UNIO - *EU Law Journal*. Vol. 10, No. 2, December 2024, pp. 70-90.
®2024 Centre of Studies in European Union Law
School of Law – University of Minho

Mapping the values of digital constitutionalism: guiding posts for digital Europe?

Miguel Pereira[*]

ABSTRACT: Since its development, the face of the internet has changed drastically, both in terms of the technology employed, the number of users, the impact and interwovenness with the lives of people and the activities of businesses all over the world. This rapid development, while clearing the way for increased production of wealth, facilitating communication, and allowing for the creation of new economic activities, has also had indelible impacts on the day-to-day lives of ordinary citizens and of constitutional democracies. These impacts seem to result from the increased platformisation of the internet, the concentration of market power around a handful of economic operators (gatekeepers), and the wide-ranging powers these operators enjoy in setting the conditions and restrictions they see fit in their terms of service. In this context, academia has highlighted many of the issues this scenario has brought about and the concerns it raises for the protection of fundamental rights and democracy. To address such issues, two approaches appear to take centre stage: a watered-down version of the early libertarian aspirations for the internet, on one hand; and, on the opposite side, a state-centric regulatory approach. A third path seems to have formed recently, that of digital constitutionalism, which looks to translate the traditional safeguards of modern constitutionalism to the digital realm, complementing them with innovative means, in light of the specific needs created by technologies such as algorithmic techniques, profiling and artificial intelligence. In this paper, we investigate the theory of digital constitutionalism and isolate its core values with a view to lay the groundwork for future research dedicated to assessing whether EU law and policy on digital services have adhered to them.

KEYWORDS: Digital constitutionalism – digital services – online platforms – transparency – rule of law.

[*] Master in European Union Law from the School of Law of the University of Minho.

1. Introduction

George Steiner identified the café as an essential staple of the idea of Europe, as the embodiment of the European tradition of exchange, resistance and cultural development. A place that is open to all, to gather and share ideas, to have a drink, play chess, write a treatise or simply find shelter from the cold. *"Enquanto existirem cafetarias, a 'ideia de Europa' terá conteúdo."*[1] This allegory encapsulates the European ideals of exchange, diversity, liberty and connectedness, which have found their latest and most stable expression in the European Union. These ideals are also the foundational aspects of the internet, most eloquently expressed in John Perry Barlow's "*A Declaration of the Independence of Cyberspace.*"[2] It is only natural, then, that the internet should assume a central role in the development of the European civilisation as its new café.

The internet as we know it today was made possible by the advent and widespread use of the World Wide Web hypermedia software[3] and browsers, such as Netscape. The early World Wide Web was dominated by simple (and mostly static) pages created by businesses and incipient manifestations of personal homepages.[4] Using the internet was a cumbersome process and access to the necessary physical means still scarce, resulting in a sparsely populated arena (with approximately 150 million users in 1998[5] compared to 5.35 billion by 2024).[6]

The rapid technological development that defined the past couple of decades allowed for incomparably greater and easier access to the internet and for the generalisation of inexpensive internet-connected devices, effectively ushering the world into an unprecedented era of globalised communication and trade. It also altered the face of the internet, now increasingly characterised by its ubiquity, *platformisation* and concentration of market power around a handful of companies. Its ubiquity, expressed in the internet's interwovenness with our daily lives, is manifested by the ever-present connectivity of mobile devices and the rise of the "*internet of things*"[7] as well as, and most importantly, by its creeping incursion into every small act, habit, and activity that we carry out – even those that were traditionally exclusive to the offline world.

[1] "*As long as cafés exist, the 'idea of Europe' will have content*" (author's translation). George Steiner, Rob Riemen (introd.) and José Manuel Durão Barroso (pref.), *A ideia de Europa* (Lisbon: Gradiva, 2006), 26–28.

[2] John Perry Barlow, "A declaration of the independence of cyberspace", *Eletronic Frontier Foundation* (blog), 8 February 1996, https://www.eff.org/cyberspace-independence.

[3] Raphael Cohen-Almagor, "Internet History", *International Journal of Technoethics* 2, no. 2 (2011): 53, https://doi.org/10.4018/jte.2011040104. The World Wide Web is described by the author as system of protocols "*building a distributed hypermedia server which would allow Netusers to prepare electronic documents that are composites of, or pointers to, many different files of potentially different types, scattered across the world.*"

[4] Cohen-Almagor, "Internet History", 45–64.

[5] Cohen-Almagor, "Internet History", 55.

[6] "Digital 2024: Global Overview Report", *Datareportal* (blog), 31 January 2024, https://datareportal.com/reports/digital-2024-global-overview-report.

[7] Felix Wortmann and Kristina Flüchter, "Internet of Things: technology and value added", *Business & Information Systems Engineering* 57, no. 3 (2015): 221, https://doi.org/10.1007/s12599-015-0383-3. While pointing to the existence of several definitions for the concept, the authors detail the one put forth by the International Telecommunication Union: "*a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*".

Another defining trait of the current digital ecosystem is the generalisation of the platform, which can be defined as a "*programmable digital architecture designed to organise interactions between users - not just end users but also corporate entities and public bodies [...] geared toward the systematic collection, algorithmic processing, circulation, and monetisation of user data*."[8] Indeed, over the last twenty years we witnessed the rise of the platform as the main instrument of interaction with the digital sphere, as well as one of the principal online business models for technology companies. Among these companies, however, a few stand out for the extraordinary market power they have amassed throughout the years,[9] the gatekeeper role they have started to assume[10] and the increasing reliance on them by the market as the basic infrastructure for most of the information flows carried through the web.[11] Considering these new characteristics, and while the foundational aspects of the internet still hold true, the digital landscape has morphed in such a way that the early libertarian values espoused by Barlow no longer seem sufficient as a suitable paradigm for internet governance.[12/13]

The impact of the evolution of the digital ecosystem is still being chronicled but enough concerns have been identified for a chorus of voices to be raised, calling for increased surveillance and regulation of digital services and technology.[14] The issues that are advanced vary, depending on the focus of the studies,[15] the type

[8] José van Dijck, Thomas Poell, and Martijn de Waal, *The Platform Society* (New York: Oxford University Press, 2018), 4.

[9] Jeffrey D Manns, "The case for preemptive oligopoly regulation", *Indiana Law Journal* 96, no. 3 (2021): 751–801.

[10] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shapping Europe's digital future*, COM(2020) 67 final.

[11] Dijck, Poell, and Waal, *The Platform Society*, 4; Lina M. Khan, "Amazon's antitrust paradox", *Yale Law Journal* 126, no. 3 (2016): 754–55; Kashmir Hill, "Life without the tech giants", *Gizmodo*, 22 January 2021, https://gizmodo.com/life-without-the-tech-giants-1830258056.

[12] The field of internet governance has traditionally been focused on infrastructural issues, both physical and technical, with the early scholarship on the matter dedicating itself to the study of the institutional frameworks in which decisions regarding these infrastructure issues were taken (*inter alia*, domain name and IP address management and institutions such as ICANN and the United Nation's Internet Governance Forum), while matters relating to content and online services were usually sidestepped. See, in this sense, Michel JG van Eeten and Milton Mueller, "Where is the governance in internet governance?", *New Media & Society* 15, no. 5 (2013): 720–36, https://doi.org/10.1177/1461444812462850. In recent years, considering the evolution of the internet and the increasing infrastructural role certain digital services providers have assumed, the scope of investigation in the field has widened to encompass the role played by these providers in internet governance – a development with which we agree. See, for instance, Laura DeNardis and Andrea M. Hackl, "Internet governance by social media platforms", *Telecommunications Policy* 39, no. 9 (October 2015): 761–70, https://doi.org/10.1016/j.telpol.2015.04.003.

[13] For an overview of the traditional subjects of internet governance research, see Laura DeNardis, "The emerging field of internet governance", Working Paper (Yale Information Society Project, Yale Law School, 2010).

[14] *Inter alia*, Shoshana Zuboff, *A era do capitalismo de vigilância - a disputa por um futuro humano na nova fronteira do poder* (Lisbon: Relógio D'Água Editores, 2020); Dipayan Ghosh, *Terms of disservice: How Silicon Valley is destructive by design* (Washington, D.C: Brookings Institution Press, 2020); Eric Nee, "Three Cheers for Regulation", *Stanford Social Innovation Review* 17, no. 3 (2019): 4, https://doi.org/10.48558/MFMS-WG62.

[15] Jack M Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation", *U.C. Davis Law Review* 51, no. 3 (2018): 1149–1210. Focusing on the impact of algorithmic governance on freedom of expression online.

of digital service or platform under review[16] and even the regional specificities of the geographies covered by those services and platforms.[17] The common thread among these worries is the societal changes that the "*platform society*" has brought about, not all of them positive. Much to the contrary, the literature dedicated to the subject matter has compiled multiple instances in which specific digital services and platforms, and their business model as a whole, have conflicted with fundamental rights and been detrimental to the protection of public values, with issues relating to data privacy and the increasing power imbalance between digital services providers, users, local communities and states taking central place in the discussions.

Shoshana Zuboff reviews online platforms' practices and the way by which big and small technology companies have built a business model based on extracting, processing, and selling (predictive) behavioural data from internet users. Some of the examples collated by the author range from the introduction in 2012 of the Google Glass wearable that involved the permanent and undetectable recording of the surroundings of the user, to the hidden program (downloaded with the package for other inoffensive applications such as a restaurant guide) that allowed for physical tracking of users across Parisian stores and shopping malls.[18] This business model requires a constant and heavy stream of data to feed these companies' predictive products and to further develop their algorithmic and artificial intelligence capabilities ("AI"). The need for a constant influx of big data has led companies, on one side, to engage in an expensive shopping spree for start-ups and smaller companies operating in a vast array of sectors,[19] on the other, to design their services (their platforms) in such a way that they acquire a sense of necessity or, ideally, unavoidability. This is particularly evident in social media platforms, which, through the use of design features and algorithmic content curation, strive to retain the users' attention for the longest span possible to increase data collection – usually in such a way that those mechanisms remain unbeknownst to the user.[20]

Along similar lines, though with a special focus on legal institutions and how these have been stretched to address and accommodate the needs of technology companies, Julie E. Cohen identifies similar hallmarks of a data-driven business model that has developed on pair with the *platformisation* of the internet. In this sense, not only are technology companies benefitting from a largely unregulated

[16] Dijck, Poell, and Waal, *The Platform Society*. The authors explore the different sectors in which platforms now operate (*i.e.* health, news media, transportation, etc.), going in detail into the most prominent in each.

[17] Favour Borokini and Ridwan Oloyede, "When fintech meets 60 million unbanked citizens", in *Fake AI*, ed. Frederike Kaltheuner (Manchester: Meatspace Press, 2021), 170–81. Covering the issues raised by the emergence of the "fintech" industry in Nigeria.

[18] Zuboff, *A era do capitalismo de vigilância - a disputa por um futuro humano na nova fronteira do poder*, 159–99.

[19] PCMag, "The biggest tech mergers and acquisitions of all time", *PCMag*, 12 April 2021, https://www.pcmag.com/news/the-biggest-tech-mergers-and-acquisitions-of-all-time.

[20] For an overview of these mechanisms and their impact on democratic debate, see Miguel Pereira, "Instant democracy: a look forward to the EU's digital future", *UNIO - EU Law Journal* 7, no. 1 (2021): 78–79, https://doi.org/10.21814/unio.7.1.3578; Georg Aichholzer and Ralf Lindner, "E-Democracy: conceptual foundations and recent trends", in *European E-Democracy in Practice*, ed. Leonhard Hennen et al., *Studies in Digital Politics and Governance* (Cham: Springer International Publishing, 2020), 11–45, https://doi.org/10.1007/978-3-030-27184-8; Ronald J. Deibert, "Three painful truths about social media", *Journal of Democracy* 30, no. 1 (2019): 25–39, https://doi.org/10.1353/jod.2019.0002.

space but, over the years, innovative interpretations on existing statues and regulations – on a number of topics, namely, and with particular relevance for our research, on intellectual property rights – have been taken up by the courts, further expanding their toolkit to exert dominance online.[21] Identifying this as a new era of political economy, the author opts for the designation, "*information capitalism*", highlighting the shift from the industrial era vocation towards manufacturing to the *informationalism* orientation "*toward the production, accumulation and processing of information*."[22] The author notes how, aside to the production factors we have traditionally been accustomed to identifying – those of capital, land and labour – a fourth production factor seems to be emerging, "*data flows extracted from people*", now serving as a basis for the business model of online platform.[23]

The objective of such aggressive data collection practices is the creation of user profiles with such granularity that inferences on the users' preferences, habits, ambitions and emotions can be drawn from their online activity with a view to predict the users future behaviour[24] and, eventually, monetising such knowledge.[25] As Alessandra Silveira points out, the *de facto* protection afforded to data subjects as regards the use of inferred data in the context of the EU framework for data protection, the General Data Protection Regulation ("GDPR"),[26] is unclear,[27] considering its proclivity towards protecting data provided by the user in detriment of that inferred from the user's input data and online activity.[28] The emergence of this data-driven business model and the obliviousness of most users to methods such as inferred data-based profiling and nudging mechanisms, reveals another dimension of the imbalance of power between users and platforms.

These factors, in some ways endemic to the current functioning of online platforms, are crystalised in the providers' Terms of Services ("ToSs"), which are unilaterally defined and amended and can themselves, in turn, be algorithmically enforced. The nature of the powers that ToSs can bestow on platforms, coupled

[21] Julie E. Cohen, *Between truth and power* (New York: Oxford University Press, 2019), Chap. 1, https://juliecohen.com/wp-content/uploads/2021/08/CohenBTP_Ch1_EverythingOldIsNew.pdf.

[22] Julie E. Cohen, *Between truth and power* (New York: Oxford University Press, 2019), Introduction, https://juliecohen.com/wp-content/uploads/2021/08/CohenBTP_Intro.pdf.

[23] Julie E. Cohen, *Between truth and power*, Chap. 1.

[24] Or, as Jack Balkin would put it, to achieve "*practical omniscience*": "*the ability to know as much as possible about who is doing what, when, and where; and the ability to predict who will do what, when, and where*." Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation", 1155.

[25] Data can be monetized by companies, either internally, when used to optimise processes and practices, or externally, when used to provide services to customers. See Petri Parvinen et al., "Advancing data monetization and the creation of data-based business models", *Communications of the Association for Information Systems* 47, no. 1 (1 October 2020): 25–49, https://doi.org/10.17705/1CAIS.04702. The authors highlight three ways for companies to monetize data externally: selling data, selling analyses of data and selling data-based services.

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal* L 119, 1-88.

[27] Alessandra Silveira, "Editorial of March 2024 - On inferred personal data and the difficulties of EU law in dealing with this matter", *Thinking and Debating Europe: The Official Blog of UNIO - EU Law Journal* (blog), 19 March 2024, https://officialblogofunio.com/2024/03/19/editorial-of-march-2024/.

[28] Alessandra Silveira, "Profiling and cybersecurity: a perspective from fundamental rights' protection in the EU", in *Legal developments on cybersecurity and related fields*, ed. Francisco Andrade, Joana Abreu, and Pedro Freitas (Cham, Switzerland: Springer International Publishing, 2023).

with States' limited ability to interfere in the digital space, has led to the recognition by some authors of *quasi*-public powers exercised by technology companies in the internet – powers which can be enforced autonomously (and automatically) through the network infrastructure, against which users find few means of recourse.[29] In fact, the existence and format of any redress mechanisms are largely left to the discretion of platforms and other internet service providers, meaning that users might only be left the option to take matters to a competent court – an option which is not likely to be taken up by most considering the costs such a step would entail (often for complaints regarding trivial matters or low value transactions).

The foregoing summary of the current digital landscape highlights the power imbalance that is characteristic of our interactions with digital services providers: market dominance by a handful of companies, exacerbated by the purchase of start-ups, ensures that users are left with few alternatives to the services they seek; recourse to these services by competitors and smaller companies ensures our dependency on them as the basic infrastructure of the internet; untransparent and aggressive data collection coupled with the employment of algorithmic capabilities to extract knowledge regarding the users and to predict their future behaviour ensures an uneven access to information by the user and service provider; and, finally, the employment of general contractual terms (ToSs), regarding which the user as no say over, conferring wide reaching powers to service providers which can, in some ways, mimic those exercised by sovereign states, ensures a comprehensive control by the provider over the contractual relationship and the provision of the service.

The effects of this scenario are multiple, and we have highlighted only a few over the course of this introduction, however, the most striking feature seems to be an increasing loss of individual autonomy resulting from a comprehensive shift in power towards digital service providers. This has resulted in the intensification of discussions concerning internet governance and the principles, processes and sources that should inform it. Two opposing conceptions seem to dominate the debate: on one side, a view which can be described as a watered-down version of the initial libertarian doctrines of the internet, focused on industry self-regulation, reinforced by user participation; on the other, a current advocating stronger state intervention through regulation and enforcement.[30]

[29] *Inter alia*, Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation", 1182-98; Giovanni De Gregorio, "From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society", *European Journal of Legal Studies* 11, no. 2 (2019): 85-89; Edward Lee, "Virtual governments", *UCLA Journal of Law & Technology* 27, no. 2 (2022): 1-32. James Balkin, recognises technology companies' ability to promulgate, implement and enforce rules, stating that this leads to the creation of expectations by the users regarding transparency, due process and participation in the governance of the platform. Giovanni De Gregorio notes how platforms have assumed three functions that are intrinsically connected to the exercise of public power: a *quasi*-judicial function through the balancing of fundamental rights – when performing content moderation, for instance, platforms often find themselves addressing conflicting fundamental rights (i.e. freedom of expression of the uploader versus right to privacy of persons contemplated in the content) –, a *quasi*-executive function through the enforcement of those decisions (i.e. content removal), and a *quasi*-legislative function through the unilateral drafting of their ToSs which set out the rules for the exercise of the above-mentioned powers. Edward Lee recognizes the same notion, adding that technology companies likely have at least as much input (if not more) on how the internet evolves as states do. The author advances three features that would improve platform governance: increased democratic participation, increased transparency and reason-giving and, finally, separation of powers.

[30] See, *inter alia*, Orly Lobel, "The law of the platform", *Minnesota Law Review* 101, no. 1 (2016): 87-166; Julie E Cohen, "The regulatory state in the information age", *Theoretical Inquiries in Law* 17,

Considering this divide, and the difficulty in finding common ground in discussions that tend to have, at least in part, an ideological undertone, a third path seems to have formed: digital constitutionalism. In fact, as Giovanni De Gregorio notes, the EU seems to have followed this path, with the adoption of the GDPR marking this paradigmatic shift.[31] The EU has since increased efforts to renovate its legislation and policy affecting the digital ecosystem, which increasingly feature notes of digital constitutionalism. It is our contention that at this stage it is possible to identify the presence and content of principles of digital constitutionalism in EU law and policy.

In this paper, we will endeavour to lay out the main characteristics of digital constitutionalism, reaching a working definition for the concept. The focus will be on recounting the elements that compose digital constitutional theory, with a view to extract the core values it espouses, laying the groundwork for future research on the identification of principles of digital constitutionalism in EU law and policy.

2. Mapping the values of digital constitutionalism

Digital constitutionalism is a legal theory which has recently gained traction in legal scholarship as a possible pathway to address the issues caused by the introduction of digital technologies in society. With some authors tracing its origins back to the early 2000s or late 1990s, there is no unitary definition of the concept and the designation it assumes varies according to the specific tone each author intends to confer to it – some focusing on the contractual aspects of the information society and the recognition of a constitutional facet to private law,[32] while others emphasise aspects concerning legitimacy and the constitutive nature of the community rules in the context of governance of digital communities,[33] or, alternatively, on more formal aspects, such as the inclusion or not in traditional constitutional law legislative instruments, particularly bills of rights.[34] Nicholas Suzor first coined the term digital constitutionalism in his study of the governance of virtual communities[35] and since then it has been adopted by scholarship in place of "*informational constitutionalism*"[36] and "*constitutive constitutionalism*."[37]

Considering the different objects of study and constitutional traditions from which each author addresses digital constitutionalism, it is hard to find an umbrella definition covering all the different strains of the theory – a difficulty which led Edoardo Celeste to review the existing literature on the matter in an

no. 2 (2016): 369–414, https://doi.org/10.1515/til-2016-0015.

[31] Giovanni De Gregorio, "The rise of digital constitutionalism in the european union", *International Journal of Constitutional Law* 19, no. 1 (2021): 41–70, https://doi.org/10.1093/icon/moab001.

[32] Brian Fitzgerald, "Software as discourse: the power of intellectual property in digital architecture", *Cardozo Arts & Entertainment Law Journal* 18, no. 2 (2000): 337–86.

[33] Nicolas Suzor, "Digital constitutionalism and the role of the rule of law in the governance of virtual communities" (PhD diss., Brisbane, Australia, Queensland University of Technology, 2010).

[34] Dennis Redeker, Lex Gill, and Urs Gasser, "Towards digital constitutionalism? Mapping attempts to craft an internet bill of rights", *International Communication Gazette* 80, no. 4 (2018): 302–19, https://doi.org/10.1177/1748048518757121.

[35] Suzor, "Digital constitutionalism and the role of the rule of law in the governance of virtual communities."

[36] Brian Fitzgerald, "Software as discourse? A constitutionalism for information", *Alternative Law Journal* 24, no. 3 (1999): 144–49.

[37] Paul Berman, "Cyberspace and the state action debate: the cultural value of applying constitutional norms to private regulation", *University of Colorado Law Review* 71, no. 4 (2000): 1263–1310.

effort to identify its objectives and reach a unitary or global conceptualisation that reconciles the different views espoused by the scholars studying the phenomenon.[38] In this section, we intend to build on Celeste's work by identifying and isolating common threads and values in the literature on digital constitutionalism with a view to use them as guiding stones in the identification of digital constitutionalism principles in existing EU law and policy.

Without it being our primary focus, we also intend to reach a working definition (that is to say, for the purposes of our investigation) based on the elements collected through the analysis carried out in this chapter. The purpose of this approach is to emphasise the values that inform the theory as these are more discernible elements in the EU *acquis*, considering that, at this stage, EU law and policy do not expressly reference Digital Constitutionalism. However, and before delving into the proposed work, we consider it useful to advance a broad notion of the theory focused not so much on its characteristics but rather, on its objectives.

In this sense, and taking a step back, it's worth recounting two of constitutional law's main purposes: (i) the protection of fundamental rights; and (ii) the limitation of powers.[39/40] These functions hold true even in the context of the EU, which, absent the existence of a formal constitution, looks to its founding treaties as a constitutional framework to ensure the limitation of powers of its Institutions and Member States ("MSs") (when applying EU law) and to ensure the effectiveness of individual freedoms and rights (as recognised under EU law).[41] Considering these two traditional functions, while keeping in mind the threats posed by private entities, which we summarised in the Introduction, and, once more, building on Edoardo Celeste and Giovanni De Gregorio's work, we consider that the purpose of digital constitutionalism is, "*to adapt constitutional values and fundamental rights to the digital environment, clarifying the new facets they assume in this new arena and extending their reach beyond the traditional vertical effect (vis-à-vis the state).*"[42] As such, while the idea is not so much the creation of a new digital constitution, digital constitutionalism

[38] Edoardo Celeste, "Digital constitutionalism: a new systematic theorisation", *International Review of Law, Computers & Technology* 33, no. 1 (2019): 76–99, https://doi.org/10.1080/13600869.2019.1562604.

[39] Anne Peters, "Compensatory constitutionalism: the function and potential of fundamental international norms and structures", *Leiden Journal of International Law* 19, no. 3 (2006): 580–85, https://doi.org/10.1017/S0922156506003487.

[40] Another traditional function and objective of Constitutional Law is the organisation of a political community in the form of an entity, the state. As we highlight in this section, the focus of our research will be on horizontal relationships in the digital realm. As such, the organizational function of Constitutional Law, at least for the moment, bears limited significance in this arena. This is not to say that this will hold true in the future, especially considering recent movements such as Web 3.0 which seem to propose a form of internet governance with a degree of constitutionalism that not only admits but requires an organizational function, more in line with what is recognizable in nation states' constitutions. On the subject, see Franco Manti, "Good government and participatory democracy. A model of social partnership", *Philosophy and Public Issues (New Series)* 7, no. 3 (2017): 123–56.

[41] Alessandra Silveira, "International constitutional court e integração (constitucional) europeia", in *International Studies on Law and Education, São Paulo/Porto, CEMOrOc-Feusp. IJI-Universidade do Porto*, 2016, 71–76, http://www.hottopos.com/isle24/71-76Silveira.pdf.

[42] Miguel Pereira, "Truffle hunting: finding meaning in the European Declaration on Digital Rights and Principles for the Digital Decade", *Thinking and Debating Europe: The Official Blog of UNIO - EU Law Journal* (blog), 14 February 2023, https://officialblogofunio.com/2023/02/14/editorial-of-february-2023/.

proposes a new outlook on constitutionalism.[43] It is not by chance that it found the most fertile ground in the EU which, as Alessandra Silveira puts it, represents a new constitutionalism in itself.[44]

It is important to note that this paper is limiting the scope of digital constitutionalism in two ways: firstly, we will consider only norms and policy issued in the context of EU institutions (thereby excluding other normative sources or constitutive/societal constitutionalism responses); secondly, we will focus exclusively on the limitation of powers and protection of fundamental rights *vis-à-vis* private entities. This contrasts with some of the literature on digital constitutionalism which includes and studies both different constitutional sources and responses but also highlights the threats posed by public actors in the digital realm and considers these as subjects of digital constitutionalism alongside private entities or persons.[45] These elements are not included in our research in consideration of the specific focus on EU law and policy, as well as the issues posed by online platforms.

2.1. Limiting (or re-balancing) powers

The limitation of powers is a traditional objective or value of constitutionalism, from which other values, such as the rule of law, transparency and accountability and proportionality, are distilled to ensure its effectiveness. As Oreste Pollicino and Giovanni De Gregorio note, "*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*."[46] Indeed, the mission of constitutionalism is exactly that of limiting the discretionary power government's may exercise over us.[47] The mission of digital constitutionalism is translating those limits to a new realm – the internet – with new actors – online platforms and other internet intermediaries.

This need results from a shift in power towards internet intermediaries which now, in certain aspects, find themselves in a position that is closer to that of states then ordinary natural or legal persons.[48] This is made evident by James Balkin who reviews this shift in power in the field of freedom of expression.[49] The author notes how, in the US, the First Amendment serves the primary function of protecting individuals against unwarranted censorship and associated this function to the traditional dyadic model of speech regulation, where the threat of censorship was posed primarily by the government. This model seems to no longer adequately describe the pressures that speech is subject to in the digital age as it is missing a key component: the privately-owned infrastructure we use to communicate. In this sense, the relationship is no

[43] For a summarised distinction between the concepts of "constitution", "contitutionalization" and "constitutionalism" see Peters, "Compensatory Constitutionalism", 581–84.

[44] Alessandra Silveira, "Constituição, ordenamento e aplicação de normas europeias e nacionais", *Polis : Revista de Estudos Jurídico-Políticos*, no. 17 (2008): 68–72, https://doi.org/10.34628/8D59-B578.

[45] Celeste, "Digital Constitutionalism", 89–92.

[46] Oreste Pollicino and Giovanni De Gregorio, "Constitutional Law in the algorithmic society", in *Constitutional challenges in the algorithmic society*, ed. Hans-W. Micklitz et al., 1st ed. (Cambridge University Press, 2021), 15, https://doi.org/10.1017/9781108914857.

[47] Nicolas P. Suzor, *Lawless: the secret rules that govern our digital lives* (Cambridge, United Kingdom; New York, NY: Cambridge University Press, 2019), 105.

[48] Andrea Simoncini and Erik Longo, "Fundamental rights and the rule of law in the algorithmic society", in *Constitutional Challenges in the Algorithmic Society*, ed. Hans-W. Micklitz et al., 1st ed. (Cambridge University Press, 2021), 33, https://doi.org/10.1017/9781108914857.

[49] Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation".

longer dyadic but pluralist as individuals now face threats of censorship from private entities: intermediaries governing the digital communication infrastructure (*i.e.* online platforms).[50] As the author notes, and others have pointed out, while states have shown inclination to take advantage of these new mechanisms to censor or control speech, enacting legislation or pressuring intermediaries to do so on their behalf, online platforms have also chosen to regulate speech for their own commercial purposes.[51] Most importantly here, they can and have done so without the obligation of creating safeguards for users who disagree with decisions taken by them affecting their freedom of expression. While the analysis carried out by Balkin is very much focused on the right to freedom of expression, the same comments on the shift of power towards online platforms and the threats posed by it can be made regarding other fundamental rights, namely, privacy and equality.[52]

This ability to govern their spaces as they see fit, combined with the business model described in the introduction and the fast-paced acquisition of competitors, seems to have changed the face of the freedom to conduct business, with some authors now considering that this freedom has consolidated into a new (private) power.[53] It is considering the threat posed by this new form of power that digital constitutionalism calls for the acknowledgement and limitation of the arbitrary power of internet intermediaries in order to, in line with the traditional mission of constitutionalism, prevent abuses of power online that affect our fundamental rights in similar ways as they would be affected offline (and by the State), were there no constitutional safeguards in place.

However, it is clear that users of online platforms and other intermediaries do not hold the same expectations regarding these service providers as they do regarding states and their governments. Nor would the relationship between users and platforms be susceptible to accommodating those expectations as, in the end, such a relationship is still a matter of private law. Part of the issue, as Nicolas Suzor notes, is, indeed, connected to the fact that we have yet to stabilise a concrete set of expectations regarding how we want intermediaries to act and what their role in civil society should be.[54] For this reason, the solutions found by modern constitutionalism are not necessarily directly applicable to the digital realm and require some adaptation. While values such as the rule of law or transparency have shown that they hold true and are needed online, the way they manifest themselves must be different as they are now meant to apply to horizontal relationships. An acritical assimilation of the traditional formulas of limitation of power could, otherwise, be either ineffective, innovation-stifling, or

[50] Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation", 1151–54.

[51] Balkin, "Free speech in the algorithmic society: big data, private governance, and new school speech regulation", 1182–84; Zuboff, *A Era do Capitalismo de Vigilância - A Disputa por Um Futuro Humano na Nova Fronteira do Poder*.

[52] Nicolas Suzor, Tess Van Geelen, and Sarah Myers West, "Evaluating the legitimacy of platform governance: a review of research and a shared research agenda", *International Communication Gazette* 80, no. 4 (2018): 385–400, https://doi.org/10.1177/1748048518757142; Dijck, Poell, and Waal, *The Platform Society*.

[53] Giovanni De Gregorio, *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, 1st ed. (Cambridge, United Kingdom: Cambridge University Press, 2022), https://doi.org/10.1017/9781009071215; Pollicino and De Gregorio, "Constitutional law in the algorithmic society".

[54] Suzor, *Lawless*, 105–71.

highly disruptive of the normal performance of services.[55] As Martin Krygier puts it, "*the challenge for anyone seeking to temper power anywhere is not primarily to emulate or parody practices that might have worked elsewhere, but to find ways of reducing the possibility of arbitrary exercise of power.*"[56]

In this sense, while most authors call for the definition of due process and transparency obligations (be them regulatory or of a voluntary nature) as a means to limit platform power, the notion that the solution must involve a devolution of power to the users seems to permeate the literature on the matter, especially if we focus on data protection issues, where user awareness and control over the collection and processing of their personal data is of paramount importance.[57] Indeed, aside to limiting the possibilities of data collection and processing, either through prohibitions or restrictions, anchoring these activities to legal instruments that require the existence of specific legal or contractual bases, the research on European data protection law recognises an intent to empower data subjects with a set of actionable rights that seek to endow them with greater knowledge about the data processing activities they're subject to and greater control over such processing (to name a few: right to portability, to access personal data, to erasure or rectification, right to object to processing).[58]

We believe this outlook more clearly reflects the distribution of power envisioned by digital constitutionalism which, rather than looking to bind states' powers, seeks to attain an adequate equilibrium of power[59] among the participants in the digital sphere, by devolving power to users, creating safeguards that prevent the abuse of powers by intermediaries and ensuring that the state's involvement is legally bound and transparent. As regards online platforms, this exercise is one of re-balancing of powers and calls for an assessment of proportionality between users' and platforms' rights and obligations.[60]

2.2. Rule of law

As has been established, limiting powers is one of the foundational and core values of digital constitutionalism. The rule of law is one of the ways through which constitutionalism manifests itself, how it realises its objective of limiting power. It has historically been considered as a necessary condition for the legitimate exercise of power, premised on the idea that, for this exercise to be legitimate, the power-wielders must acknowledge and be bound by limitations to its powers and that these limitations

[55] As an example, we can consider the impossibility of escalating all content-related decisions made by online platforms to first instance courts. The costs in legal fees and time would make this solution unpractical and would completely alter the way that online platforms work, possibly eliminating the characteristics that attract users. See, Suzor, *Lawless*, 144–49.

[56] Martin Krygier, "What's the *Point of the Rule of Law?*", *Buffalo Law Review* 67, no. 3 (2019): 789.

[57] The GDPR offers what is currently one of the most comprehensive sets of data subject rights in the world, paying particular attention to those rights which allow the data subjects to intervene in data collection, storage and processing activities, among which we highlight the right to object to processing (Article 21 GDPR), right to data portability (Article 20 GDPR) and the right to erasure (Article 17 GDPR). See Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union General Data Protection Regulation: what it is and what it means", *Information & Communications Technology Law* 28, no. 1 (2019): 88–92, https://doi.org/10.1080/13600834.2019.1573501.

[58] Paul De Hert et al., "The right to data portability in the GDPR: towards user-centric interoperability of digital services", *Computer Law & Security Review* 34, no. 2 (April 2018): 193-203, https://doi.org/10.1016/j.clsr.2017.10.003.

[59] Celeste, "Digital constitutionalism", 78-79.

[60] De Gregorio, *Digital constitutionalism in Europe*, 210-11.

are to be found in the law. Put differently, "*the 'rule of law' doctrine was the main legal tool 'invented' by constitutional theory to delimit the king's power and protect personal freedom and rights. To be 'legitimate', any power has to be subjected to the rule of law*".[61]

As Martin Krygier notes, the concept of the rule of law is frequently reduced to its more formal aspects (those connected to the conditions that rule-making and enforcing should adhere to) and closely linked to the idea of state, its institutions and instruments.[62] The author notes how increasingly little attention is paid to the reasons for its existence and its substantial content in favour of an assimilation of the concept with the principles and processes through which it operates. Krygier criticises this approach, noting the faults that it carries with it, of which we highlight a few, namely, how the different architecture and functioning of different institutions requires different approaches tailored to the specific needs that require addressing, as well as the different, non-state threats, regarding which rule of law values should also be considered, i.e. online platforms.[63] In the author's view, discussions surrounding the rule of law should start with focusing on the problem it seeks to address, which is how power is exercised and how arbitrary exercises of power can be prevented.

Noting the link between law and power, the former as a vehicle to exercise the latter, Krygier identifies the three forms of arbitrary exercise of power most commonly adduced by scholarship on the matter – from which, *a contrario sensu,* we extract three forms of limitation of power. First, power is exercised arbitrarily when it is unbound, beyond any "*regular control or limit, or accountability.*" As such, the rule of law imposes limits on the exercise of power, namely, those inscribed in the law itself – power must be wielded according to a set of rules that allow for control over its exercise, that limit such exercise and that provide for accountability in relation to those against whom it is exercised. Second, power is exercised arbitrarily when it is exercised unpredictably, that is to say, "*when those it affects cannot know, foresee, understand or comply*" with decisions made by those wielding such power. Conversely, the rule of law requires, not only the publicity of the reasons and rules legitimising the exercise of power, but also the stability and intelligibility of said rules. Third, power is exercised arbitrarily whenever those affected by it are not given a chance to be heard or to question, to inform the power-wielders about relevant circumstances or to "*affect*" the exercise of power, in essence, power is exercised arbitrarily whenever the person affected by the exercise of power is not given due chance to raise their interests or positions regarding the decisions affecting them.[64] Considering this last form of arbitrary power, the rule of law requires that those affected by a decision be given space to understand and question the decision, to raise their interests (relevant to the matter) and to "*affect*" or impact the exercise of power, namely through requiring that the decision be reviewed – in other words, the rule of law requires that there be a due process.

Similar positions can be found in digital constitutionalism literature. Suzor, who gives great emphasis to the legitimating facet of the rule of law,[65] considers that it requires that governance be anchored in legality in order to be legitimate

[61] Simoncini and Longo, "Fundamental rights and the rule of law in the algorithmic society", 31.

[62] Krygier, "What's the point of the rule of law?".

[63] Krygier, "What's the point of the rule of law?", 749–58.

[64] Krygier, "What's the point of the rule of law?", 759–68.

[65] Suzor, *Lawless*, 105–6.

(that is to say, limited by law) and identifies three traditional principles of the rule of law: consent, predictability and procedural fairness.[66] The author proposes that the legitimacy of the governance of online platforms be assessed against rule of law principles, focusing on the procedural issues that it addresses.

The first principle that is identified is that of "*meaningful consent*" ("*governance limited by law*"). According to this principle, power is made legitimate, is consented to, when it is exercised in a way that is limited by a set of rules, when those rules require that it be accountable to those against whom the power is exercised, that those who wield it abide by the rules prescribed for its exercise and that such rules may only be amended through specific procedures and within appropriate limits.[67] The second principle which Suzor uses to assess the governance of online platforms is that of "*formal legality*", which essentially calls for equality and predictability regarding the application of rules. This means that users of online platforms should be aware of the rules that apply to them and of the reasons for decisions that affect them. Additionally, this principle requires that rules be equally enforced and "*stable enough to guide behaviour.*"[68] Finally, the author refers us to the principle of "*due process*" which requires the establishment of a process for the resolution of disputes. Due process relates to the procedural safeguards put in place to ensure that decision-makers are impartial, that their decisions are transparent, that the discretion they enjoy in deciding is limited and that there are avenues of appeal to the decisions taken by them. Specifically, when applied to online platforms, Suzor suggests that due process should, at least, require that regulatory decisions taken by platforms be made according to valid criteria and processes, and that users adversely affected by such decisions be granted means of recourse and independent review of said decisions, including internal dispute resolution mechanisms, arbitration or access to courts.[69]

Along the same lines, though with a greater focus on automation of legal processes, explainability of algorithmic outcomes and due process issues, Frank Pasquale highlights as essential features of the rule of law the possibility of holding decision makers accountable for their decisions as well as for explaining the reasons that led them to take them.[70] Looking at due process rights, the author identifies three core elements, common to those collected from other authors mentioned in this section: a person's ability to explain their case and how their interests are affected before a decision is made; the possibility of obtaining an explanation regarding a decision taken against them; and, the capacity to appeal said decision. Additionally, the author adds a fourth element of special significance in the context of automated decision making and online platforms: the right to receive a judgement by a human being.[71]

[66] Nicolas Suzor, "Digital constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms", *Social Media + Society 4*, no. 3 (2018): 2, https://doi.org/10.1177/2056305118787812.

[67] Suzor, "Digital constitutionalism", 5-6.

[68] Suzor, "Digital constitutionalism", 6-7.

[69] The author notes how this minimum due process standards are not applied across the board, with little in the way of transparency regarding the rationale or processes behind decision making and forced arbitration in the platforms home jurisdiction or restrictions on access to courts (namely, the possibility of bringing class actions against the platform) included in some platforms' ToSs. See Suzor, "Digital constitutionalism", 7-8

[70] Frank Pasquale, "A rule of persons, not machines: the limits of legal automation", *George Washington Law Review* 87, no. 1 (2019): 5.

[71] Frank Pasquale, "Inalienable due process in an age of ai: limiting the contractual creep toward automated adjudication", in *Constitutional challenges in the algorithmic society*, ed. Hans-W. Micklitz *et al.*, 1st ed. (Cambridge University Press, 2021), 45-48, https://doi.org/10.1017/9781108914857.

This view is echoed by Amnon Reichman and Giovanni Sartor who, considering the rule of law as "a *mechanism to counter the rule of whim, desire, arbitrariness, or corrupt self-interest*", believe that automated decision-making will always require the involvement of a human being, a "*human in the loop or over the loop*." Reichman and Sartor also reinforce the importance of formal aspects related to restricting the possibilities of exercising arbitrary powers in decision-making that should also be considered when algorithms are involved in the process. These aspects are those of establishing the competence to make decisions, the process to reach one and the discretion that decision-makers enjoy in terms of determining the elements that are relevant to the decision and what weight they should be given.[72]

From the above we can extract three core values of the rule of law that hold true offline and online, as well as one that is specific to the digital environment and the "*algorithmic society*."[73] First, the rule of law requires that governance be limited by clear sets of rules that restrain the exercise of power, including the power to make rules. Second, the rule of law requires that those rules be stable, made public (known to the community) and that those affected by the exercise of power be informed of the reasons that led to the decision affecting them. Third, the rule of law requires that due process guarantees be put in place to limit the level of discretion allowed in the discharging of powers and to ensure the availability of avenues to contest decisions with which affected persons disagree with. Fourth, when algorithms are involved in the decision-making process, the rule of law requires that persons be given the chance to request human intervention in the decision.

2.3. Transparency

Connected to the two values already reviewed in this section, we find the value of transparency. Different from the rule of law, principles of publicity of rules, and reason-giving regarding specific decisions, transparency encompasses the wider governance activity of institutions and seeks to dissipate opacity in their functioning. In the words of Frederick Schauer, "*for some fact, information, or process to be transparent is to be open and available for examination and scrutiny*."[74] While varying degrees of transparency can be recognised, based on what should be open for examination and who should get access to examine[75], transparency can be looked at, in its negative dimension, as the mere availability of information, regardless of whether someone will actually make use of it[76] – it is, therefore,

[72] Amnon Reichman and Giovanni Sartor, "Algorithms and regulation", in *Constitutional challenges in the algorithmic society*, ed. Hans-W. Micklitz *et al.*, 1st ed. (Cambridge University Press, 2021), 160–62, https://doi.org/10.1017/9781108914857.

[73] Hans-W. Micklitz et al., eds., *Constitutional challenges in the algorithmic society*, 1st ed. (Cambridge, United Kingdom: Cambridge University Press, 2021), https://doi.org/10.1017/9781108914857.

[74] Frederick Schauer, "Transparency in three dimensions", *University of Illinois Law Review* 2011, no. 4 (2011): 1343.

[75] The author proposes that transparency be assessed along three variables, answering the questions of i) which institution or person should be subject to transparency requirements; ii) what (activities, information, processes, etc.) should be made transparent; and, finally, iii) which institutions or persons should be able to access that which is to be made transparent. Schauer, "Transparency in Three Dimensions", 1346.

[76] The author distinguishes between availability and usability, linking availability to the simple dissemination of information (negative dimension), while usability is linked to a more positive obligation of making use of the information that was disclosed. Schauer, "Transparency in three dimensions", 1343–44.

distinguishable from the aforementioned principles of the rule of law, which tend to be triggered by specific processes (often at the request of the affected persons) or individual decisions, as opposed to the more generalised release of information regarding the functioning of institutions, processes or decisions that transparency calls for.

At this stage, it is useful to make a note on the relationship between transparency and accountability which is not, as Schauer would agree,[77] as clear cut as may seem at first sight. In fact, as Jonathan Fox observes, while intuitively the notion may make sense, empirical evidence on the relationship between the two concepts is not as convincing as is to be expected, nor are the rationales put forward to sustain such relationship as solid as they purport to be.[78] As Fox notes, while transparency may be a necessary condition for accountability, it is not a sufficient one.[79] Notwithstanding that, it does make it harder for institutions to engage in misguided or damaging conduct as those in a place to exercise control over such institutions will be better positioned to respond to said conduct – in this sense, transparency functions as a regulatory/governance strategy which relies on disclosure of information to generate responses.[80] This is what Schauer calls "*Transparency as Regulation*", an idea associated with the old adage that "*information is power*", which is to say, "*that for one person or institution to have information about another is for the former to have power over the latter.*"[81]

Following Schauer's analysis of the concept of transparency, the author goes on to explore three other aims of transparency: (i) "*Transparency as Democracy*"; (ii) "*Transparency as Efficiency*"; and (iii) "*Transparency as Epistemology*." Turning to "*Transparency as Democracy*", the author notes some of the virtues that it shows as a form of public control over institutions. Besides highlighting its contributions to the fight against corruption in the public sector, Schauer calls attention to the benefits that transparency brings to public decision-making and places it at the core of democratic governance.[82] Indeed, by calling attention to issues of public interest, transparency has the potential to not only foster democratic debate, but to inform decision-makers and push them to act. Finally, looking at "*Transparency as Efficiency*" and "*Transparency as Epistemology*", Schauer observes how the first can be identified with the current view that holds that transparency drives market efficiency and, the latter, with the idea of the free marketplace of ideas – in this sense, transparency facilitates the apprehension of the truth, promising more knowledge and greater progress.[83]

Along the same lines, Tal Zarsky notes the importance of recounting and reassessing the benefits or, rather, the (theoretical) justification for transparency by first distinguishing different levels of transparency based on the recipients of the information, the audience that should get access to the information

[77] Schauer, "Transparency in three dimensions", 1346.

[78] Jonathan Fox, "The uncertain relationship between transparency and accountability", *Development in Practice* 17, no. 4–5 (2007): 664, https://doi.org/10.1080/09614520701469955.

[79] The author reviews empirical data on the issue, highlighting how increased transparency does not always result in increased accountability. Fox, "The uncertain relationship between transparency and accountability", 665.

[80] Schauer, "Transparency in three dimensions", 1347–48.

[81] Schauer, "Transparency in three dimensions", 1347.

[82] Schauer, "Transparency in three dimensions", 1348–50.

[83] Schauer, "Transparency in three dimensions", 1350–51.

being disclosed.[84] The author identifies four central theories of transparency: (i) transparency as an enhancer of fair and efficient policy making; (ii) transparency as a tool for attaining knowledge through crowdsourcing; (iii) transparency as a means to ensure protection of privacy rights; and (iv) transparency as an enhancer of individual autonomy.

Transparency as an enhancer of fair and efficient policy is closely linked to the concept of democracy and market efficiency, viewed as a means of control over governmental and corporate action – here, ideally, the recipients of information would be the general public.[85] With a different aim, transparency as crowdsourcing functions as a positive feedback loop to policy makers, allowing greater access by society to governmental data can result in positive and meaningful feedback being passed on to decision makers, which can take it into account for the relevant policy making activity – here, the audience of these disclosures might be restricted to selected individuals or institutions due to a series of concerns such as sensitivity of the data or impact on governmental functioning.[86] As for transparency as an enhancer of privacy rights, the author considers that this facet of transparency is connected to the notion of control in data protection law, as a prerequisite for the actual exercise of control, calling therefore, for the awareness, on the part of the data subject, of a data processing activity and of the data and means used in such processing. This facet of transparency links to the general principle of individual autonomy, in the sense that it provides individuals with information to make choices as to which level of control over their privacy rights they are willing to cede to others – in this case, the intended audience might not be the general public, nor specific institutions or experts but, rather, the data subject.[87] It should be noted here, however, that the author considers that transparency as an enhancer of individual autonomy also relates to the narrower scope which we include in the rule of law value: the possibility of obtaining explanations on individual decisions by affected individuals. The author, viewing the issue from a US Constitutional perspective, does not believe that the impact of wrongful automated decisions (in the majority of the cases) fulfils the constitutional criteria to be afforded protection under the due process clause and hence, includes these under the more general monicker of transparency – though, they go on to observe that regulatory initiatives seeking to enhance transparency in the context of automated predictive schemes should look to due process principles to guide their development.[88]

Looking at transparency issues as regards digital technologies, one of the primary concerns that scholarship focuses on is the use of predictive algorithms. As we highlighted in the introduction, the digital ecosystem is now dominated by online platforms which rely on algorithms and AI technology to manage their spaces. As

[84] Tal Z. Zarsky, "Transparent predictions", *University of Illinois Law Review* 2013, no. 4 (2013): 1532.

[85] The author refers to "shaming" and market forces as the materialization of this notion of transparency which looks to promote accountability. In this sense, "shaming" would be effective when decision-makers can be "shamed" into adopting certain decisions or refraining from adopting said decisions due to public outcry on the subject (the weaknesses this argument faces are, first, the public must have sufficient interest and understanding of the topic to effectively be mobilized and, second, the officials must be susceptible to "shaming" – *i.e.* low level officials or bureaucrats have limited public exposure and are, hence, less susceptible to being shamed) and companies would be susceptible to pressure by other actors in the market (i.e. consumers) which could be able to react to information that is disclosed. Zarsky, "Transparent oredictions", 1533–38.

[86] Zarsky, "Transparent predictions", 1538–41.

[87] Zarsky, "Transparent predictions", 1541–45.

[88] Zarsky, "Transparent predictions", 1545–50.

several authors have noted, algorithms are not purely neutral task-executers, much to the contrary, they are the result of a series of policy and technical decisions carried out by humans and, as such, are not only prone to error but can (and do) reflect the values of those that design them and, more importantly, of the businesses that deploy them.[89] Seemingly technical decisions can have profound and real-life effects.[90] Even in the context of AI technologies, especially those based on machine-learning, which result from a more autonomous analysis of the data by the program, the pitfalls of bias and error can be found.[91] The process of selecting the data that feeds the machine learning algorithm,[92] for instance, it has had an indelible impact on the outputs of the software, as Amazon's attempt at implementing a hiring algorithm exemplifies.[93]

All the issues listed above relate to the design of the algorithm/AI technology, but these are not the only concerns that can be identified in the use of such technologies. Other issues relating to the interpretation of the algorithmic outputs and even the purpose of its deployment raise questions, questions that, while mostly posed by scholars and experts, impact the average user. Indeed, it is quite possible that these questions would preoccupy the average user as well if they were aware of how much of their behaviour online is governed by algorithms – which is not the case.[94] Transparency is, therefore, an issue of importance in the digital world and its importance is inextricably linked to the increasing use of automated technologies and to the increasingly impactful and complex decisions they are being called to make, such as those affecting credit scores,[95] the attribution of social benefits[96] or the targeting of tax audits.

[89] See, *inter alia*, Pollicino and De Gregorio, "Constitutional law in the algorithmic society"; Razvan Amironesei *et al.*, "The case for interpretive techniques in machine learning", in *Fake AI*, ed. Frederike Kaltheuner and Razvan Amironesei (Manchester: Meatspace Press, 2021), 76–87; Donghee Shin, "User perceptions of algorithmic decisions in the personalized ai system: perceptual evaluation of fairness, accountability, transparency, and explainability", *Journal of Broadcasting & Electronic Media* 64, no. 4 (2020): 541–65, https://doi.org/10.1080/08838151.2020.1843357.

[90] Zarsky reviews the transparency (or lack thereof) of predictive algorithms as implemented by the state, citing as an example the use in the United States of these algorithms by the IRS to select the individuals that should be subject to tax auditing. Zarsky, "Transparent predictions".

[91] The authors alert to the dangers of over-reliance on benchmarked datasets, for which there is a tendency to associate a high degree of neutrality, which could result in wide-spread and systematic reproduction of biases throughout the industry. Amironesei et al., "The case for interpretive techniques in machine learning", 81–84.

[92] For an overview of the functioning of machine learning technologies, see, Arlindo Oliveira, *Inteligência Artificial* (Lisbon: Fundação Francisco Manuel dos Santos, 2019), 59–69.

[93] By providing its algorithms with the resumes the company had received over the past ten years before the implementation of the software, the company expected the program to assess new applicants and provide recruiters with the top contenders. However, there was an implicit bias in the dataset which related to the fact that most applicants were men. The algorithm interpreted this as a one of the characteristics successful applicants should have and excluded women from the results. See Dastin, Jeffrey, "Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters,* 11 October 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

[94] Shin, "User perceptions of algorithmic decisions in the personalized ai system", 547–48.

[95] Pasquale, "A rule of persons, not machines: the limits of legal automation", 9.

[96] The Dutch authorities implemented an algorithm that was meant to identify fraud in child benefits, but which resulted in consequences, such as the recognition of tax debts or the ineligibility for social benefits or tax breaks, on the basis of the suspicion identified by the algorithm. See Heikkilä, Melissa, "Dutch scandal serves as a warning for Europe over risks of using algorithms", *Politico*, 29 March 2022, https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.

In this sense, Zarski, focusing primarily on their use by states, reviews the issues caused by predictive algorithms and recommends steps to increase transparency in each stage of the development and implementation of predictive models. The author identifies three stages in the development and implementation of predictive algorithms, namely, i) collection of data and aggregation of datasets, ii) data analysis, and iii) usage. To introduce transparency requirements in the first stage, data collection and aggregation of datasets, according to the author, would require, at least, the disclosure of the type of data and databases used to build the algorithm. If considered more extensively, transparency in this stage would require the disclosure of the actual data underlying the model.[97] In the data analysis stage, Zarsky considers that transparency could be achieved not only by disclosing the technology used to develop the model, such as the software that was used, but also by revealing the human decisions taken in this stage – *i.e.* support levels of the inferences and the confidence levels in the outputs arrived at by the analysts and an explanation on how they arrived at them.[98] Finally, in the usage phase, the author notes how discussions on the issue revolve around a call for transparency regarding the particulars of the predictive model, the strategies and practices for using said data. Fulfilling this condition might require the production of "*new information*", essentially, an *ex post* assessment of the impacts of the implementation of the predictive model.[99]

De Gregorio, assessing the European framework governing content moderation and data protection, also links transparency to privacy, individual autonomy and democratic concerns. In this sense, the author recognises a new role in transparency: that of reducing informational asymmetry.[100] Noting the opaqueness of the functioning of automated decision-making algorithms and the increasing datafication of human behaviour, De Gregorio points to the potential that digital technologies have of becoming instruments of social control. In his words, "*individuals are increasingly transparent operating in a virtual world which is increasingly opaque*."[101] Transparency here functions as a sort of equaliser, looking to bridge the informational gap between users and online platforms and other intermediaries.

Focusing on the impacts of opaqueness on democracy, De Gregorio highlights the lack of transparency in content curation and moderation practices and the resulting fragmentation of the public sphere due to the birth of multiple online public spheres, calling for greater transparency in these processes (and greater control on the part of the users).[102] The issue is exacerbated by the lack of information on the content moderation processes and by the deployment of automated decision-making technology. The author calls attention to the fact that the guidelines used by human content moderators are kept as private documents, hidden from public sight, and recognises the lack of transparency of the functioning of content moderation algorithms which run the risk of becoming "*opaque self-executing rules*."[103] As such, the solution must involve, on the one hand, the provision of an explanation of the content moderation rules to users, both *ex ante* and *ex post* (when content is removed or blocked), on the other, the introduction of the human-in-loop principle – here

[97] Zarsky, "Transparent predictions", 1523–24.

[98] Zarsky, "Transparent predictions", 1524–26.

[99] Zarsky, "Transparent predictions", 1527–30.

[100] De Gregorio, *Digital constitutionalism in Europe*, 50.

[101] De Gregorio, *Digital constitutionalism in Europe*, 217.

[102] De Gregorio, *Digital constitutionalism in Europe*, 169–76.

[103] De Gregorio, *Digital constitutionalism in Europe*, 184–86.

fulfilling a role not only as a due process guarantee (the possibility of getting a judgement by a human being) but also as a transparency safeguard, allowing users to rely on a "*human translation*" of the content moderation process.[104] To finalise, we highlight how the author points to transparency and procedural safeguards as the formula that European digital constitutionalism found to ensure more autonomy and diversity in online content.[105]

From the preceding analysis we can discern the different purposes that transparency seeks to accomplish from a constitutional perspective, as well as some of the manifestations that academia recognises or advocates for in the digital realm. Transparency is, therefore, seen as a necessary (though not sufficient) condition for the functioning of democratic societies as a check on power, bringing the activities of those who wield it to light and empowering civil society to demand (or not) a response to abuses. Transparency reinforces privacy and individual autonomy where it informs individuals of their rights and the processes that govern their digital lives, bridging the informational gap between users and intermediaries. Finally, transparency calls for the disclosure of information to the wider public and to specialised bodies as a conduit for the development of knowledge, as an allowance for crowdsourcing of information and enabler of good policymaking.

Ensuring this value is upheld in the digital realm requires that transparency be viewed in a new light, especially considering the generalisation of the use of machine learning technologies and automation of decisions. As such, transparency in the "*algorithmic society*" requires that information about the use of predictive algorithms and automated decision-making technologies be known to the user and that the core elements related to the data that underlies such technology, as well as the policy decisions that informed its development, be disclosed. Additionally, and more specifically regarding online platforms, transparency would manifest by disclosing the internal guidelines used by human analysts when reviewing content and by affording the user the possibility of having a "*human translation*" of the automated processes that affected them – here transparency links to the issue of explainability of automated decisions.

2.4. Reaching a working definition

Considering the values we have identified in the literature and recounted above, we propose the following working definition that highlights the objectives, values and responses that digital constitutionalism seeks to promote, building on the provisional definition we advanced in the beginning of this chapter. Digital constitutionalism is the ideology that promotes the adaptation of constitutional values and fundamental rights to the digital environment, clarifying the new facets they assume in this new arena and extending their reach beyond the traditional vertical effect (*vis-à-vis* the state), with the intent to limit and re-balance the exercise of power online, namely by devolving power to individuals in their interactions with digital services providers, implementing due process safeguards that promote a more predictable and accountable environment and by introducing transparency requirements that reinforce users' ability to enjoy and enforce their rights online.

[104] De Gregorio, *Digital constitutionalism in Europe*, 207–11.

[105] De Gregorio, *Digital constitutionalism in Europe*, 201.

3. Conclusion

We started this paper inspired by George Steiner's inquiries into the idea of Europe, laid out in a book that was first published at a time when the continent was facing an existential and constitutional crisis. In his efforts to understand whether the idea of Europe is salvageable, Steiner recounts Europe's rich history and traditions, paying attention to the role that cultural diversity played in fostering a shared commonality of values. In his pursuit for an answer to the moment of crisis he recognised Europe to be facing, the author finds that the solution lies, as it usually does, in turning back to the humanist principles that have informed the last centuries of European development.

From where we stand, we can only note that Europe is, yet again, facing a crisis – and a constitutional one at that – and that some of the woes Steiner expressed have become more concrete realities then they were, nearly 20 years ago. While many other factors characterise this moment of crisis, the role that the internet and some of its more influential stakeholders played is, undeniably, central to this crisis. In opposition to the new café that we expected the internet to become, it seems that instead we have been trapped in a digital version of Bentham's panopticon, which, good intentions notwithstanding, is designed as something even more nefarious than a surveillance tool, it is, rather, a behavioural control mechanism. In the panopticon, the warden sits at the centre of the prison and the prisoners in the walls surrounding it, the light shining through behind them allows for constant surveillance by those in the centre and limits the visibility of those in the cells. The warden always has full view of the prisoners, but the latter do not know when they are being watched, as such they have to conform to the desired behaviour of the prison staff at all times.

In this context, we cannot agree with Orly Lobel when, reviewing the mechanisms for user feedback (*i.e.* user rating systems), the author states that these provide for a "*true foucauldian panopticon*", hinting that such feedback mechanisms allow for two-way surveillance (the platform in relation to the user and the user in relation to the platform). As we strived to highlight in the introduction of this paper, the current set-up is one of imbalance, whereas online platforms have a complete view over our activities online, obfuscate the processes that they implement to govern their spaces and guide our behaviour towards data-collection and monetisation, we, as users, have little view over their operations, little understanding as to how they are structured and, most importantly, how they impact us. In this light, while the notion of the panopticon might be a suitable descriptor, it does not seem that the users have been invited to the central tower. Indeed, rating mechanisms are more akin to wrapping our fingers on the prison cell door then to holding its keys in hand.

It is precisely for this reason that we believe we are facing a constitutional crisis. Although market imperatives and a conservative approach towards interferences with private freedoms were justifiable in its inception and enabled the development of the internet we know today, the absence of adequate constitutional safeguards, which we take as a given in all other aspects of our lives and societies, seem to have contributed to the difficulties that the digital realm is now facing (and causing). It is for this reason that we look to digital constitutionalism with hope and, as we have observed throughout this text, so it seems that the EU is also placing their hopes and efforts in a digital constitutionalism approach to addressing the issues caused by digital technologies, restating the importance of individual autonomy as a central value of the European ethos.

In this setting and having summarised the concerns with digital technologies that scholarship has identified, we find it fitting to recount the values of digital constitutionalism we endeavoured to isolate and densify in the second part of this paper – values whose purpose is of counteracting the aforementioned absence of constitutional safeguards.

As seen, we found that the first value that digital constitutionalism holds is that of limitation of powers, in this case, the limitation of digital services providers' and, specifically, online platforms' powers with a view to re-balance the positions of users and service providers in their interactions. To this end, such re-balancing implies not only the limitation of the service providers' powers, but also the reinforcement of users' position, by affording them safeguards and creating actionable rights.

On the other hand, the rule of law also appears in the literature as a core value of digital constitutionalism, as a function of the objective of limiting powers. As such, the rule of law is seen as a restriction on powers in the sense that it requires that the discharging of powers be limited by rules, including the powers that allow for the generation of such rules. Additionally, the rule of law mandates that those rules be known beforehand by those against whom power is discharged. It also requires that persons understand the decisions against them and that they be afforded an opportunity to contest such decisions. In the digital context, and in view of the increasing use of algorithmic decision-making, the rule of law requires that decisions affecting persons be, at least, supervised by human beings and that, when means of recourse against said decisions are activated, the judgement on the merits of the decision be handed down by a human being.

Finally, we see that transparency is a common value in digital constitutionalism scholarship. In this context, transparency is viewed also as a check on power, providing insight into the functioning of the services that affect our lives, fostering individual autonomy by bridging the informational gap, allowing for more informed decisions on the part of the users, and for the development of open-source knowledge regarding the "*algorithmic society*." Concerning its implementation by digital services providers, academia highlights the concern with the wide-spread use of algorithms and advocates that users should, at the very least, be: (i) made aware of when they are interacting with algorithms; (ii) given meaningful information regarding the purposes of such use; and (iii) informed about the processes and data used for their functioning. To this end, transparency calls for a human translation of the algorithmic results as well as for the sharing of meaningful information regarding non-algorithmic processes (such as those involved in content moderation), namely the procedures followed in that regard.

Having identified these values as core elements of digital constitutionalism and the related literature, it is now time to turn to the EU *acquis* in search of reflections of the same. The purpose of future investigation in this matter, on our end, will be to assess, first, the adherence by EU law and policy to digital constitutionalism principles and the level of density with which they can be gleaned in this corpus. A final objective, upon verification of the existence of such principles, will be to reach a tentative definition on the same.