

# Constitutional Law in the Algorithmic Society

*Oreste Pollicino and Giovanni De Gregorio*<sup>\*</sup>

## 1.1 INTRODUCTION

Technologies have always led to turning points in society.<sup>1</sup> 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.<sup>2</sup> In the digital economy, data and information are fundamental assets which can be considered raw materials the processing of which can generate value.<sup>3</sup> 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,<sup>4</sup> as more recently defined as information capitalism.<sup>5</sup>

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

<sup>\*</sup> 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.

<sup>1</sup> Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008).

<sup>2</sup> 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.

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

<sup>4</sup> Daniel Schiller, *Digital Capitalism. Networking the Global Market System* (MIT Press 1999).

<sup>5</sup> Julie Cohen, *Between Truth and Power. The Legal Construction of Information Capitalism* (Oxford University Press 2020).

has been defined as an ‘algorocracy’.<sup>6</sup> It is no coincidence that transparency is at the core of the debate about algorithms.<sup>7</sup> There are risks to fundamental rights and democracy inherent in the lack of transparency about the functioning of automated decision-making processes.<sup>8</sup> 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.<sup>9</sup> 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.<sup>10</sup> 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.<sup>11</sup> 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.<sup>12</sup>

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.<sup>13</sup> This veil of neutrality

<sup>6</sup> John Danaher, ‘The Threat of Algorocracy: Reality, Resistance and Accommodation’ (2016) 29 *Philosophy & Technology* 245.

<sup>7</sup> 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.

<sup>8</sup> 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.

<sup>9</sup> Paul Nemitz, ‘Constitutional Democracy and Technology in the Age of Artificial Intelligence’ (2018) *Royal Society Philosophical Transactions A*.

<sup>10</sup> Nicolas Suzor, ‘Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms’ (2018) 4 *Social Media + Society* 3.

<sup>11</sup> 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.

<sup>12</sup> Brent D. Mittelstadt et al., ‘The Ethics of Algorithms: Mapping the Debate’ (2016) 3 *Big Data & Society*.

<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup>

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,

<sup>14</sup> 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).

<sup>15</sup> 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.<sup>16</sup> 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

<sup>16</sup> 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.<sup>17</sup> 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.<sup>18</sup> 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.<sup>19</sup> 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.<sup>20</sup> 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.<sup>21</sup> 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

<sup>17</sup> 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*.

<sup>18</sup> Yochai Benkler, *The Wealth of Networks* (Yale University Press 2006).

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

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

<sup>21</sup> 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.<sup>22</sup> 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.<sup>23</sup> 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.<sup>24</sup>

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,

<sup>22</sup> Giovanni Pitruzzella and Oreste Pollicino, *Disinformation and Hate Speech: A European Constitutional Perspective* (Bocconi University Press 2020).

<sup>23</sup> Maurizio Barberis, *Populismo digitale. Come internet sta uccidendo la democrazia* (Chiarelettere 2020).

<sup>24</sup> 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.<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup>

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.<sup>28</sup> Indeed, the uncertainty in the novel situations is a natural challenge for constitutional democracies, precisely for the principle of the rule of law.<sup>29</sup> 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

<sup>25</sup> David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001).

<sup>26</sup> *Ibid.*, Art 22.

<sup>27</sup> 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.

<sup>28</sup> Monroe E. Price, 'The Newness of Technology' (2001) 22 *Cardozo Law Review* 1885.

<sup>29</sup> 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.<sup>30</sup> As Krygier observed, it also has the goal of securing freedom from certain dangers or pathologies.<sup>31</sup> 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.<sup>32</sup> The case of *Yahoo v. Licra* is a paradigmatic example of the constitutional challenges on the horizon in the early 2000s.<sup>33</sup> More precisely, some authors have argued that regulation based on geographical boundaries is unfeasible, so that applying national laws to the Internet is impossible.<sup>34</sup> 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

<sup>30</sup> 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 Juizes Portugueses v. Tribunal de Contas*; Case C-216/18 PPU, *LM*; Case C-619/18, *Commission v. Poland* (2018).

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

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

<sup>33</sup> *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.

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



exclusively to its laws'.<sup>35</sup> In the cyber-anarchic view, the rise of internet law would cause the disintegration of state sovereignty over cyberspace,<sup>36</sup> thus potentially making any regulatory attempt irrelevant for the digital environment. This was already problematic for the principle of the rule of law, since self-regulation of cyberspace would have marginalised legal norms, de facto undermining any guarantee.

These positions have partially shown their fallacies, and scholars have underlined how States are instead available to regulate the digital environment through different modalities,<sup>37</sup> along with how to solve the problem of enforcement in the digital space.<sup>38</sup> Nonetheless, this is not the end of the story. Indeed, in recent years, new concerns have arisen as a result of the increasing economic power that some business actors acquired in the digital environment, especially online platforms. This economic power was primarily the result of the potentialities of digital technologies and of the high degree of freedom recognised by constitutional democracies in the private sector.<sup>39</sup> The shift from the world of atoms to that of bits has led to the emergence of new players acting as information gatekeepers that hold significant economic power with primary effects on individuals' everyday lives.<sup>40</sup>

Within this framework, while authoritarian States have been shown to impose their powers online,<sup>41</sup> constitutional democracies have followed another path. In this case, public actors rely on the private sector as a proxy in the digital environment.<sup>42</sup> The role of the private sector in the digitisation of the public administration or the urban environment can be considered a paradigmatic relationship of collaboration between the public and private sectors. Likewise, States usually rely on the algorithmic enforcement of individual rights online, as in the case of the removal of illegal content like terrorism or hate speech.<sup>43</sup> In other words, the intersection between public and private leads one to wonder just how to avoid that public values are subject to the determinations of private business interests. The Snowden revelations have already underlined how much governments rely on

<sup>35</sup> *Ibid.*, 1376.

<sup>36</sup> John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996) <https://www.eff.org/it/cyberspace-independence>.

<sup>37</sup> Lawrence Lessig, *Code 2.0: Code and Other Laws of Cyberspace* (Basic Books 2006); Jack Goldsmith, 'Against Cybermarchy' (1998) 65(4) *University of Chicago Law Review* 1199.

<sup>38</sup> Joel R. Reidenberg, 'States and Internet Enforcement' (2004) 1 *University of Ottawa Law & Technology Journal* 213.

<sup>39</sup> Giovanni De Gregorio, 'From Constitutional Freedoms to Power. Protecting Fundamental Rights Online in the Algorithmic Society' (2019) 11(2) *European Journal of Legal Studies* 65.

<sup>40</sup> Emily B. Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2012) 24 *International Review Law, Computers and Technology* 3.

<sup>41</sup> Giovanni De Gregorio and Nicole Stremmlau, 'Internet Shutdowns and the Limits of the Law' (2020) 14 *International Journal of Communication* 1.

<sup>42</sup> Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016) 82 *Brookling Law Review* 105.

<sup>43</sup> Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598.

Internet companies to extend their surveillance programmes and escape accountability.<sup>44</sup> Even if public actors do not act as participants in the market or a regulator, they operate through an ‘invisible handshake’ based on the cooperation between market forces and public powers.<sup>45</sup>

This situation leads constitutional democracies to adopt liberal approaches to the digital environment, with the result that self-regulation plays a predominant role. Ordo-liberal thinking considers the market and democracy as two intimate forces. Nonetheless, when market logics and dynamics based on the maximisation of profit and private business purposes prevail over the protection of individuals’ fundamental rights and freedoms, it is worth wondering about the role of regulation in mitigating this situation. The challenges raised by the implementation of artificial intelligence technologies compels to define what the proper legal framework for artificial intelligence requires. The creation of a hard law framework rather than of a soft law one is not without consequences. Both options offer a variety of benefits but also suffer from disadvantages, which should be taken into account when developing a framework for artificial intelligence systems.

Technology is also an opportunity, since it can provide better systems of enforcement of legal rules but also a clear and reliable framework compensating the fallacies of certain processes.<sup>46</sup> There is thus no definitive ‘recipe’ for protecting democratic values, but there are different means to achieve this result, among which there is also technology. Indeed, new technologies like automation should not be considered as a risk per se. The right question to ask instead is whether new technologies can encourage arbitrary public power and challenges for the rule of law.<sup>47</sup> The challenges to fundamental rights raised by these technologies would lead one to avoid approaches based on self-regulation. This strategy may not be sufficient to ensure the protection of fundamental rights in the information society. At the same time, it is well-known that hard law can represent a hurdle to innovation, leading to other drawbacks for the development of the internal market, precisely considering the global development of algorithmic technologies. In the case of the European proposal for the Artificial Intelligence Act,<sup>48</sup> the top-down approach of the Union, which aims to leave small margins to self-regulation, might be an attempt to protect the internal market from algorithmic tools which would not comply with the

<sup>44</sup> David Lyon, *Surveillance after Snowden* (Polity Press 2015).

<sup>45</sup> Niva Elkin-Koren and Micheal Birnhack, ‘The Invisible Handshake: The Reemergence of the State in the Digital Environment’ (2003) 8 *Virginia Journal of Law & Technology*.

<sup>46</sup> Steven Malby, ‘Strengthening the Rule of Law through Technology’ (2017) 43 *Commonwealth Law Bulletin* 307.

<sup>47</sup> Mireille Hildebrandt, ‘The Artificial Intelligence of European Union Law’ (2020) 21 *German Law Journal* 74.

<sup>48</sup> Proposal for Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Acts COM (2021) 206 final.

European standard of protection. Rather than making operators accountable for developing and implementing artificial intelligence systems, the regulation aims to prevent the consolidation of external standards.

Therefore, a fully harmonised approach would constitute a sound solution to provide a common framework and avoid fragmentation, which could undermine the aim of ensuring the same level of protection of fundamental rights. Besides, co-regulation in specific domains could ensure that public actors are involved in determining the values and principles underpinning the development of algorithmic technologies while leaving the private sector room to implement these technologies under the guidance of constitutional principles. The principle of the rule of law constitutes a clear guide for public actors which intend to implement technologies for public tasks and services. To avoid any effect on the trust and accountability of the public sector, consistency between the implementation of technology and the law is critical for legal certainty. Nonetheless, it is worth stressing that this is not an easy task. Even when legislation is well designed, limiting public power within the principle of legality could be difficult to achieve from different perspectives, like the lack of expertise or the limited budget to deal with the new technological scenario.<sup>49</sup> Besides, with the lack of any regulation, private actors are not required to comply with constitutional safeguards. In this case, the threats for the principle of the rule of law are different and linked to the possibility that private actors develop a set of private standards clashing with public values, precisely when their economic freedoms turn into forms of power.

The COVID-19 pandemic has highlighted the relevance of online platforms in the information society. For instance, Amazon provided deliveries during the lockdown phase, while Google and Apple offered their technology for contact-tracing apps.<sup>50</sup> These actors have played a critical role in providing services which other businesses or even the State had failed to deliver promptly. The COVID-19 crisis has led these actors to become increasingly involved in our daily lives, becoming part of our social structure.

Nonetheless, commentary has not been exclusively positive. The model of the contact-tracing app proposed by these tech giants has raised various privacy and data protection concerns.<sup>51</sup> The pandemic has also shown how artificial intelligence can affect fundamental rights online without human oversight. Once Facebook and Google sent their moderators home, the effects of these measures extended to the process of content moderation, resulting in the suspension of various accounts and the removal of some content, even though there was no

<sup>49</sup> Roger Brownsword, 'Technological Management and the Rule of Law' (2016) 8(1) *Law Innovation and Technology* 100.

<sup>50</sup> 'Privacy-Preserving Contact Tracing' *Apple.com* (accessed 30 July 2020) at [www.apple.com/covid19/contacttracing](http://www.apple.com/covid19/contacttracing).

<sup>51</sup> Jennifer Daskal and Matt Perault, 'The Apple-Google Contact Tracing System Won't Work. It Still Deserves Praise' *Slate* (22 May 2020) at <https://slate.com/technology/2020/05/apple-google-contact-tracing-app-privacy.html>.

specific reason for it.<sup>52</sup> This situation not only affected users' right to freedom of expression but also led to discriminatory results and to the spread of disinformation, thus pushing one to wonder about the roles and responsibilities of private actors in the information society.

#### 1.4 THE ROLE AND RESPONSIBILITIES OF PRIVATE ACTORS

At the advent of the digital era, the rise of new private actors could be seen merely as a matter of freedom. The primary legal (but also economic) issue thus was that of protecting such freedom while, at the same time, preventing any possible abuse thereof. This is the reason why competition law turned out to be a privileged tool in this respect,<sup>53</sup> sometimes in combination with *ex ante* regulation. Constitutional democracies have adopted a liberal approach – for instance, exempting online intermediaries from liability and providing a minimum regulation to ensure a common legal environment for circulating personal data.<sup>54</sup> Such an approach was aimed at preserving a new environment, which, at the end of the last century, seemed to promise a new phase of opportunities.

Thanks to minimum intervention in the digital environment, the technological factor played a crucial role. The mix of market and automated decision-making technologies has led to the transformation of economic freedoms into something that resembles the exercise of powers as vested in public authorities. The implementation of algorithmic technologies to process vast amounts of information and data is not exclusively a matter of profits any longer. Such a power can be observed from many different perspectives, like in the field of competition law, as economic and data power.<sup>55</sup> For the purposes of constitutional law, the concerns are instead about forms of freedoms which resemble the exercise of authority. The development of new digital and algorithmic technologies has led to the rise of new opportunities to foster freedom but also to the consolidation of powers proposing a private model of protection and governance of users. The freedom to conduct business has now turned into a new dimension, namely that of private power, which – it goes without saying – brings significant challenges to the role and tools of constitutional law.

One may actually wonder where the connection between algorithms and powers lies, apparently so far, but in fact, so close. To explain why these two expressions are connected, we argue that the implementation of the former on a large scale has the

<sup>52</sup> Elizabeth Dwoskin and Nitasha Tiku, 'Facebook Sent Home Thousands of Human Moderators due to the Coronavirus. Now the Algorithms Are in Charge' *The Washington Post* (24 March 2020) at [www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus](http://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus).

<sup>53</sup> Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016).

<sup>54</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular, electronic commerce, in the Internal Market ('Directive on electronic commerce') (2000) OJ L 178/1.

<sup>55</sup> Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Wolter Kluwer 2016).

potential to give rise to a further transmutation of the classic role of constitutionalism and constitutional theory, in addition to that already caused by the shift from the world of atoms to the world of bits,<sup>56</sup> where constitutionalism becomes ‘digital constitutionalism’ and power is relocated between different actors in the information society.<sup>57</sup> This statement needs an attempt to clarification. As is well-known, constitutional theory frames powers as historically vested in public authorities, which *by default* hold the monopoly on violence under the social contract.<sup>58</sup> It is no coincidence that constitutional law was built around the functioning of public authorities. The goal of constitutions (and thus of constitutional law) is to allocate powers between institutions and to make sure that proper limits are set to constrain their action, with a view to preventing any abuse.<sup>59</sup> In other words, the original mission of constitutionalism was to set some mechanisms to restrict government power through self-binding principles, including by providing different forms of separation of powers and constitutional review. To reach this goal, it is crucial to focus on the exploration of the most disruptive challenges which the emergence of private powers has posed to the modern constitutional state and the various policy options for facing said transformations. This requires questioning the role that constitutions play in the information society and leads one to investigate whether constitutions can and should do something in light of the emergence of new powers other than those exercised by public authorities. Our claim is that if constitutions are meant as binding on public authorities, something new has to be developed to create constraints on private actors.

Therefore, focusing on the reasons behind the shift from freedom to conduct business to private power becomes crucial to understanding the challenges for constitutional law in the algorithmic society. Private actors other than traditional public authorities are now vested with some forms of power that are no longer economic in nature. The apparently strange couple ‘power and algorithms’ does actually make sense and triggers new challenges in the specific context of democratic constitutionalism. Algorithms, as a matter of fact, allow to carry out activities of various nature that may significantly affect individuals’ rights and freedoms. Individuals may not notice that many decisions are carried out in an automated manner without, at least *prima facie*, any chance of control for them. A broad range of decision-making activities are increasingly delegated to algorithms which can advise and in some cases make decisions based on the data they process. As scholars have observed, ‘how we perceive and understand our environments and interact with them and each other is increasingly mediated by algorithms’.<sup>60</sup> In other words, algorithms are not necessarily driven by the pursuit of public interests but are instead

<sup>56</sup> Nicholas Negroponte, *Being Digital* (Alfred A. Knopf 1995).

<sup>57</sup> Giovanni De Gregorio, ‘The Rise of Digital Constitutionalism in the European Union’ (2021) *International Journal of Constitutional Law*.

<sup>58</sup> Thomas Hobbes, *The Leviathan* (1651).

<sup>59</sup> Andras Sajó and Renata Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).

<sup>60</sup> Mittlestadt et al. (n 11), 1.

sensitive to business needs. Said concerns are even more serious in light of the learning capabilities of algorithms, which – by introducing a degree of autonomy and thus unpredictability – are likely to undermine ‘accountability’ and the human understanding of the decision-making process. For instance, the opacity of algorithms is seen by scholars as a possible cause of discrimination or differentiation between individuals when it comes to activities such as profiling and scoring.<sup>61</sup>

In the lack of any regulation, the global activity of online platforms contributes to producing a para-legal environment on a global scale competing with States’ authorities. The consolidation of these areas of private power is a troubling process for democracy. Indeed, even if, at a first glance, democratic States are open environments for pluralism flourishing through fundamental rights and freedoms, at the same time their stability can be undermined when those freedoms transform into new founding powers overcoming basic principles such as the respect of the rule of law. In this situation, there is no effective form of participation or representation of citizens in determining the rules governing their community. In other words, the creation of a private legal framework outside any representative mechanism is a threat to democracy due to the marginalisation of citizens and their representatives from law-making and enforcement. This situation shows why it is important to focus on the constitutional remedies to solve the imbalances of powers in the algorithmic society.

### 1.5 CONSTITUTIONAL REMEDIES

Within this troubling framework for the protection of fundamental rights and democracies, constitutional law could provide two paths. The first concerns the possible horizontal application of fundamental rights vis-à-vis private parties. The second focuses instead on the path that could be followed in the new season of digital constitutionalism and on a constellation of new rights that could be identified to deal with the new challenges posed by algorithms.

A good starting point is Alexy’s assumption that the issue of the horizontal effect of fundamental rights protected by constitutions (and bills of rights) cannot be detached in theoretical terms from the more general issue of the direct effect of those rights.<sup>62</sup> In other words, according to the German legal theorist, once it is recognised that a fundamental right has a direct effect, that recognition must be characterised by a dual dimension. The first vertical dimension concerns the classic relationship of ‘public authority vs individual freedom’, while the second horizontal dimension focuses on the relationship between privates but also, as mentioned previously, the much less classic relationship between new private powers and individuals/users.

<sup>61</sup> Danielle K. Citron and F. Pasquale, ‘The Scored Society: Due Process for Automated Predictions’ (2014) 89 *Washington Law Review* 1; Tal Zarsky, ‘Transparent Predictions’ (2013) 4 *University of Illinois Law Review* 1507.

<sup>62</sup> Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press 2002), 570.

The problem with Alexy's assumption, which is quite convincing from a theoretical point of view, is that the shift from the Olympus of the legal theorist to the arena of the law in action risks neglecting the fact that the approach of courts from different jurisdictions might be quite different, as far as the concrete recognition of the horizontal effect of fundamental rights is concerned. This should not come as any surprise because the forms and limits of that recognition depend on the cultural and historical crucible in which a specific constitutional order is cultivated.

As far as the United States is concerned, the state action doctrine apparently precludes any possibility to apply the US Federal Bill of Rights between private parties and consequently any ability for individuals to rely on such horizontal effects, and accordingly to enforce fundamental rights vis-à-vis private actors.<sup>63</sup> The reason for this resistance to accepting any general horizontal effect to the rights protected by the US Federal Bill of Rights is obviously that the cultural and historical basis for US constitutionalism is rooted in the values of liberty, individual freedom, and private autonomy. The state action doctrine is critical to understanding the scope of the rights enshrined in the US Constitution. Indeed, were the fundamental rights protected by the US Constitution to be extended to non-public actors, this would result in an inevitable compression of the sphere of freedom of individuals and, more generally, private actors. For instance, such friction is evident when focusing on the right to free speech, which can only be directly enforced vis-à-vis public actors. Historically, the state action doctrine owes its origins to the civil rights cases, a series of rulings dating back to 1883 in which the US Supreme Court recognised the power of the US Congress to prohibit racially based discrimination by private individuals in the light of the Thirteenth and Fourteenth Amendments. Even in the area of freedom of expression, the US Supreme Court extended the scope of the First Amendment to include private actors on the grounds where they are substantially equivalent to a state actor.

In *Marsh v. Alabama*,<sup>64</sup> the US Supreme Court held that the State of Alabama had violated the First Amendment by prohibiting the distribution of religious material by members of the Jehovah's Witness community within a corporate town which, although privately owned, could be considered to perform a substantially recognisable 'public function' in spite of the fact that, formally speaking, it was privately owned. In *Amalgamated Food Emps. Union Local 590 v. Logan Valley Plaza*,<sup>65</sup> the US Supreme Court considered a shopping centre similar to the corporate town in *Marsh*. In *Jackson v. Metropolitan Edison*,<sup>66</sup> the US Supreme Court held that equivalence should be assessed in the exercise of powers traditionally reserved exclusively to the state. Nonetheless, in *Manhattan*

<sup>63</sup> Stephen Gardbaum, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102 *Michigan Law Review*, 388; Mark Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' (2003) 1 *International Journal of Constitutional Law* 79; Wilson R. Huhn, 'The State Action Doctrine and the Principle of Democratic Choice' (2006) 84 *Hofstra Law Review* 1380.

<sup>64</sup> *Marsh v. Alabama* 326 U.S. 501 (1946).

<sup>65</sup> *Amalgamated Food Emps Union Local 590 v. Logan Valley Plaza* 391 U.S. 308 (1968).

<sup>66</sup> *Jackson v. Metropolitan Edison Co* 419 U.S. 345 (1974).

*Community Access Corp. v. Halleck*,<sup>67</sup> the US Supreme Court more recently adopted a narrow approach to the state action doctrine, recalling in particular, its precedent in *Hudgens v. NLRB*.<sup>68</sup>

This narrow approach is also the standard for protecting fundamental rights in the digital domain, and consequently, the US Supreme Court seemingly restricts the possibility of enforcing the free speech protections enshrined in the First Amendment against digital platforms, as new private powers.<sup>69</sup> More specifically, and more convincingly, it has been observed by Berman that the need to call into question the implications of a radical state action doctrine<sup>70</sup> can lead, in the digital age, to the transformation of cyberspace into a totally private ‘constitution free zone’.<sup>71</sup> Balkin has recently highlighted a shift in the well-established paradigm of free speech, described as a triangle involving nation-states, private infrastructure, and speakers.<sup>72</sup> In particular, digital infrastructure companies must be regarded as governors of social spaces instead of mere conduit providers or platforms. This new scenario, in Balkin’s view, leads to a new school of speech regulation triggered by the dangers of abuse by the privatised bureaucracies that govern end-users arbitrarily and without due process and transparency; it also entails the danger of digital surveillance which facilitates manipulation.<sup>73</sup>

Despite the proposal that a ‘functional approach’ be adopted<sup>74</sup> and partial attempts to reveal the limits on fully embracing the state action doctrine in the digital age, the US Supreme Court recently confirmed in its case law the classic view of the intangibility of the state action doctrine.<sup>75</sup> However, even one of the US scholars who is more keenly aware of the de facto public functions carried out by the digital platforms concedes that

however important Facebook or Google may be to our speech environment, it seems much harder to say that they are acting like the government all but in name. It is true that one’s life may be heavily influenced by these and other large companies, but influence alone cannot be the criterion for what makes something a state actor; in that case, every employer would be a state actor, and perhaps so would nearly every family.<sup>76</sup>

<sup>67</sup> *Manhattan Community Access Corp v. Halleck* 587 U.S. \_\_\_\_ (2019).

<sup>68</sup> *Hudgens v. NLRB* 424 U.S. 507 (1976).

<sup>69</sup> Jonathan Peters, ‘The “Sovereigns of Cyberspace” and State Action: The First Amendment’s Application (or Lack Thereof) to Third-Party Platforms’ (2017) 32 *Berkeley Technology Law Journal* 989.

<sup>70</sup> Paul S. Berman, ‘Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to ‘Private’ Regulation’ (2000) 71 *University of Colorado Law Review* 1263.

<sup>71</sup> Bassini (n 42) 182.

<sup>72</sup> Jack M. Balkin, ‘Free Speech Is a Triangle’ (2012) 118 *Columbia Law Review*.

<sup>73</sup> Balkin (n 44).

<sup>74</sup> Peters (n 81) 1022–24.

<sup>75</sup> *Manhattan Community Access Corp v. Halleck* (n 79).

<sup>76</sup> Tim Wu, ‘Is first Amendment Obsolete?’ in Lee C. Bollinger and Geoffrey R. Stone (eds), *Free Speech Century* (Oxford University Press, 2019) 272.



Shifting from the United States to Europe, the relevant historical, cultural, and consequently constitutional milieu is clearly very different. The constitutional keyword is *Drittwirkung*, a legal concept originally developed in the 1950s by the German Constitutional Court,<sup>77</sup> presuming that an individual plaintiff can rely on a national bill of rights to sue another private individual alleging the violation of those rights. In other words, it can be defined as a form of horizontality in action or a total constitution.<sup>78</sup> It is a legal concept that, as mentioned, has its roots in Germany and then subsequently migrated to many other constitutional jurisdictions, exerting a strong influence even on the case law of the CJEU and ECtHR.<sup>79</sup>

It should not come as any surprise that a difference emerged between the US and European constitutional practices in regard to the recognition of horizontal effects on fundamental rights. As previously noted, individual freedom and private autonomy are not constitutionally compatible with such recognition. On the other hand, however, human dignity as a super-constitutional principle supports such recognition, at least in theory.<sup>80</sup> The very concept of the abuse of rights, which is not recognised under US constitutional law, while instead being explicitly codified in the ECHR and the EUCFR,<sup>81</sup> seems to reflect the same Euro-centric approach.

In the light of this scenario, it is no coincidence that, as early as 1976, the CJEU decided in *Defrenne II* to acknowledge and enforce the obligation for private employers (and the corresponding right of employees) to ensure equal pay for equal work, in relation to a provision of the former Treaty establishing the European Economic Community.<sup>82</sup> Article 119 of the EC Treaty was unequivocally and exclusively addressed to Member States. It provided that ‘each Member State shall ensure that the principle of *equal pay* for male and female workers for work of *equal value* is applied’. When compared to the wording of that provision, it could be observed that each provision of the EUCFR is more detailed and, therefore, more amenable to potential horizontal direct effect. It is no coincidence that, in 2014, while in *AMS* the CJEU adopted a minimalist approach to the possible horizontal direct effect only of those provisions of the EU Charter of Fundamental Rights from

<sup>77</sup> The Lüth case concerned a *querelle* about the distribution of the anti-Semitic movie “Jüdisches Leben in Deutschland” in a private location. Following the conviction, Lüth appealed to the German Constitutional Court complaining about the violation of her freedom of expression. The German Constitutional Court, therefore, addressed a question relating to the extension of constitutional rights in a private relationship. In this case, for the first time, the German court argued that constitutional rights not only constitute individual claims against the state but also constitute a set of values that apply in all areas of law by providing axiological indications to the legislative power, executive, and judicial. In the present case, the protection of freedom of expression does not only develop vertically towards the state but also horizontally since civil law rules must be interpreted according to the spirit of the German Constitution. German Constitutional Court, judgment of 15 January 1958, BVerfGE 7, 198.

<sup>78</sup> Mattias Kumm, ‘Who Is Afraid of the Total Constitution? Constitutional Rights as Principles and the Constitutionalization of Private Law’ (2006) 7(4) *German Law Journal* 341.

<sup>79</sup> *X e Y v. The Netherlands*, App no 8978/80, judgment of 26 March 1985.

<sup>80</sup> Catherine Dupré, *The Age of Dignity. Human Rights and Constitutionalism in Europe* (Hart 2016).  
<sup>81</sup> Art 17 ECHR; Art 54 EUCFR.

<sup>82</sup> Case C-43/75 *Defrenne v. Sabena* [1976] ECR 455.

which it could derive a legal right for individuals and not simply a principle, it also applied Articles 7 and 8 EUCFR in relation to the enforcement of digital privacy rights, specifically against search engines in *Google Spain*.<sup>83</sup>

Several years later, the CJEU had the opportunity to further develop the horizontal application of the EUCFR. More specifically, in four judgments from 2018 – *Egenberger*,<sup>84</sup> *IR v. JQ*,<sup>85</sup> *Bauer*,<sup>86</sup> and *Max Planck*<sup>87</sup> – the CJEU definitively clarified the horizontal scope of Articles 21, 31(2), and 47 of the EUCFR within disputes between private parties.<sup>88</sup> In the light of the emerging scenario, it seems clear that a potential initial answer to the new challenges of constitutional law in the age of new private powers could be found in the brave horizontal enforcement of fundamental rights, especially in the field of freedom of expression and privacy and data protection.

However, as mentioned previously, it is also worth reaching beyond the debate about the horizontal/vertical effects of fundamental rights in the digital age in order to suggest an alternative weapon for the challenges that will need to be faced during the new round of digital constitutionalism. Most notably, it is necessary to design a frame that describes the relationship between the three parties that Balkin puts at the heart of the information society: platforms, states, and individuals.<sup>89</sup> In other words, a digital *habeas corpus* of substantive and procedural rights should be identified, which can be enforced by the courts as they are inferred from existing rights protected under current digital constitutionalism.<sup>90</sup> Therefore, a new set of rights can be derived by such revisited understanding of individuals in the new digital context – among others, the right that decisions impacting the legal and political sphere of individuals are undertaken by human beings, and not exclusively by machines, even the most advanced and efficient ones.

The significant shift of paradigm that individuals are witnessing in their relationship with power thus requires to revisit their traditional status and to focus on a set of rights that can be enforced vis-à-vis not only governmental powers but also private actors. In particular, hard law could certainly play a role in order to remedy the lack

<sup>83</sup> *Google Spain* (n 41).

<sup>84</sup> Case C-414/16 *Vera Egenberger v. Evangelisches Werk für Diakonie und Entwicklung eV*. ECLI:EU:C:2018:257.

<sup>85</sup> Case C-68/17 *IR v. JQ*, ECLI:EU:C:2018:696.

<sup>86</sup> Joined Cases C-569/16 and C-570/16 *Stadt Wuppertal v. Maria Elisabeth Bauer and Volker Willmeroth v. Martina Broßonn*, ECLI:EU:C:2018:871.

<sup>87</sup> Case C-684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV v. Tetsuji Shimizu*, ECLI:EU:C:2018:874.

<sup>88</sup> Aurelia Colombi Ciacchi, 'The Direct Horizontal Effect of EU Fundamental Rights: ECJ 17 April 2018, Case C-414/16, *Vera Egenberger v. Evangelisches Werk für Diakonie und Entwicklung eV*. and ECJ 11 September 2018, Case C-68/17, *IR v. JQ*' (2019) 15(2) *European Constitutional Law Review* 294; Eleni Frantziou, *The Horizontal Effect of Fundamental Rights in the European Union: A Constitutional Analysis* (Oxford University Press 2019); Sonya Walkila, *Horizontal Effect of Fundamental Rights in EU Law* (Europa Law Publishing 2016).

<sup>89</sup> Jack Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 *University of California Davis* 1151.

<sup>90</sup> De Gregorio (n 56).

of fairness, transparency, and accountability which appears as the most important challenge to face in respect of the implementation of algorithmic systems. Although ensuring transparency could be complex, for multiple reasons such as trade secrets, it is possible to mitigate this issue by granting different forms of transparency and defining some procedural safeguards, which online platforms should abide by when making decisions which, otherwise, would be deprived of any public guarantee. While substantive rights concern the status of individuals as subjects of a kind of sovereign power that is no longer exclusively vested in public authorities, procedural rights stem from the expectation that individuals have of claiming and enforcing their rights before bodies other than traditional jurisdictional bodies, which employ methods different from judicial discretion, such as technological and horizontal due process. As a result of this call for algorithmic accountability, a new set of substantive and procedural rights would constitute an attempt to remedy the weakness and the transparency gap that individuals suffer from their technologically biased relationship with private actors and the lack of any bargaining power.

The right to explanation is only just one of the new rights that could contribute to mitigating the lack of fairness, transparency, and accountability in automated decision-making. Indeed, together with the right to obtain information on the way their data are being processed, individuals should also rely on a right to easy access (right to accessibility) and on a right to obtain translation from the language of technology to the language of human beings. While the former is meant as the right to be provided with the possibility to interact with algorithms and digital platforms implementing the use thereof, the latter requires the use of simple, clear, and understandable information and allows users not only to rely on, for example, the reasons for the removal of online content, but also to better exercise their rights before a judicial or administrative body.

These substantive rights find their justification in the ‘hidden price’ that individual users pay to digital platforms, while enjoying their services apparently free of charge – a cost that is not limited to personal data. Human behaviours, feelings, emotions, and political choices as well have a value for algorithms, most notably to the extent that they help machines learn something about individual reactions based on certain inputs. The new set of rights seems to respond to Pasquale’s questions about the transparency gap between users and digital platforms:

Without knowing what Google actually does when it ranks sites, we cannot assess when it is acting in good faith to help users, and when it is biasing results to favour its own commercial interests. The same goes for status updates on Facebook, trending topics on Twitter, and even network management practices at telephone and cable companies. All these are protected by laws of secrecy and technologies of obfuscation.<sup>91</sup>

<sup>91</sup> Frank Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

If, on the one hand, this new digital *pactum subjectionis* requires new rights being recognised and protected, it is also necessary to understand how their enforcement can be effective and how they can actually be put into place. This new set of substantive rights is associated with the need for certain procedural guarantees that allow individuals to ensure that these expectations can actually be met. Therefore, it is necessary to investigate also the ‘procedural counterweight’ of the creation of new substantive rights, focusing on the fairness of the process through which individuals may enforce them. Indeed, since within existing literature the focus up to date has been on the exercise of powers, there is no reason to exclude from the scope of application of procedural guarantees those situations where powers are conferred upon private bodies charged with the performance of public functions.<sup>92</sup>

Digital platforms can be said to exercise administrative powers which are normally vested in public authorities. However, looking at the way rights can be exercised vis-à-vis these new actors, vagueness and opacity can still be noticed in the relevant procedures. Among others, the right to be forgotten shows in a clear way the lack of appropriate procedural safeguards, since steps such as the evaluation of the requests of delisting and the adoption of the relevant measures (whether consisting of the removal of a link or of the confirmation of its lawfulness) entirely rely on a discretionary assessment supported by the use of algorithms. Therefore, the mere horizontal application of the fundamental right to protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights of the European Union does not prove to be satisfactory. Also, the notice and takedown mechanisms implemented by platforms hosting user-generated content and social networks do not entirely meet the requirements of transparency and fairness that make the status of users/individuals enforcing their rights vis-à-vis them comparable to the status of citizens exercising their rights against public authorities.

In order for these new substantive rights to be actually protected, and made enforceable vis-à-vis the emerging private actors, procedural rights play a pivotal role. Crawford and Schultz have explored the need to frame a ‘procedural data due process’.<sup>93</sup> The application of such a technological due process would also impact the substantive rights, as they should preserve, in accordance with the Redish and Marshall model of due process, values such as accuracy; appearance of fairness; equality of inputs; predictability, transparency, and rationality; participation; revelation; and privacy-dignity.<sup>94</sup> The due process traditional function of keeping powers separate has to be fine-tuned with the specific context of algorithms, where interactions occur between various actors (algorithm designers, adjudicators, and individuals). Citron has pointed out some requirements that automated systems

<sup>92</sup> Giacinto della Cananea, *Due Process of Law Beyond the State* (Oxford University Press 2016).

<sup>93</sup> Kate Crawford and Jason Schultz, ‘Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms’ (2014) 55 *Boston College Law Review* 93.

<sup>94</sup> Martin Redish and Lawrence Marshall, ‘Adjudicatory Independence and the Values of Procedural Due Process’ (1986) 95(3) *Yale Law Journal* 455.

should meet in order to fulfil the procedural due process, including (a) adequate notice to be given to individuals affected by the decision-making process; (b) opportunity for individuals of being heard before the decision is released; (c) and record, audits, or judicial review.<sup>95</sup> According to Crawford and Schultz's model of procedural data due process, the notice requirement can be fulfilled by providing individuals with 'an opportunity to intervene in the predictive process' and to know (i.e., to obtain an explanation about) the type of predictions and the sources of data. Besides, the right to being heard is seen as a tool for ensuring that once data are disclosed, individuals have a chance to challenge the fairness of the predictive process. The right to being heard thus implies having access to a computer program's source code, or to the logic of a computer program's decision. Lastly, this model requires guarantees of impartiality of the 'adjudicator', including judicial review, to ensure that individuals do not suffer from any bias while being subject to predictive decisions.

The proposal for the Digital Services Act provides an example of these procedural safeguards limiting platforms' powers.<sup>96</sup> With the goal of defining a path towards the digital age, the proposal maintains the rules of liability for online intermediaries, now established as the foundation of the digital economy and instrumental to the protection of fundamental rights. In fact, based on the proposal, there will no changes in the liability system but rather some additions which aim to increase the level of transparency and accountability of online platforms. It is no coincidence that, among the proposed measures, the DSA introduces new obligations of due diligence and transparency with particular reference to the procedure of notice and takedown and redress mechanisms.

## 1.6 CONCLUSIONS

Algorithmic systems have contributed to the introduction of new paths for innovation, thus producing positive effects for society as a whole, including fundamental rights and freedoms. Technology is also an opportunity for constitutional democracies. Artificial intelligence can provide better systems of enforcement of legal rules or improve the performance of public services. Nonetheless, the domain of inscrutable algorithms characterising contemporary society challenges the protection of fundamental rights and democratic values while encouraging lawmakers to find a regulatory framework balancing risk and innovation, considering the role and responsibilities of private actors in the algorithmic society.

The challenges raised by artificial intelligence technologies are not limited to freedom of expression, privacy, and data protection. Constitutional democracies

<sup>95</sup> Danielle K. Citron, 'Technological Due Process' (2008) 85(6) *Washington University Law Review* 1249.

<sup>96</sup> Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) COM (2020) 842 final.

are under pressure to ensure legal certainty and predictability of automated decision-making processes which can collectively affect democratic values. Individuals are increasingly surrounded by ubiquitous systems that do not always ensure the possibility of understanding and controlling their underlying technologies. Leaving algorithms without any safeguards would mean opening the way towards techno-determinism, allowing the actors who govern these automated systems to arbitrarily determine the standard of protection of rights and freedoms at a transnational level under the logics of digital capitalism. This is why it is critical to understand the role of regulation in the field of artificial intelligence, where cooperative efforts between the public and private sector could lead to a balanced approach between risk and innovation. Constitutional democracies cannot leave private actors to acquire areas of power outside constitutional limits.

Within this framework, both the horizontal effect doctrines and new substantive and procedural rights seem to be promising candidates among the available remedies. In the face of these challenges, it is likely that *ius dicere* will by no means lose its predominant role over political power acquired in recent years. The challenges raised by new automated technologies are likely to operate as a call for courts to protect fundamental rights in the information society while increasing pressures on lawmakers to adopt new rights and safeguards.<sup>97</sup> It is conceivable that, despite the codification of new safeguards, the role of courts in interpreting the challenges raised by new technologies is far from being exhausted, also due to the role of online platforms. Indeed, artificial intelligence technologies have raised different questions concerning the protection of fundamental rights, which still have not been answered through the political process. We have seen how constitutional law can provide some solutions to these new challenges. Nonetheless, in the absence of any form of regulation, the role of courts is likely to be predominant. The COVID-19 pandemic has only amplified this dynamic. It has confirmed the role of legislative inertia in the face of the new challenges associated with the implementation of technology and the increasing role of online platforms in providing services and new solutions to combat the global pandemic.

Therefore, the primary challenge for constitutional democracies in the algorithmic society might be to limit the rise of global private powers replacing democratic values with private determinations. This does not entail intervening in the market or adopting a liberal approach, but involves defining a constitutional framework where public and private powers are bound by safeguards and procedures.

<sup>97</sup> Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?* (Hart 2021).