price, 'The Newness of Technology' (2001) 22 *Cardozo Law Review* 1885.
[29] Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology* 1.

measure the degree of accountability, the fairness of application, and the effectiveness of the law.[30] As Krygier observed, it also has the goal of securing freedom from certain dangers or pathologies.[31] The rule of law is primarily considered as the opposite of arbitrary public power. Therefore, it is a constitutional bastion limiting the exercise of authorities outside any constitutional limit and ensuring that these limits answer to a common constitutional scheme.

Within this framework, the increasing spread and implementation of algorithmic technologies in everyday life lead to wondering about the impact of these technologies on individuals' fundamental rights and freedoms. This process may tend to promote a probabilistic approach to the protection of fundamental rights and democratic values. The rise of probability as the primary dogma of the algorithmic society raises questions about the future of the principle of rule of law. Legal certainty is increasingly under pressure by the non-accountable determination of automated decision-making technologies. Therefore, it is worth focusing on the regulatory framework which could lead to a balance between ensuring the protection of democratic values without overwhelming the private sector with disproportionate obligations suppressing innovation.

1.3 REGULATION AND POLICY

Fundamental rights and democratic values seem to be under pressure in the information society. This threat for constitutional democracies might lead to wondering about the role of regulation and policy within the framework of algorithmic technologies. The debate about regulating digital technologies started with the questioning of consolidated notions such as sovereignty and territory.[32] The case of *Yahoo* v. *Licra* is a paradigmatic example of the constitutional challenges on the horizon in the early 2000s.[33] More precisely, some authors have argued that regulation based on geographical boundaries is unfeasible, so that applying national laws to the Internet is impossible.[34] Precisely, Johnson and Post have held that 'events on the Net occur everywhere but nowhere in particular' and therefore 'no physical jurisdiction has a more compelling claim than any other to subject events

[30] Recent rulings of the European Court of Justice have highlighted the relevance of the rule of law in EU legal order. See Case C-64/16, Associação Sindical dos Juízes Portugueses v. Tribunal de Contas; Case C-216/18 PPU, *LM*; Case C-619/18, Commission v. Poland (2018).

[31] Martin Krygier, 'The Rule of Law: Legality, Teleology, Sociology' in Gianlugi Palomblla and Neil Walker (ed), *Relocating the Rule of Law* (Hart 2009), 45.

[32] John P. Barlow, 'A Declaration of Independence of the Cyberspace' (Electronic Frontier Foundation 1996), www.eff.org/cyberspace-independence.

[33] *Licra et UEJF* v. *Yahoo Inc and Yahoo France TGI Paris* 22 May 2000. See Joel R. Reidenberg, 'Yahoo and Democracy on the Internet' (2001/2002) 42 *Jurimetrics* 261; *Yahoo!, Inc.* v. *La Ligue Contre Le Racisme* 169 F Supp 2d 1181 (ND Cal 2001). See Christine Duh, 'Yahoo Inc. v. LICRA' (2002) 17 *Berkeley Technology Law Journal* 359.

[34] David R. Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1371.