



EUROPEAN COURT OF HUMAN RIGHTS

COUR EUROPÉENNE DES DROITS DE L'HOMME

**Digital Private Powers Exercising Public Functions:
The Constitutional Paradox in the Digital Age and its Possible Solutions**

by Oreste Pollicino*

(Early Draft)

Abstract: It is increasingly evident that, in the digital context, the principles underlying the rule of law are under stress. The presentation will start from one of the cornerstones of the principle of the rule of law and of constitutional law, how limiting the new forms of private power that compete with public powers, moving from the Trump's social media silencing in the United States to the Facebook's decision in Australia to ban news services and also to the complex system of enforcement of the right to be forgotten in Europe. How to deal with these constitutional short circuits? What common ground can be found by looking at the new perspectives of digital constitutionalism?

Summary

1. Introduction.
2. Rule of law in Digital Transition.
3. Information Private Powers.
4. Constitutional Remedies and Regulatory Approaches.
 - 4.1 Horizontal Application of Fundamental Rights.
 - 4.2 Procedural Safeguards.
5. Conclusions.

1. Introduction

In January 2021, Twitter decided to block the account of the former President Donald Trump in the aftermath of the violent conflict at the Capitol driven by the Trump's statements inciting reactions against the US political situation. Just one month later, Facebook banned Australian publishers and users from sharing or viewing Australian as well as international news content. Then, just a couple of days later, the social media changed its view, once the Australian government decided to step back and negotiate with Facebook the News Media and Digital Platforms Mandatory Bargaining Code which would require force Google and Facebook to negotiate with news publishers, pay for news, share data and advertising revenues. Besides, the Government of India's request to Twitter to block more than a thousand accounts supportive of farmers' protests led the social media to comply with this public order.

There are different ways to look at this sequence of events. These cases show how platforms have consolidated their role of gatekeepers over information globally. Facebook's (temporary) choice to limit news in Australia or the Twitter's choice to ban the presidential account or shutdown content in India are not just business decisions, reflecting platform's economic freedoms and business purposes. They represent the exercise of functions reflecting those of

public authorities, thus, showing how powers are relocated among different actors in the information society, within the push towards a new phase of digital constitutionalism.¹

The principle of rule of law has not been spared in this process of rethinking (but not transforming) traditional categories in lights of the technological factor. It remains, in the words of President Robert Spano, a lodestar,² both in the offline and online world. According to President Spano, ‘the foundational moral idea behind the rule of law, which lies at the core of Convention protections, is the respect for personal autonomy and the exclusion of the arbitrary use of governmental power’.³ He continues stating that ‘[t]he law must be transparent, stable, foreseeable and allow for mechanisms of dispute resolution that are independent and impartial. Moreover, law must not only apply to the people, but also, and even more crucially, to those that hold the reins of power at any given moment’.⁴

The rule of law has a direct impact on the life of every citizen: it is a precondition for ensuring equal treatment before the law, protecting fundamental and legal rights, preventing abuse of power by public authorities and holding decision-making bodies accountable.⁵ In other words, the rule of law can be seen as an instrument to measure the degree of accountability, the fairness of application and effectiveness of the law.⁶ As Krygier observed, it is also a goal of freedoms from certain dangers or pathologies.⁷ 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 ensure that these limit answer to a common constitutional scheme.

The principle of the rule of law indeed constitutes a clear guide for public actors which intends to implement technologies for public tasks and services. To avoid any effect on trust and accountability of the public sector, consistency between the implementation of technology and the law is critical for the principle of the rule of law. 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.⁸ New technological development has always led to the dilemma

*Professor of Constitutional Law, Bocconi University, Milan and member of the Executive Board, European Agency for Fundamental Rights, Vienna

¹ Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Toward Digital Constitutionalism?* forthcoming, (Hart 2021); Giovanni De Gregorio, ‘The Rise of Digital Constitutionalism in the European Union’ *International Journal of Constitutional Law*, 2021.

² Robert Spano, ‘The Rule of Law as the Lodestar of the European Convention on Human Rights: The Strasbourg Court and the Independence of the Judiciary’ (2021) *European Law Journal*.

³ *Ibid.*, 3.

⁴ *Ibid.*

⁵ Jeremy Waldron, ‘The Concept and the Rule of Law’ (2008) 43(1) *Georgia Law Review* 1.

⁶ 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).

⁷ Martin Krygier, ‘The Rule of Law: Legality, Teleology, Sociology’ in Gianluigi Palombilla and Neil Walker (ed), *Relocating the Rule of Law* (Hart 2009), 45

⁸ Roger Brownsword, ‘Technological management and the Rule of Law’ (2016) 8(1) *Law Innovation and Technology* 100.

between risk and opportunity fostered by its newness.⁹ The uncertainty in the novelties is a natural challenge for the rule of law due to the increasing degree of uncertainty concerning the applicable legal framework and the exercise of power which can exploit technologies based on legal loopholes.¹⁰

Nonetheless, if the principle of the rule of law would constitute a paradigmatic limit in relation to public powers at least *in abstracto*, the same consideration could not be extended to private entities which in the lack of regulation are not always required to comply with constitutional safeguards. In this case, the threats for the said principle different and linked to the possibility that private actors develop a set of private standards which clashes with public values, precisely when their economic freedoms turn into forms of power. This is evident when focusing on how information flows online and the characteristic of the public sphere which is increasingly personalised rather than plural.¹¹ 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 whose transparency and accountability cannot be ensured.¹²

In this context, the rule of law is under pressure from multiple sides. However, technology is also an opportunity for the rule of law since it can provide better systems of enforcement of legal rules but also a clear and reliable framework compensating the fallacies of certain processes.¹³ Therefore, there is no definitive 'recipe' for protecting public 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 the challenges for the rule of law.¹⁴

I believe that potential answers to address this situation can be found by looking at constitutional law and at the roots of constitutionalism whose genetical code tends to limit public (and more precisely governmental) powers, thus, protecting individuals against any abuse by the state. Against this framework, the shift of power from public to private hands requires rethinking and, in case, revisiting some well-established constitutional assumptions. Therefore, this work aims to examine the challenges for the rule of law coming from digital private powers. The primary goal of this work is to define the potential remedies to this situation from a constitutional law perspective. The first part of the work describes the challenges of the rule of law in the shift from the world of atoms to the worlds of bits. The second part examines the exercise of private information power. The third part analyses the constitutional instruments to address this situation, especially when we look at the horizontal application of fundamental rights and the introduction of new rights as procedural safeguards.

⁹ Monroe E. Price, 'The Newness of Technology' (2001) 22 *Cardozo Law Review* 1885.

¹⁰ 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.

¹¹ Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4(3) *Social Media + Society*.

¹² 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.

¹³ Steven Malby, 'Strengthening the rule of law through technology' (2017) 43 *Commonwealth Law Bulletin* 307.

¹⁴ Mireille Hildebrandt, 'The Artificial Intelligence of European Union Law' (2020) 21 *German Law Journal* 74.

2. Rule of Law in Digital Transition

It has been already outlined principle of the rule of law is under pressure in the information society. Nonetheless, it would be a mistake considering the technological factor as the only source of concern in question.¹⁵ Nonetheless, the technological factor exacerbates and amplifies this troubling situation for the Union. Since the advent of the Internet at the end of the last century, we have been used to rethink categories in the lights of digital technologies. It is not by chance that the debate started questioning consolidated notions like sovereignty and territory.¹⁶ The case *Yahoo v. Licra* is a paradigmatic example of the new challenges on the horizon of that time.¹⁷ More precisely, some authors have argued that regulation based on geographical boundaries was infeasible so that applying national laws to the Internet was therefore impossible.¹⁸ Precisely, Johnson and Post 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 exclusively to its laws’.¹⁹ In the cyber-anarchic view, the rise of Internet law would have caused the disintegration of state sovereignty over cyberspace, thus, potentially making any regulatory attempt irrelevant for the digital environment. This was already problematic for the principle of the rule of law since the self-regulation of the cyberspace would have marginalized legal norms *de facto* undermining any guarantee.

These positions have partially shown their fallacies and scholars underlined how States are instead available to regulate the digital environment through different modalities,²⁰ and how to solve the problem of enforcement in the digital space.²¹ Nonetheless, this was not the end of the story. Indeed, over these years, new concerns raised as results of the increasing areas of 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 new digital technologies and the high degree of freedom recognized by constitutional democracies

¹⁵ See, in particular, Wojciech Sadurski, *Poland Constitutional Breakdown* (Oxford University Press 2019); Gabor Halmai, ‘A Coup Against Constitutional Democracy: The Case of Hungary’ in Mark A. Graber et al, *Constitutional Democracy in Crisis?* (Oxford University Press 2018). See also Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening the Rule of Law within the Union. A Blueprint for Action COM(2019) 343 final.

¹⁶ John P Barlow, ‘A Declaration of Independence of the Cyberspace’ (Electronic Frontier Foundation, 1996) <www EFF.org/cyberspace-independence>.

¹⁷ *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.

¹⁸ David R Johnson and David Post, ‘Law and Borders: The Rise of Law in Cyberspace’ (1996) 48(5) *Stanford Law Review* 1371.

¹⁹ *Ibid*, 1376.

²⁰ Lawrence Lessig, *Code 2.0: Code and Other Laws of Cyberspace* (Basic Books 2006).

²¹ Joel R Reidenberg, ‘States and Internet enforcement’ (2004) 1 *University of Ottawa Law & Technology Journal* 213.

to the private sector.²² The shift from the world of atoms to the world of bit has led to the emergence of unknown players acting as information gatekeepers that hold significant economic power with primary effects on individuals' everyday life.²³

At the advent of the digital era, the emergence of these new actors could be seen merely as a matter of freedom to conduct business. The main legal (but also economic) issue, thus, was protecting such freedom while, at the same time, preventing any possible abuse of the same. This is the reason why competition law turned out to be a privileged tool in this respect,²⁴ sometimes in combination with *ex ante* regulation. The Union has limited its approach to the e-Commerce Directive which has only laid down liability exemptions for illegal content applicable to Internet service providers with a view to facilitating the flourishing of these services and the flow of content.²⁵ Therefore, the e-Commerce Directive encapsulates the approach that inspired lawmakers and regulators (most notably in the United States) at the time of the rise of the Internet: *minimum* regulation, that aimed at preserving freedom to conduct business (while not burdening Internet service providers in connection with third party illegal content) while preventing abuses of the same (in case Internet service providers exercised editorial responsibility instead of being merely neutral and passive vis-à-vis content).

Thanks to minimum intervention in the digital environment, the technological factor played a crucial role once again. In the meantime, the development of algorithmic technologies to process and gained profit from the vast amount of information and data. Nonetheless, it is not exclusively a matter of profits any longer. The mix of market and automated decision-making technologies has led to the transformation of economic freedoms into something that is resembling the exercise of powers as vested in public authorities.²⁶ Such a power can be observed from many different perspectives like in the field of competition law as economic and data power.²⁷

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 fostering freedoms but also to the consolidation of powers threatening the principle of the rule of law due to its ability to propose a private model of protection and users' governance.²⁸ Beyond public powers, the freedom of conduct business has now turned into a new dimension, namely that of private power, which –

²² 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.

²³ Emily B. Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2012) 24(3) International Review Law, Computers and Technology.

²⁴ Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016).

²⁵ 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.

²⁶ Giovanni De Gregorio, 'From Constitutional Freedoms to the Power of the Platforms: Protection Fundamental Rights Online in the Algorithmic Society' (2019) 12 European Journal of Legal Studies 65.

²⁷ Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Wolter Kluwer 2016).

²⁸ Oreste Pollicino and Giovanni De Gregorio, 'Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics' IACL Democracy Roundtable (11 November 2020) <<https://www.iacl-democracy-2020.org/blog/2016/3/23/blog-post-sample-9wntn-6ye75-hwawc-47gsl-5ymrn>>.

it goes without saying – brings significant challenges to the role and tools of constitutional law. It is indeed important to focus on the reasons behind the shift from freedom to conduct business to private power. The most important reason seems to lie with the implementation of algorithms on a large scale by the emerging private actors. As a consequence, private actors other than the traditional public authorities are now vested with some forms of power, that is no longer of merely economic nature.

The apparently strange couple ‘power and algorithms’ does actually make sense and triggers new challenges in the specific context of the rule of law. Algorithms, in fact, permit 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.²⁹ As scholars observed, ‘how we perceive and understand our environments and interact with them and each other is increasingly mediated by algorithms’.³⁰ In other words, algorithms are not necessarily driven by the pursuit of public interests, being instead 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.³¹

One may actually wonder where lies the connection between algorithms and powers, apparently so far, in effect so close. To explain why these two expressions are put in connection, we would argue that the implementation of the latter on a large scale has the 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.³²

The statement needs an attempt of clarification. As it 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.³³ It is no coincidence that constitutional law has been built around the functioning of public authorities. The goal of constitutions (and thus of constitutional law) is to allocate powers among institutions and to make sure that proper limits are set on the same, with a view to preventing any abuse.³⁴ In other words, the original mission of constitutionalism is to set some mechanisms to restrict government power through self-

²⁹ Brent D. Mittlestadt et al., ‘The Ethics of Algorithms: Mapping the Debate’ (2016) 3(2) *Big Data & Society*.

³⁰ *Ibid.* 1.

³¹ 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.

³² Nicholas Negroponte, *Being Digital* (Alfred A Knopf 1995).

³³ Thomas Hobbes, *The Leviathan* (1651).

³⁴ Andras Sajó and Renata Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).

binding principles, including by providing different forms of separation of powers and constitutional review.

To reach its goal, it is crucial focusing 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 to face said transformations. This requires questioning the role that constitutions play in the information society and leads to investigate whether constitutions can and must do something in respect of the emergence of new powers other than those exercised by public authorities: my 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, the challenges at stake involve broadly 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 whose boundaries of protection are increasingly shaped and determined by machines.

3. Information Private Powers

The sequence of events in the introduction provides paradigmatic examples of how online platforms can exercise powers mirroring state authority. In particular, looking at how information is governed online, it is possible to understand how the technological factor raises primary challenges to the principle of the rule of law.

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 considering 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.³⁵ This however does not imply that threats have not appeared on the horizon. On the opposite, the implementation of automated decisions-making systems is concerning when focusing on the protection of the right to freedom of expression online. Even before the rise and spread of artificial intelligence technologies in the last years, European courts, especially the European Court of Human Rights, has underlined the threats that the digital environment raised for protection for freedom of expression.³⁶

At first glance, the characteristics of the Internet would not raise any risk for pluralism which was originally concerned about scarcity of resources. Indeed, in the atomic world, one of the priorities in the media sector is to protect pluralism of information. On the internet, legal rules (and especially public law) should take a step back in the name of the alleged self-corrective capacity of the information market. Nonetheless, the digital environment has challenged media pluralism.³⁷ Indeed, a general liberal approach does not convince, in our opinion, for at least three reasons.

³⁵ Yochai Benkler, *The Wealth of Networks* (Yale University Press 2006).

³⁶ Oreste Pollicino, 'Judicial Protection of Fundamental Rights in the Transition from the World of Atoms to the Word of Bits: The Case of Freedom of Speech' (2019) 25 *European Law Journal* 155.

³⁷ Peggy Valcke et al. (eds), *Media Pluralism and Diversity: Concepts, Risks and Global Trend* (Springer 2015).

First of all, the problem of scarcity should not be seen from a technical perspective but a human standpoint. If it is true that the problem of scarcity of technical resources is not affecting the internet, the attention and the time available continue to be a scarce 'product'. In fact, while the amount of information available is growing, the hours per day could not be amplified. Against this background, in this information overload the user temptation will be to search for news, information and ideas which enhance their previous thoughts and preference, bringing to the group polarization process quite well described by Sunstein.³⁸ In other words, in the world of bits, much more than in the world of atoms, deliberation tends to move groups, and the individuals who compose them, toward a more extreme point in the direction indicated by their own judgments. Paradoxically, the Internet, despite (or better, maybe, exactly because of) the unlimited amount of information, there is a less pluralistic exchange of different opinions than in the traditional media where still exist the scarcity of sources issue. 'Filter bubbles' or 'echo chambers' expose users to opinions they already agree with and never come across challenging content.³⁹

The situation is indeed the result of the technological factors. The rise of the Internet and new digital services based on artificial intelligence technologies has changed the public sphere. The increasing implementation of these technologies by private actors like search engine and social networks led to wondering how and to what extent automated decision-making technologies affect (or even determine) the paradigm of protection of the right to freedom of expression online. This is not a neutral activity for the principle of the rule of law. The set of a global private standard of protection tends to create a hybrid paradigm of protection no matter whether legal orders require or safeguard across the globe.

These considerations could be extended even beyond the field of the right to be forgotten online. It would be enough focusing on social media like Facebook or YouTube to understand how freedom of expression and artificial intelligence are intertwined in the information society.⁴⁰ Indeed, to organise and moderate billions of content each day, platforms also rely on artificial intelligence to decide whether to remove content or signal some expressions to human moderators.⁴¹

The result of this environment is troubling for the rule of law from different perspectives. Firstly, artificial intelligence systems contribute to interpreting legal protection of fundamental rights by *de facto* setting a private standard of protection in the digital environment.⁴² Secondly, 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.⁴³ In

³⁸ Cass Sunstein, *Republic.com 2.0* (Princeton University Press 2007).

³⁹ Eli Pariser, *The Filter Bubble* (Penguin 2011).

⁴⁰ Jack M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 UC Davis Law Review 1149.

⁴¹ Tarleton Gillespie, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (Yale University Press 2018).

⁴² Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598.

⁴³ Giovanni De Gregorio, 'Democratising Content Moderation. A Constitutional Framework' (2019) Computer Law and Security Review.

other words, the challenge in this case is to measure the compliance with the principle of the rule of law. Indeed, the implementation of machine learning technologies does not allow to scrutinise decisions over expressions which are still private but involving the public at large. In the lack of regulation of legal safeguards, online platform will continue to be free to assess and remove speech according to their business purposes.

To understand when automation meets (and influence) free speech, it would be enough to closely look at the way in which information flows online. An example can provide insights on this situation: the enforcement of the right to be forgotten online. Indeed, search engines rely on automated decision-making systems helping to organize and delist the vast amount of link they host. These private (and automated) determination leads to balancing the right to data protection with other fundamental rights, especially the right to freedom of expression. In the landmark decision of the ECJ in the *Google Spain* case,⁴⁴ the main question raised by the domestic judge was whether a search engine could be required by a data protection authority to remove links to old or non-accurate personal data without prior consultation with the owner of the relevant website from which the data are indexed.

Even if, at first glance, the answers of the Advocate General and the ECJ were focused on the field of data protection, nevertheless, the same question could be looked from a different angle focusing on whether there is a right to have personal data available on a website covered by free speech. As observed by the Advocate General observed, ‘making content available on the internet counts as such as use of freedom of expression, even more so when the publisher has linked his page to other pages and has not limited its indexing or archiving by search engines, thereby indicating his wish for wide dissemination of content’.⁴⁵ Although the Advocate General considered the implementation of a notice and take-down procedure based on individuals’ subject data complaints as a measure which would undermine the freedom of expression of the search engine, the ECJ required search engines to delist information based on data subjects’ request.

This decision has recognised the role of a private actor (power?) managing a search engine to be the (almost) final arbiter between two contrasting rights (privacy vs right to be informed)Indeed, outside any safeguard and by implementing automated systems, Google enjoys broad margins of discretion in deciding whether to delist information. This private activity hides a public functioning consisting of the balancing and enforcing of fundamental rights online.⁴⁶ Indeed, when the search engine receives the notice of the data subject is required to decide whether to hold or dismiss the request. In order to do so, search engines perform a balancing activity between the interests at stake.

A strange and very disturbing process of privatization of the rule of law principle the digital context.

⁴⁴ Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014). See Orla Lynskey, ‘Control over personal data in a digital age: *Google Spain v AEPD and Mario Costeja Gonzalez*’ (2015) 78 *Modern Law Review* 522.

⁴⁵ Opinion of the Advocate General in C-131/12, 122.

⁴⁶ Marco Bassini, ‘Fundamental Rights and Private Enforcement in the Digital Age’ 25(2) *European Law Journal* 182.

4. Constitutional Remedies and Regulatory Approaches

Within this troubling framework, the primary question is about the scope of constitutional remedies limiting the threats to the principle of the rule of law in the information society. From a constitutional perspective, it is not just relevant defining the adequate legal framework for artificial intelligence technologies. It is even more important to limit the exercise of autonomous public and private powers undermining the protection of fundamental rights and freedoms. Two possible remedies can be identified. 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 phase of digital constitutionalism, precisely exploring a constellation of new rights to deal with the new challenge raised by artificial intelligence technologies.

4.1 Horizontal Application of Fundamental Rights

It is evident that, in order to understand the feasibility of such remedies in the context of new digital challenges, it is important to take a step back and to explore briefly the theoretical foundations of the issue. A good starting point could be the 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 the same rights.⁴⁷ In other words, according to the German legal theorist, once it is recognised that a fundamental right has 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 above, the much less classic relationship between new private powers and individuals/users.

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 US 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

⁴⁷ Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press 2002).

vis-à-vis private actors.⁴⁸ 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. 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. If 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.

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*⁴⁹ 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*,⁵⁰ the US Supreme Court considered a shopping centre similar to the corporate town in *Marsh*. In *Jackson v Metropolitan Edison*,⁵¹ the US Supreme Court held that equivalence should be assessed in the exercise of powers traditionally reserved exclusively to the state. Nonetheless, as noted in Chapter 4, in *Manhattan Community Access Corp v Halleck*,⁵² the US Supreme Court more recently adopted a narrow approach to the state action doctrine, recalling in particular its precedent in *Hudgens v NLRB*.⁵³

This narrow approach is also the standard for protecting fundamental rights in the digital domain and, consequently, the US Supreme Court would seem to restrict the possibility to enforce the free speech protection enshrined in the First Amendment against digital platforms, as new private powers.⁵⁴ As observed by Berman, the need to call into question the implications of a radical state action doctrine can lead, in the digital age, to the transformation of cyberspace into a totally private constitution free zone.⁵⁵ 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.⁵⁶ Precisely, digital infrastructure companies must be regarded as governors of social spaces instead of mere conduit providers or platforms. This new scenario,

⁴⁸ 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.

⁴⁹ *Marsh v Alabama* 326 US 501 (1946).

⁵⁰ *Amalgamated Food Emps Union Local 590 v Logan Valley Plaza* 391 US 308 (1968).

⁵¹ *Jackson v Metropolitan Edison Co* 419 US 345 (1974).

⁵² *Manhattan Community Access Corp v Halleck* 587 US ____ (2019).

⁵³ *Hudgens v NLRB* 424 US 507 (1976).

⁵⁴ 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.

⁵⁵ 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.

⁵⁶ Jack M Balkin, 'Free Speech Is a Triangle' (2018) 118 Columbia Law Review 2011.

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 a danger of digital surveillance that facilitates manipulation.⁵⁷

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.⁵⁸ 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.⁵⁹

Shifting from the US 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,⁶⁰ which presumes 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.⁶¹ 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.⁶²

It should not come as any surprise that a difference emerged between US and European constitutional practice as regards the recognition of horizontal effect to fundamental rights. As noted above, 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.⁶³ 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,⁶⁴ seems to reflect the same Euro-centric approach.

⁵⁷ Jack M Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296.

⁵⁸ 587 US ____.

⁵⁹ Tim Wu, 'Is the First Amendment Obsolete?' in Lee C Bollinger and Geoffrey R Stone (eds), *Free Speech Century* (Oxford University Press 2019) 272.

⁶⁰ The *Lüth* case concerned a *querelle* about the distribution of the anti-Semitic movie *Jüd Jüss* in a private location. Following the conviction, Lüth appealed to the German Constitutional Court complaining of 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 develops not only 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.

⁶¹ 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.

⁶² *X and Y v The Netherlands*, App no 8978/80, Judgment of 26 March 1985.

⁶³ Catherine Dupré, *The Age of Dignity. Human Rights and Constitutionalism in Europe* (Hart 2016).

⁶⁴ European Convention on Human Rights (1950), Art 17; Charter of Fundamental Rights of the European Union (2012) OJ C 326/391, Art 54.

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.⁶⁵ Article 119 of the EC Treaty was unequivocally and exclusively addressed at the 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 EUCFR from 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*.

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*,⁶⁶ *IR v JQ*,⁶⁷ *Bauer*,⁶⁸ and *Max Planck*⁶⁹—the CJEU definitively clarified the horizontal scope of Articles 21, 31(2) and 47 EUCFR within disputes between private parties.⁷⁰ In the light of the emerging scenario, it seems clear that a potential initial answer to the new challenges for 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 above, it is also worth reaching beyond the debate on horizontal/vertical effects of fundamental rights in the digital age in order to propose an alternative weapon consisting of a digital *habeas corpus* of substantive and procedural rights. 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 to claim and enforce their rights before bodies other than traditional jurisdictional bodies, which employ methods different from judicial discretion, such as technological and horizontal due process. Another potential option could focus on whether human dignity characterising European constitutionalism can be enforced as ‘counter-limit’ that, regardless of any horizontal/vertical effect, is likely to create sufficient constraints even for private actors, as the *Omega* case delivered by the Court of Justice seems to demonstrate.

⁶⁵ Case C-43/75 *Defrenne v Sabena* (1976) ECR 455.

⁶⁶ Case C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV*, ECLI:EU:C:2018:257.

⁶⁷ Case C-68/17 *IR v JQ*, ECLI:EU:C:2018:696.

⁶⁸ 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.

⁶⁹ Case C-684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV v Tetsuji Shimizu*, ECLI:EU:C:2018:874.

⁷⁰ 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 e.V.* 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).

Also, the judgment in Google Spain has paved the way to a new paradigm for framing fundamental rights protection in the digital realm. Whereas the decision, on one hand, attached to private actors, namely search engine providers, the task of balancing freedom of information and data protection, on the other one, it seems to imply that human dignity is (and has to remain) the cornerstone of the balance of interests. Dignity can be, thus, enforced as a limit to the exercise of freedom to conduct business, with a view to preventing that the shifting from freedom to power leads to any abuse by private actors. A new set of fundamental rights can be derived by the protection of human dignity: more broadly, a 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, and provided that minimum safeguards are protected.

4.2 Procedural Safeguards

With regard to new rights, consideration should be given at least to the right to explanation (meaning the right of an individual to obtain information about the way his/her data are being processed) together with the right to easy access (right to accessibility) and the right to obtain a translation from the language of technology into the language of human beings. While the first of these rights is meant as the right to be allowed the opportunity to interact with algorithms, the right to easy access requires that simple, clear and understandable information be used; moreover, it entitles users to receive not only the reasons, for example, for the removal of online content, but also to exercise their rights more effectively before a judicial or administrative body.

Both rights already have constitutional roots in the existing framework for the protection of fundamental rights, which clearly starts from a theological and technology-oriented interpretation of Article 10 ECHR, Article 11 EUCFR and the First Amendment of the US Constitution. If some basis within constitutional theory is sought, this gap can perhaps be filled or reduced by leveraging the value of human dignity as a cornerstone of human rights protection. If this holds true, a new set of fundamental rights can be derived from the protection of human dignity: more broadly, a right that decisions impacting the legal and political sphere of individuals be made by human beings and not exclusively by machines, even the most advanced and efficient ones, and a requirement that minimum safeguards be protected.

However, these rights, and more specifically the right to explanation, can establish another solid constitutional root in the right to data protection as enshrined in the EUCFR and in the GDPR. As mentioned above, the GDPR introduces, *inter alia*, a new safeguard guaranteeing individuals the right not to be subject to a decision taken by a machine based on the processing of their data, including profiling, that results in legal consequences for them. Regardless of whether the GDPR already provides grounds for such a right to explanation to be enforced, the assumption is that the time is ripe for a new *pactum subjectionis*. Due to the significant shift that individuals are witnessing in their relationship with power, it is necessary to revisit their status and to focus on a set of rights that can be enforced vis-à-vis not only governmental powers, but also private actors.

The assumption here is that these substantive rights are justified by the hidden price that individual users pay to digital platforms while enjoying their service apparently free of charge, a cost that is not limited to personal data. Moreover, from an anthropological perspective, human behaviour, feelings, emotions and political choices have a value for algorithms, most notably insofar as they help machines to learn something about individuals' reactions based on a certain input. The new catalogue of rights seems to respond to the questions concerning the transparency gap between users and digital platforms. According to Pasquale, 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.⁷¹

If, on the one hand, this new digital *pactum subjectionis* requires new rights to be recognised and protected, it is also necessary to understand how their enforcement can be effective, how they can actually be put into practice. In other words, it is necessary to couple the claim for a new catalogue of substantive rights with the need for certain procedural guarantees that allow individuals to ensure that these 'quasi-legal' expectations can actually be met. Therefore, it is necessary to speculate also on the 'procedural counterweight' to the creation of new substantive rights, focusing on the fairness of the process by which individuals can enforce them. In fact, since speculation has hitherto focused on the exercise of powers, there is no reason to exclude from the scope of procedural guarantees those situations in which powers are vested in private bodies charged with the performance of certain public functions.⁷²

Digital platforms can be said to exercise administrative powers that are normally vested in public authorities. However, considering how rights can be exercised vis-à-vis these new actors, vagueness and opacity can still be discerned within the relevant procedures. Among others, the right to be forgotten clearly shows the lack of appropriate procedural safeguards, since steps such as the evaluation of a delisting request and the adoption of the relevant measures (whether consisting of the removal of a link or confirming that it is lawful) rely on an entirely discretionary assessment, supported by the use of algorithms. Therefore, the merely horizontal application to the fundamental right to data protection does not prove to be satisfactory. Moreover, the notification and take down mechanisms implemented by platforms hosting user-generated content do not entirely fulfil the requirements of transparency and fairness so as to render the status of the user/individual enforcing his/her rights vis-à-vis these platforms comparable to the status of citizens exercising their rights against public authorities. It is argued that the time is ripe for filling this gap.

Procedural rights will play a pivotal role in ensuring that these new substantive rights are actually protected and rendered enforceable vis-à-vis emerging private actors. Within the context of research into big data and predictive privacy violations (including those caused by the use of predictive algorithms), Crawford and Schultz have stressed the need to frame a form

⁷¹ Pasquale (n), 9.

⁷² Giacinto della Cananea, *Due Process of Law Beyond the State* (Oxford University Press, 2016).

of ‘procedural data due process’.⁷³ The application of such a form of technological due process would also have an impact on substantive rights as the same should preserve, in accordance with the Redish and Marshall model of due process, values such as accuracy; the appearance of fairness; equality of inputs; predictability, transparency and rationality; participation; revelation; and privacy-dignity.⁷⁴ The traditional function of due process of keeping powers separate must be fine-tuned to the specific context of algorithms, where interactions occur between various actors (algorithm designers, adjudicators and individuals). Citron has pointed out some of the requirements that automated systems should meet to fulfil procedural due process requirements, including the adequate notice to be given to individuals affected by the decision-making process; the opportunity for individuals to be heard before the decision is released; and the record, audits or judicial review.⁷⁵ According to Crawford and Schultz,⁷⁶ the requirement of notice can be fulfilled by providing individuals with ‘an opportunity to intervene in the predictive process’ and to know about (ie to obtain an explanation concerning) the type of predictions and the sources of data. On the other hand, the right to be heard is seen as a tool for ensuring that, once data are disclosed, individuals have the opportunity to challenge the fairness of the predictive process. The right to be heard thus implies having access to a computer program’s source code or to the logic on which a computer program’s decision is based. Finally, this model requires guarantees of the impartiality of the ‘adjudicator’, including judicial review, in order to ensure that individuals do not suffer from any bias when subject to predictive decisions.

In the European context, some of these procedural safeguards limiting platform’s power are coming to with the adoption of the Digital Services Act (‘DSA’).⁷⁷ With the goal to 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, as also underlined by the ECJ.⁷⁸ 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.

Within this framework, it would be interesting to wonder how the sequence of the events described in the introduction would be read in the Europe. In particular, the decision of Twitter to block the presidential account could not be taken without ensuring certain transparency and procedural safeguards, defining a form of digital due process showing the steps of platform decision-making. Likewise, Trump could also rely on redress mechanism to challenges the

⁷³ 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.

⁷⁴ Martin H Redish and Lawrence C Marshall, ‘Adjudicatory Independence and the Values of Procedural Due Process’ (1986) 95(3) Yale Law Journal 455.

⁷⁵ Danielle K Citron, ‘Technological Due Process’ (2008) 85(6) Washington University Law Review 1249.

⁷⁶ Crawford and Schultz (n 103).

⁷⁷ 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.

⁷⁸ Case C-70/10 Scarlet v SABAM (2011); C-360/10 Netlog v SABAM (2012).

social media' decision. This however did not happen on the other side of the Atlantic or in Australia where the decision of Facebook to ban news media was unaccountable.

The lack of transparency and safeguards in this field also leads to wonder about the role of the Facebook Oversight Board. This body would promise to review some of the most important cases of removal addressed by Facebook and its first decisions promise to provide users with a new potential remedy against discretionary content removal, while making Facebook's decision-making on content moderation more accountable and transparent. Such an alternative dispute resolution system raise several question in terms of legitimacy, impartiality and accountability, thus, raising further question for the rule of law.

These cases do not only promise more responsibility and accountability of Facebook's governance of online speech, but also showcase private actors' power to autonomously enforce community guidelines, while seeking legitimacy from an (independent) Oversight Board.

Against this trend, the Union is trying to reduce digital private powers by regulating their activities and designing a digital due process. This new set of rights would be a first step to ensure that the principle of the rule of law is not replaced by business interests. This shows how procedural safeguards can play a critical role in fostering due process and protect individual autonomy.

5. Conclusions

In the algorithmic society, the rule of law is under pressure from multiple sides. Artificial intelligence technologies have contributed to introducing new paths for innovation producing positive effects for the entire society, including fundamental rights and freedoms. Public and private actors are increasingly relying on these technologies respectively to provide public services or perform their businesses. Nonetheless, the domain of inscrutable algorithms characterising contemporary societies challenges the protection of fundamental rights and democratic values while encouraging lawmakers to find a regulatory framework balancing risk and innovation. The global pandemic has not only amplified the reliance on surveillance instruments by public actors but also the concerns relating to online platforms as transnational private powers exercising forms of public functions.

The rise of digital private powers challenges the traditional characteristics of constitutional law, thus, encouraging to wonder how to face the challenges brought by the emergence of new forms of powers in the algorithmic society. Constitutions have been meant to limit public, more precisely governmental powers, to protect individuals against any abuse by the state. 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. This would lead to redrawing the relationship between constitutional law and private law, including the duties to regulate the cybernetic complex, within or outside the jurisdictional boundaries.

Within this framework, constitutional law can provide at least two instruments to remedy the challenges to the principle of the rule of law. Firstly, the horizontal application of fundamental rights could mitigate the power of transnational private actors determining as

standard of protection of rights and freedoms competing with public authority. Secondly, new substantive and procedural rights would provide a comprehensive approach to ensure that the implementation of artificial intelligence technologies by public and private actors does not lead individuals into a new form of *status subjectionis* without safeguards.

The significant paradigm shift that individuals are witnessing in the relationship with power would therefore seem to require focusing on a series of rights that can be applied not only to public authorities, but also to private actors. It is therefore a question of understanding what level of protection it is necessary to guarantee individuals. In particular, an approach aimed at regulation such as the one advanced by the DSA could certainly help to remedy the lack of equity, transparency and accountability that would seem the most important challenge to be faced with respect to the use of artificial intelligence systems by public and private actors.