Received: 3 May 2023 | Revised: 12 June 2023 | Accepted: 29 June 2023

DOI: 10.1111/eulj.12472

SPECIAL ISSUE ARTICLE

WILEY

The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism

Oreste Pollicino*

Abstract

The paper explores the evolution of private powers in the digital landscape, developing a quadrangular systematisation of such a phenomenon based on four main aspects: space, values, (private) actors, and (digital) constitutional remedies. Taking a trans-Atlantic approach, the paper shows how these categories, typical of constitutionalism, apply to the context of the Internet and of new digital technologies both in the United States and in Europe. On the one hand, the United States has up to now maintained the supremacy of the notorious Section 230 of the Communications Decency Act. On the other hand, European legislation has undergone a significant change, moving from a phase of digital liberalism, of which the 2000 e-Commerce Directive is the emblem, towards a new era of digital constitutionalism, passing through the age of judicial activism of European courts. In this sense, Europe has increasingly attempted to introduce limits to private (digital) powers, with a view to better protect and enforce (also horizontally) users' fundamental rights. Additionally, the evolution of digital constitutionalism, from a vertical-sectoral approach to a horizontal and procedure-based one, significantly showcased by the recent Digital Services Package, is underscored, signalling the recent movement of the EU into its second phase of digital constitutionalism. In this respect, the paper argues that the great benefit of stressing the procedural dimension, which may be defined as a European application of "due (data) process" to the relationship between individuals and private powers, is that it is potentially able to help consolidate a (necessary) trans-Atlantic bridge.

1 | INTRODUCTION

What are the signs and constituent elements of private digital power? Why have the emergence and consolidation of this power been so significant for constitutional law, and why is it not (or no longer) simply a matter that can be

* Oreste Pollicino, Full Professor of Constitutional Law, Bocconi University, Milan (Italy); Member of the Management Board of the European Union Agency for Fundamental Rights.

dealt with using the instruments of antitrust law? When and why did the most important digital companies at global level metamorphose from economic operators into full-blown private powers often in competition with public authorities? What tools are available to constitutionalism, considered from a trans-Atlantic perspective, to counter the exponential expansion of these powers, taking account of the relevant constellation of the rights in play, from freedom of expression through the protection of freedom of enterprise to the right to privacy?

These are the research questions that the following pages will attempt to answer.

There is a growing literature related to the relationship between constitutional law and private powers in cyberspace and to the emerging notion of digital constitutionalism.[1] However until now, there have been no analyses of the constitutive elements of the geometry of digital power, of the process of "transfiguration" that has transformed private actors in cyberspace from economic operators into genuine private powers, or of the reaction that this transfiguration has triggered on the part of modern constitutionalism. Constitutionalism has been forced to identify a new scope of action in order to remain true to its original mission of limiting power in order to ensure respect for fundamental rights, the rule of law and democracy which may be affected negatively in the absence of adequate mechanisms of checks and balances. Specifically, this study will shift its focus from a classical vertical approach juxtaposing authority and freedom towards a horizontal approach. The objective will be to identify the most suitable instruments for limiting and containing the private power wielded by major online platforms. A new geometry of digital powers will be proposed, based on a quadrangular shape, and this shall represent the main argument and the added value to the existing literature.

The reference to geometry has been used already by Jack Balkin who, noting how digital power (in particular with regard to freedom of expression) is characterised by the fact that it transcends the binary relationship between public power and individual user, has incorporated a third level (or corner) and on this basis has recently coined the metaphor of 'free speech as a triangle', with the third corner being occupied by private platforms.[2] Within the account proposed here, the geometry of digital power will instead be conceptualised as having a quadrangular shape corresponding to the four constitutive dimensions: 1. space; 2. values; 3. actors; and 4. remedial (with the fourth focusing on the responses of constitutionalism to the consolidation of that power).

The reason for this quadripartite division may be summarised as follows: within the new algorithmic society, private transnational corporations (operators) are *de facto* increasingly performing public functions through the "governance" of digital spaces (space). Within this context, the value framework that characterises the European legal order on the one hand and the US system on the other hand, especially as regards the balancing of the rights at play (axiological dimension), is fundamental in understanding why different constitutional reactions by different legal orders are heavily influenced by the value-based approach which characterises the respective bills of rights and the constitutional case-law of the legal orders at stake. The last relevant corner is the one corresponding to the constitutional remedies dimension. It bears the question of what instruments are available to public law to counter and to limit private digital powers, which appear, however, to be following an increasing growth trajectory.

The article will therefore be structured according to this quadripartite understanding corresponding to the quadrangular shape of the new geometry of digital power(s). Section 2 will consider the first constituent element of the mentioned geometry, namely space (and territory). Section 3 will focus, looking at the second constitutive element, on trans-Atlantic diversity in terms of the values and judicial frames endorsed, respectively, by European courts and by the US Supreme Court as regards their approach to technology. Section 4 will then focus on the third constituent element, involving the major platforms and their metamorphosis into private powers. Finally, Section 5 will examine, as the fourth and last element of the quadrangular shape, the potential responses from US and European constitutionalism to limit the amplification of private digital power. The article will then end with some brief concluding remarks.

[1]G. De Gregorio, 'The Rise of Digital Constitutionalism in the European Union', (2021) 19 *International Journal of Constitutional Law*, 41; O. Pollicino, *Judicial Protection of Fundamental Rights Online: A Road Towards Digital Constitutionalism?* (Hart, 2021); G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press, 2022); E. Celeste, 'Digital Constitutionalism: A New Systematic Theorisation', (2019) 33 *International Review of Law, Computers & Technology*, 76; N. Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms', (2018) 4 *Social Media + Society* (2018), 10.1177/2056305118787812; D. Redeker, L. Gill and U. Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights', (2018) 80 *International Communication Gazette*, 302.
[2]J.M. Balkin, 'Free Speech is a Triangle', (2018) 118 *Columbia Law Review*, 2011.

From a methodological point of view, the investigation will cover, from a transatlantic perspective, the European Union and US experiences. This choice does not wish to deny the emergence and consolidation of other regional areas with a significative impact on a geopolitical digital landscape, such as the Chinese model. Nevertheless, the privileged focus of this analysis aims, on the one hand, to be confined to liberal democracy experiences and, on the other, to critically point out the need to take more seriously the transatlantic bridge related to the biunivocal migration of constitutional ideas, from one side of the Ocean to the other, connected with new digital technologies.

2 | SPACE (AND TERRITORY)

Space is the first structural aspect that has long been a neuralgic issue in the debate concerning online regulation, following its emergence as a new frontier. At the dawn of cyberspace, the new digital dimension brought promises of freedom, first and foremost from state control. The main argument which will be developed in this regard is how space has been one of the privileged "playgrounds" where the alleged anarchic nature of cyberspace, on the one hand, and, on the other, the European Union's ability to apply its relatively demanding legislative frame, also in relation to digital platforms having their server farms outside the European Union but providing their services to European citizens, have been challenged.

It is sufficient to consider the 'Declaration of the Independence of Cyberspace' by John Perry Barlow of 1996, which solemnly addressed states as follows: 'Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.'[3]

As has rightly been pointed out, within this perspective, there is 'apparently no role and no power for states. On this view, national actors are *elsewhere*; they are unable to dictate their sovereignty and to extend enforcement of legal norms within a space idealised as a separate territory'.[4]

Twenty-five years later, it may readily be concluded that history subsequently resulted in the emergence of a highly different reality from that envisioned by Barlow. There are at least two reasons for this. The first is that nation states have demonstrated that they are able not only to regulate but also to "hyper-regulate" cyberspace which, it is important to recall, is comprised not only of bits and bytes but also first and foremost of physical infrastructures and undersea cables, and thus has a "real-world" dimension, forming part of that analogue world from which Barlow rather unrealistically (self) declared independence. Consider also how non-democratic systems such as that in China have been able to create the "Great Firewall", and also recently how, following its invasion of Ukraine, Russia established virtual walls as well as disinformation and censorship strategies, which caused very tangible and significant harm to the exercise of freedom of expression and the right to be informed.

The second reason is that what should have been, according to Barlow's utopian vision, a new world free from conditioning and domination, in which the community of users had the ability to self-regulate in accordance with their reference framework of values, ended up turning into a space that proved to be highly accessible for private powers. Although they did not by any means realise the dystopian visions (which were just as harmful as utopian views), for example of Morozov[5] and in part also of Zuboff,[6] they did, however, undoubtedly condition the process of self-determination of users, which should have acted as the cornerstone for building the space imagined by Internet pioneers.

[3]J.P. Barlow, 'A Declaration of Independence of the Cyberspace' (Electronic Frontier Foundation, 8 February 1996), available at https://www.eff.org/cyberspace-independence (accessed 2 May 2023).

[4]M. Bassini, 'Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione', (2021) 2 *Rivista di Diritto dei Media*, 86.

[5]E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (PublicAffairs, 1997).

[6]S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

It was also due to the influence of these initial viewpoints, which *ex post* proved to be highly naive, that the very first commentators who engaged with the advent of cyberspace and its legal consequences within US literature immediately split in two groups: those who supported a cyber-anarchist viewpoint;[7] and those, by contrast, who argued against the normative and descriptive premises underpinning that viewpoint.[8] The antithetical positions of state regulation, which were perhaps inspired also by a "libertarian prejudice" inclined to mistrust the subjection of "new" phenomena to public law regulation, were based on the recognition of a supposed superiority of self-regulation within cyberspace.

As is known, these concerns quickly gave ground to other viewpoints that were not hostile to state regulation. They found it easier to take root, amongst other things, as a result of the very first rulings within the case-law which, above all in the United States, acknowledged that cyberspace was not so special as to detach the activities that occurred within it from any rule of conduct that had already been adopted to govern the 'world of atoms'.[9] More specifically, the US courts' response to the anarchist viewpoint, in establishing their own jurisdiction over cases involving online disputes, confirmed that there are adjudicators within a space that had been thought to be immune to regulation by public authorities.[10] This could result in a paradoxical scenario under which 'the area of Internet law, for years considered the most emblematic expression of the limitations of national law in facing the challenges of globalisation, would, by contrast, prove to be one of the few fields of law still encapsulated in national law, in which not only a global approach, but also a transnational one risks proving not to be fully adequate'.[11]

There is at least one fundamental step that illustrates the difficulties associated with the spatial element in cyberspace. In the United States, one of the main problems that lawyers and other legal practitioners were forced to engage with concerned the risk that the Internet, thanks to the ease with which it could be accessed, might turn into a vehicle for conveying banned or restricted content in the "real world",[12] resulting in a free-for-all ability to circumvent prohibitions imposed by law. The problem was well exemplified by the debate surrounding the "cyberporn panic", which moreover resulted in the first attempt to regulate cyberspace in the Communications Decency Act (CDA)[13] passed by the US Congress in 1996. The Act not only regulated the role of intermediaries for the first time but also introduced some limitations on online access to manifestly offensive or obscene content, riding the wave of the concerns mentioned above. The next year, the US Supreme Court ruled that these provisions violated the First Amendment as they imposed excessive and disproportionate restrictions on the constitutional right of an adult public to access explicit content. Its judgment in *Reno v. ACLU*[14] is significant not only due to the courageous stance taken to uphold freedom of expression in the face of a significant interest such as child protection, but also because it acknowledged the development of a new means of communication and its characteristics, taking the view that the digital world could perhaps offer an opportunity for realising the digital metaphor of the "marketplace of ideas" evoked by Justice Holmes in 1919.[15] The Court's judgment could not have foreseen that the nature of the digital world was shortly set to change radically, shifting towards an oligopoly of which there were, however, no signs at that time.

More recently, in the *Packingham* case,[16] the Supreme Court went further than simply reasserting within the digital world the notion embraced in *Reno* of the free marketplace of ideas, asserting somewhat controversially that 'While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the

[7]D.R. Johnson and D.G. Post, 'Law and Borders: The Rise of Law in Cyberspace', (1996) 48 *Stanford Law Review*, 1371.
[8]On this matter, see also J.L. Goldsmith, 'Against Cyberanarchy', (1998) 65 *University of Chicago Law Review*, 1199.
[9]See U. Kohl, *Jurisdiction and the Internet* (Cambridge University Press, 2009); D.J.B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford University Press, 2017); J. Hörnle, *Internet Jurisdiction Law and Practice* (Oxford University Press, 2020).
[10]O. Pollicino and M. Bassini, 'The Law of the Internet between Globalization and Localization', in M. Maduro, K. Tuori and S. Sankari (eds.), *Transnational Law: Rethinking Law and Legal Thinking* (Cambridge University Press, 2014), 346.
[11]Ibid., 347.
[12]See also L. Lessig, 'The Law of the Horse: What Cyberlaw Might Teach', (1999) 113 *Harvard Law Review*, 501.
[13]Communications Decency Act (1996).
[14]*Reno v. ACLU*, 521 U.S. 844 (1997).
[15]*Abrams v. United States*, 250 U.S. 616 (1919).
[16]*Packingham v. North Carolina*, 582 U.S. (2017).

exchange of views, today the answer is clear. It is cyberspace—the "vast democratic forums of the Internet"'. This was a clear position statement, perhaps a little naive and in places risky, which proposed an equivalence between the classical *agorà* of the world of atoms and the exchange of ideas, which can be ensured (or not) by the free (or less free) digital *agorà*.

With regard to the spatial issue, there has equally been pressure within the case-law on this side of the Atlantic to endorse the view that, irrespective of where the new digital powers' IT infrastructure is actually located, if they provide their services in the European digital market, they must also submit to the rules, and thus the system of values, inherent to the constitutional traditions common to the Member States. That case-law has obviously gestated within a specific environment (and it could not be otherwise) different from that of the US case-law, which was reacting to the anarchist perspective described above. Whilst the latter inevitably had to focus primarily on the need to protect freedom of expression, the ECJ's case-law has given priority to data protection, the First Amendment so to speak of European constitutionalism. Indeed, given the different prevailing axiological paradigm, the position could not have been more different.[17]

Within this particular area, the case-law of the Court of Justice has not only given clear priority to the right to data protection over and above other protected interests but has also endorsed the notion that, in spite of the fact that data processing is now largely digitalised, the rights of individuals and national borders 'established in order to protect them' still have some significance.

Two jurisprudential moves appear to be illustrative of this approach. They will also be addressed below in Section 5 focusing on the reactions of legal systems' digital sovereignty to the emergence of digital powers, and specifically on the activism of the ECJ in enforcing privacy rights. The ECJ's first significant decision was given in the famous *Google Spain* case.[18] This judgment is not particularly significant for our present purposes due to its substantive content (the application of data protection rules to a search engine *qua* processor), but rather on account of its underlying premise: the extension to persons established outside the EU that process the data of individuals resident in the Member States of the rules set out at that time in Directive 95/46/EC.[19] The Court of Justice thus pre-empted the General Data Protection Regulation (GDPR),[20] where the current Article 3(2) now contains a similar provision, which firmly asserts the principle that the economic exploitation of the personal data of European citizens cannot be detached from and shorn of the guarantees required under EU law, which establish the highest level of protection as enshrined, *inter alia*, in Articles 7 and 8 of the Charter of Fundamental Rights and Article 8 ECHR. The *Google Spain* judgment thus marked the point of no return, establishing the need also for non-EU operators, which are largely from the United States, to comply with the significant body of EU laws, which evidently reflect the axiological dimension of the constitutional traditions common to the Member States. The question of space is thus inherently linked to the issue of sovereignty also in cyberspace. Nothing new for constitutional law!

The second leading case in this area, which sought to demonstrate that space and more specifically territory are essential features of power also in its digital dimension, was the *Digital Rights Ireland* case.[21] In this case, the ECJ annulled the 2006 Data Retention Directive[22] on the grounds that it violated the Charter of Fundamental Rights, also insofar as 'that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control … by an independent authority … is fully ensured'. This goes far

[17]B. Petkova, 'Privacy as Europe's First Amendment', (2019) 25 *European Law Journal*, 140.

[18]Case 131/14, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

[19]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[20]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) [2016] OJ L119/1.

[21]Cases 293/12 and 594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238.

[22]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

beyond the issue of determining the applicable law, as the operative term is technically "within", which demonstrates that this fundamental category of constitutional right is alive and kicking "within" cyberspace, despite attempts to conceptualise a virtual space comprising (non-)rules and categories that are detached from their counterparts in the world of atoms.

3 | VALUES AND THE RELEVANCE OF JUDICIAL FRAME

Moving to the second constitutive element of the quadrangular shape related to the geometry of digital power, as mentioned above, the spatial dimension is closely linked to the debate concerning the protection of the rights at stake as well as the value framework used as a backdrop for balancing operations by courts and lawmakers, which has, as such, an effect on the reinforcement, weaking or containment of new digital powers. This is not an irrelevant debate as it vividly exemplifies the existence of different regulatory models underpinning the predominance of equally different values.

In fact, digital power affects not only the freedom of expression of individual users but also other interests relevant under constitutional law, such as for instance privacy, data protection equality and non-discrimination. It is no coincidence that such values represent the keystones of respectively US and European constitutionalism,[23] which are not always readily reconciled with each other.

The different outlooks extend, even more deeply, to the role that digital technology can play as a factor in the expansion of freedoms and rights held in the world of atoms, or by contrast in increasing the risk (as compared to the position in the world of atoms) that those very same rights may be harmed. These two interpretative options can have extremely significant implications for the way in which the emergence of the new digital order can be observed, and consequently for the new forms of power that it entails.

Considered from this perspective, it may be interesting to compare how the "digital factor" and its capacity to enhance or reduce the impact of emerging private powers is understood by US courts and by their counterparts in Europe, drawing specifically on the concept of "frame" from philosophy of language,[24] and deriving from it the notion of the "judicial frame". We shall focus in particular on how the different framework values adopted respectively by the ECtHR in Strasbourg and the US Supreme Court in relation to the protection of freedom of expression online can be decisive in identifying the level of protection that should be granted to that freedom when it comes into conflict with other fundamental rights. This is obviously crucially important in assessing those balancing operations that are necessary in order to deal with new digital powers.

There is a profound underlying fissure between the US approach focused on the First Amendment and a strictly European approach based on the axiological predominance of data protection rights. Although the mismatch between these two respective outlooks has already been discussed above, it is important to consider in greater detail a few critical aspects.

Freedom of expression has historically been interpreted as the North Star of US constitutional law, as the right characterising the entire legal order. This approach is apparent within the value framework embraced by the Supreme Court, which, since its very first judgments in this area, has been inclined to exalt the unprecedented libertarian dimension to the Internet. In the eyes of the US Supreme Court, the new free marketplace of ideas immediately offered a framework and a new space for the exercise of this freedom, which must be considered through lenses and according to categories that differ from those applied to traditional media. This resulted in the choice in

[23]See M. Rosenfeld and A. Sajó, 'Spreading Liberal Constitutionalism: An Inquiry into the Fate of Free Speech Rights in New Democracies', in S. Choudhry (ed.), *The Migration of Constitutional Ideas* (Cambridge University Press, 2007), 142. See also J.M. Balkin, 'Cultural Democracy and the First Amendment', (2016) 110 *Northwestern University Law Review*, 1153. With respect to the specific framing of the right to data protection within European constitutionalism, see Petkova, above, n. 17.

[24]According to Lakoff, from a cognitive perspective, frames must be intended as "communication protocols" that are necessary to connect language and cerebral circuits. G. Lakoff and M. Johnson, *Metaphors We Live By* (University of Chicago Press, 1980), 61.

Reno v. ACLU to adapt the metaphor of the free marketplace of ideas from Justice Holmes' famous dissenting opinion, the enduring relevance of which could be called into question in the light of the changes that affected the Internet over the first few years of its life.

This ruling, and the other ones analysed in Section 4, are indicative of a clear inclination of the US Supreme Court to safeguard the exercise of free speech rights, and consequently to guarantee a kind of "*carte blanche*" for Internet service providers through an instrument that was considered to be capable of ensuring an extraordinary expansion in their margin for manoeuvre. This value framework evidently resulted in the expansion of private digital power, especially during the period immediately following the creation of cyberspace.

Moving now to the judicial frame that has characterised the relevant case-law of the European courts, the European legal order has a different value framework in axiological terms as regards protection for freedom of expression. In simple terms, we can state that in Europe this right competes on an equal footing with other fundamental rights and does not enjoy the axiological priority that is afforded to the status and interpretation of the First Amendment under US law.

This configuration is confirmed by at least two elements, both of which can be identified within the text of the ECHR. First and foremost, Article 10(2) ECHR provides for something that would be unacceptable within US constitutionalism. It expressly codifies limits and hence restrictions on that freedom, and also on all other rights and freedoms provided for in the Convention, where justified based on the principle of proportionality, representing a paramount element of European constitutionalism.

Second, embracing another concept that is unknown within US constitutional law, the ECHR (and also the EU Charter of Fundamental Rights) expressly provides for the possibility of the abuse of rights,[25] confirming the approach based on non-absolutism, balancing and equal status among rights that is characteristic of the constitutional traditions common to the Member States.

It is therefore no surprise that, starting from value contexts with such different facets (as well as even more fundamental differences), an analysis of the relevant case-law appears to point towards a judicial frame that is generally opposed to that prevailing within US courts. Rather than exalting the Internet as a driving force for freedom of expression, that value frame conceptualises and gives weight above all to those aspects of it that are critical in the face of competing rights.

It is no coincidence that this stance characterised by greater caution has resulted in judgments that warn about possible risks for other rights equally deserving of protection. This approach is, moreover, justified by the more secular outlook of European states, especially when compared to the United States, which is visibly apparent also within the relevant provisions of the Charter of Fundamental Rights and the ECHR.

Turning now to the cases in which the ECtHR has been called upon to rule on applications resulting from supposed violations of freedom of expression online, a clear trend is apparent to rein in the expansive scope which—at least in word—had distinguished the previous case-law concerning the application of Article 10 in the world of atoms.[26] This new nuanced view of the scope of freedom of expression online appears to be rooted in the conviction that the use of digital technologies entails a greater potential to cause harm to the other interests with which the exercise of free speech must engage.[27] Naturally, this "relative" and "fall-back" status within operations concerning the balancing of the fundamental rights protected by the ECHR is certainly nothing new. However, this status appears to have been accentuated within Internet case-law, which has had immediate repercussions on attempts to rein in the expansive reach of digital technology, as well as the algorithmic power behind that technology.

[25]European Convention on Human Rights, Nov. 4, 1950, 213 UNTS 221, art. 17.

[26]App. 5493/72, *Handyside v. United Kingdom*, ECLI:CE:ECHR:1976:1207JUD000549372. In this decision, as well as in the case-law discussed below, it is possible to identify clear indications pointing towards an expansion of freedom of expression, the scope of which is arguably capable of embracing, in the European Court of Human Rights' interpretation, also those expressions that do not offer a significant contribution to the democratic process and to the construction of public opinion, and that express a content which is offensive, shocking and disturbing.

[27]O. Pollicino and M. Bassini, 'Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis', in A. Savin and J. Trzaskowski (eds.), *Research Handbook on EU Internet Law* (Edward Elgar, 2014), 508.

This "narrow" reading can be traced back to the 2011 judgment in *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*,[28] and has been reiterated in various decisions including at least *KU v. Finland*[29] and *Delfi AS v. Estonia*,[30] a decision issued by the Grand Chamber in 2015 which also confirmed the general trend described above that is more favourably inclined towards possible restrictions on freedom of expression online.

To summarise and inevitably simplify the respective scope of the US and European judicial frames with regard to online regulation, and hence the containment of digital power, they appear to be inspired by diametrically opposite approaches. The US approach, which is inspired by a firm conviction that digital technology is inherently capable of amplifying freedoms (digital trust), assumes that any content regulation will not provide any increased benefits for freedom; the European approach, on the other hand, views new technologies with greater scepticism (digital distrust), considering it likely that technology will jeopardise other rights, and as such asserts the need for, and indeed the legitimacy of, corrective measures that may limit the exercise of free speech rights.

It should be added that the ambition in Europe—which is not at all untoward—of guaranteeing a high level of data protection for European citizens also in relation to processing by digital operators, which are largely American, risks being frustrated if the conditions are not met for the eagerly awaited "trans-Atlantic bridge" to enable communications between the two continents and their respective legal systems. The attempts hitherto made, which are exemplified by the *Schrems* case,[31] show how the US can still demand a "geographical rent" within negotiations and how Europe has been persisting in a "reactive" strategy based essentially on judicial review. It must also be hoped that the agreement recently reached in May 2022 can mark a clear course change, moving beyond the communication difficulties that beset previous attempts at engagement. This will be a key test, also in light of the forthcoming changes in Europe, which will be discussed in Section 5 on constitutional reactions in the United States and the European Union to the amplification of digital power. These include, in particular, the Digital Services Act (DSA)[32] and the Digital Markets Act (DMA),[33] although it is also important not to overlook the changes set to be introduced by the Data Governance Act[34] and the Artificial Intelligence Act.[35] In other words, the dialogue is still a work in progress, although it throws up the same problems that are common within the world of atoms: different sensitivities arising in relation to different interests, which are difficult to reconcile with one another. Thus, even in the digital world, borders have never played such an important role.

Based on this analysis, the key distinction appears to be between a (judicial) frame of resistance to technology (rooted in Europe) and an alternative frame that is more open to technology (which prevails within the relevant US case-law). It is clear that the former value frame, which characterises the argumentative structure used in European case-law, tends to view with greater suspicion those private powers that use digital technology as an instrument for developing their own business models although also—which is more interesting from the constitutional perspective—as a genuine digital *agorà*. On the other hand, the immediate consequence of the US frame is to valorise the digital public forum, in some cases regarding it as equivalent (albeit in a controversial way) to privileged *loci* of public debate within the world of atoms. All of this obviously benefits the new intermediaries that often use as a shield the extensive protection granted by the First Amendment for freedom of expression.

In any case, regardless of which particular frame is chosen, this operation is never neutral as it is conditioned by another important alternative, which is often underestimated within accounts of the courts' engagement with

[28]App. 33,014/05, *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, ECLI:CE:ECHR:2011:0505JUD003301405.
[29]App. 2872/02, *K.U. v. Finland*, ECLI:CE:ECHR:2008:1202JUD000287202.
[30]App. 64,569/09, *Delfi AS v. Estonia*, ECLI:CE:ECHR:2015:0616JUD006456909.
[31]Case 362/14, *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650.
[32]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
[33]Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.
[34]Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.
[35]Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021 COM(2021) 206 final.

technology: the possibility that the courts may adopt—mirroring the juxtaposition between Hart's external and internal points of view[36]—an internal point of view to the new technology (according to the US model of digital trust) or by contrast an external point of view (according to the European model involving a form of digital distrust).

4 | THE (PRIVATE) ACTORS

Moving now to the investigation of the third constitutive element of the quadrangular shape related to the geometry of digital power, against this background it should be added, first of all, that this is obviously not the first time that the problem concerning the relationship between public law and private powers has arisen,[37] nor that private powers end up *de facto* regulating certain markets—consider, for instance, sporting federations—exerting so much influence over a particular economic sector as to hold, *de facto*, a power that is substantially political *latu senso*.

However, there are two reasons for this discontinuity and hence the significance of private power within the new digital world and, consequently, in the light of my main argument related to digital constitutionalism responses to the new threat represented by such powers, to analyse in depth the nature of such private economic actors. The first reason is quantitative: the pervasiveness of the process of digitalisation, mechanisms for algorithmic automation and the enormous volumes of data available in order to conduct processing and also to pre-empt users' preferences have endowed the major multinationals operating within the digital sector with unprecedented influence and a global reach. The second novelty is qualitative, so to speak. It concerns the breadth, pluralism and freedom of public debate. In fact, we have never witnessed in the past what is currently happening within the digital domain. Specifically, private operators exert such significant dominance over this special type of market, namely the free marketplace of ideas—to paraphrase the legendary metaphor used by Holmes[38]—that they are capable of so effectively conditioning public debate. As a matter of fact, it has recently been argued that 'fostering a large community—similar to a public sphere—is key to the business model' of the major platforms.[39]

From this perspective, for instance, and with particular reference to a specific jurisdiction, the parallel that has been drawn within the case-law of the Supreme Court of the United States between the space controlled by private online operators and the classical public forum, as the cradle of public discourse within the analogical domain, is extremely delicate and in many ways controversial, especially if a prescriptive and not only descriptive force must be attributed to that metaphorical language.[40]

It should be added that the recent pandemic has dramatically brought to the fore the essential role performed by digital services (and hence also of the suppliers of those services) in enabling a number of activities to continue even during severe restrictions on freedom of movement, so much so as to reinvigorate a previously dormant debate concerning the possible constitutionalisation of a "right of digital access" or a right to access the Internet. In these cases, the major providers of digital services have even been referred to as new 'digital utilities',[41] with all the related implications in terms of significant regulation.[42]

[36]Herbert L.A Hart, *The Concept of Law* (Oxford University Press, 1961).

[37]See G. Lombardi, *Potere privato e diritti fondamentali* (Giappichelli, 1970); C.M. Bianca, *Le autorità private* (Jovene, 1977).

[38]*Abrams v. United States*, 250 U.S. 616 (1919). See, most notably, Justice Holmes' dissenting opinion, 624 ff.

[39]M. Poiares Maduro and F. de Abreu Duarte, 'Regulating Big Tech Will Take Pluralism and Institutions' (*Euronews*, 7 October 2021), available at https://www.euronews.com/2021/10/07/regulating-big-tech-will-take-pluralism-and-institutions-view (accessed 2 May 2023).

[40]Milan Kundera had already understood the sensitiveness of metaphorical language when, describing the main character of his most famous book, he highlighted Tomàs' unawareness of the dangers entailed by metaphors and stated that it is best not to play with metaphors. M. Kundera, *The Unbearable Lightness of Being* (Faber, 1984).

[41]L. D'Urbino, 'Big Tech's Covid-19 Opportunity' (*The Economist*, 3 April 2020), available at https://www.economist.com/leaders/2020/04/04/big-techs-covid-19-opportunity (accessed 2 May 2023).

[42]See the following extract from Justice Thomas' concurring opinion in *Biden v. Knight First Amendment Institute at Columbia University* 593 U.S. ____ (2021): 'The similarities between some digital platforms and common carriers or places of public accommodation may give legislators strong arguments for similarly regulating digital platforms. "[I]t stands to reason that if Congress may demand that telephone companies operate as common carriers, it can ask the same of" digital platforms. *Turner*, 512 U.S. 180 (1997) at 684 (opinion of O'Connor, J.)'.

The aspects pointed out above are undoubtedly emblematic of the radical transformation triggered by the new digital world over the last two decades both on society as well as on the private "gatekeepers" of cyberspace, which have *de facto* "transformed" from economic operators into authorities in a technical sense, often exercising para-constitutional functions. In light of these preliminary reflections, it is proposed that we conceptualise digital power in terms of a quadrangular geometry, also with reference to the shift from a vertical dimension to a horizontal dimension.

Against this background, the structure of cyberspace and the physiognomy of the problematic issues that have been sketched out above represent the result of a series of legislative choices that lawmakers embraced, above all in the United States and the European Union, around the turn of the millennium. As mentioned in relation to the spatial dimension, a debate was launched concerning regulation of the Internet: with the emergence of the new technology questions arose concerning the ongoing validity in the Internet age of legal rules created by sovereign states. As the illusion of a web that was free from potential state interference proved to be short-lived, a need arose for regulation that was consistent with the special nature of the digital ecosystem, which was satisfied both in Europe and in the United States by a minimalist approach aimed at promoting the wide circulation of content. It should be recalled that the context within which lawmakers took their first steps was radically different from the context of today, which explains why reform projects such as the DSA and the DMA are regarded as epic reforms, almost revolutionary in tone. The dominant concern within the minds of not only US but also European lawmakers was to establish rules that could guide the actions of service providers (which had not yet emerged as full-blown gatekeepers, or at least as platforms) in order not to impede the circulation of content online.

The structure underpinning these legislative acts reflects above all the openness to freedom of expression that is inherent to US constitutionalism. As was also confirmed by the US Supreme Court's interpretation of freedom of expression in *Reno v. ACLU*, during those years the Internet was regarded as a forum for exchanging ideas and giving effect to the free marketplace of ideas prophesied by Justice Holmes (although that had perhaps never previously been realised). Against a backdrop of mistrust in regulation, and in particular a marked hostility to any form of content regulation that distinguished between content that was legitimately available online and content that could be accessed in the real world (moreover, the Supreme Court itself had held that there was no evidence of any increased benefit resulting from regulation, compared to an absence of regulation[43]), US lawmakers chose a paradigm, set out in Section 230 of the Communications Decency Act, which is still an object of debate. This Act, which is still in force, gives effect to that libertarian fervour embodied in the First Amendment, which was celebrated at the dawn of the Internet.[44] The legislation exempts service providers from any responsibility for any moderation of defamatory content: irrespective of whether the service provider has chosen to remove content or to leave it online, that choice cannot result in any liability for it, save under exceptional circumstances. The reason for this choice, which massively favoured service providers, was to avoid any room for doubt regarding the legal classification of service providers. This hence solved the dilemma that had arisen within US case-law over whether to classify them as "distributors" or "publishers". It has been noted that the choice made, which, moreover, resulted in an enhancement of the protection provided for under the First Amendment,[45] resulted from the need to avoid virtuous forms of content moderation and policing by websites based on appropriate implementation mechanisms: this would have entailed a regime of editorial responsibility, which would have been excessively penalising for operators that were not formally involved in content control, especially on an *ex ante* basis. As has been stressed by the literature, Section 230 CDA—which was nonetheless subject to some (unrealistic and ultimately unsuccessful) attempts at reform during the Trump presi-

[43]See *Reno v. ACLU*, above, n. 14: 'The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship'.
[44]J. Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell University Press, 2017).
[45]See, more recently, E. Goldman, 'Why Section 230 Is Better Than the First Amendment', (2019) 95 *Notre Dame Law Review Reflection*, 33.

dency[46] and was at the centre of the recent US Supreme Court's decision[47] in the *Gonzalez v. Google* case, concerning the existence of a liability of the search engine for the promotion of ISIS-sponsored content which led to the terrorist attacks and killings in Paris of November 2015[48]—resulted from a bipartisan initiative aimed at avoiding the paradox, as is clearly apparent in the *Stratton Oakmont v. Prodigy* judgment[49] of the Supreme Court of New York, that the efforts made by a platform to carry out content policing in good faith could subject the operator of such a site to a more severe liability standard, such as that applicable to publishers and content providers.[50] The need to maintain separate liability standards flowed from the need to favour as far as possible the spread of new "virtual *agorà*" that could host and retransmit third party content, including content created by individual users themselves. Within this perspective, considering platforms as equivalent to content creators would have severely penalised the aim of favouring the exercise of freedom of speech in cyberspace. It was considered that this aim could be most readily achieved by providing that service providers should not incur any liability. Besides, the imposition of "direct" liability for content published by third parties would have significantly undermined the business models of content-sharing platforms.

That freedom of action was also needed for a contingent reason: there was a conviction that minimalist legislation inspired by a digital liberalist vocation[51] would leave greater freedom to the new actors that were starting to operate online to promote the new technology by spreading content on the Internet without any fear of subsequent sanctions, thereby engaging a process of collateral censorship.[52]

This idea of digital liberalism readily migrated from one side of the Atlantic to the other. Indeed, albeit several years later, Europe also adopted a regulatory framework inspired by concerns not to inconvenience the business models of "information society service providers": in other words, to favour e-commerce as much as possible.[53] The (few) provisions dedicated to the liability regime were set out within Directive 2000/31/EC, known as the "E-Commerce Directive",[54] which laid down two fundamental rules: first of all, the lack of any general requirement of preventive supervision for service providers (in keeping with the absence of any editorial liability and with the aim of maintaining as much as possible the free flow of online content without any "conditioning"); second, the provision of a "notice and take down" mechanism, which was imported from the special rules (providing for an exception to Section 230) contained in the US Digital Millennium Copyright Act (DMCA).[55] This framework is based on the absence of any direct liability on the part of the service provider for any unlawful content; it provides, by contrast, that the service provider incurs liability where it fails to ensure the removal of any manifestly unlawful content, despite effectively being aware of it.

[46]See J. Mathews, 'Trump vs. Twitter' (*Verfassungsblog*, 30 May 2020), available at https://verfassungsblog.de/trump-vs-twitter/ (accessed 2 May 2023); G. De Gregorio and R. Radu, 'Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech' (*MediaLaws*, 6 June 2020), available at https://www.medialaws.eu/trumps-executive-order-another-tile-in-the-mosaic-of-governing-online-speech/ (accessed 14 July 2023).

[47]*Gonzalez v. Google LLC*, 598 U.S. __ (2023). The Hearing of the parties arguments before the Supreme Courts, held last February, have been quite instructive. More precisely it is worth mentioning the opinion of justice Elena Kagan. On the one hand, she admitted: 'We're a court, we really don't know about these things,' adding, 'These are not like the nine greatest experts on the internet.' Kagan's suggestion seems to be that reviewing section 230 is a job for Congress and not for the Court. On the other hand, Kagan also pointed out probably the most evident weakness of the legislation at stake: 'this was a pre-algorithm statute in a post algorithm world'. A. Liptak, 'Supreme Court Seems Wary of Limiting Protections for Social Media Platforms' (*New York Times*, 21 February 2023), available at https://www.nytimes.com/2023/02/21/us/google-supreme-court-youtube.html (accessed 14 July 2023).

[48]I. Millihiser, 'A new Supreme Court case could fundamentally change the internet' (*Vox*, 6 October 2022), available at https://www.vox.com/policy-and-politics/2022/10/6/23389028/supreme-court-section-230-google-gonzalez-youtube-twitter-facebook-harry-styles (accessed 2 May 2023); D. Coldewey, 'The Supreme Court takes on Section 230' (*Tech Crunch*, 3 October 2022), available at https://techcrunch.com/2022/10/03/the-supreme-court-takes-on-section-230/ (accessed 2 May 2023). Similarly, the US Supreme Court is expected to deliver a decision concerning the liability of intermediaries for the promotion of terroristic content in the case of *Twitter, Inc. v. Taamneh*. See 'Twitter, Inc. v. Taamneh (SCOTUSblog, October 2022), available at https://www.scotusblog.com/case-files/cases/twitter-inc-v-taamneh/ (accessed 2 May 2023).

[49]*Stratton Oakmont v. Prodigy*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

[50]Just a few years earlier, the US District Court for the Southern District of New York, in *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) had seemingly seconded the assimilation of online platforms to distributors, suggesting a similarity with news-stands, libraries and book-shops as far as control over content is concerned.

[51]De Gregorio, *Digital Constitutionalism in Europe*, above, n. 1.

[52]J.M. Balkin, 'Free Speech and Hostile Environments', (1999) 99 Columbia Law Review, 2295.

[53]De Gregorio, *Digital Constitutionalism in Europe*, above, n. 1.

[54]See L. Edwards (ed.), *The New Legal Framework for e-Commerce in Europe* (Bloomsbury, 2005).

[55]Digital Millennium Copyright Act 1998 (DMCA).

It is clearly apparent that the legal framework in Europe and the United States was adopted within a specific context, where there were good prospects of cyberspace becoming a location for realising the metaphor of the free marketplace of ideas. Within this scenario of major competition between virtual communities, it was inevitable that the concern of lawmakers would be to keep regulatory pressure to a minimum, trusting in the inherent capacity of cyberspace to "self-regulate", offering alternative spaces that were capable of establishing and legitimising themselves.

Within this context, it has been competition law that has reigned supreme in the United States, although also in Europe, as the only instrument allowing for *ex post* intervention in relation to the concentrations of economic power that gradually and inevitably emerge. The relevant context is specifically the market and the relevant freedom is freedom of enterprise. A profound paradigm shift occurred within the space of a few years. The new players that had emerged in the digital era transformed from economic operators into private powers, following which antitrust law proved to be inadequate, resulting in the need for intervention using the instruments typical of constitutional law.

This is also because, in the meantime, the Internet was also undergoing a major transformation, which had significant repercussions on the physiognomy and role of platforms. The rules introduced in the United States in 1996 and in Europe in 2000 appeared to be increasingly obsolete. They were ill-suited to the characteristics specific to the new platforms that were establishing themselves and, during the initial stages of those platforms (as we shall see when considering the reactions of digital sovereignty to the consolidation of private power), required a major dose of creativity, if not even manipulation, within the case-law of the ECJ.

It is now necessary to consider the reasons underlying the paradigm shift mentioned above. More specifically, a question arises as to why, at a particular moment in time, operators doing business in cyberspace transformed into full-blown private powers in competition with public authorities, thereby inevitably increasing the relevance of constitutional law arguments.

In order to provide an adequate response, we must look back a few decades and consider who, at the end of the last century,[56] was the first to point out the initial transformation, which ultimately ended up representing a significant step.

This was Lawrence Lessig, who argued that, within a context such as that of cyberspace, individual content could only be suitably regulated if the inherent specificity of this technology was taken into account, namely its architecture, or better its code. Lessig's comment "code is law" points to the capacity of different matrices (including legal norms) to impinge upon the regulation of individual conduct, contributing both directly and indirectly to the establishment of rules of conduct. This insight of Lessig encapsulated some of the key aspects of the debate into cyberspace regulation. The most important one for our present purposes is, starting from the centrality of the role of technology for effective regulation, the fact that a shift was underway within fundamental decision-making over that regulation from the lawmaker to the IT technician, in other words to the expert capable of deciphering the code. As has been pointed out,[57] it is no coincidence that the first provisions laid down by lawmakers in this area concerned the role of intermediaries, in awareness of the central importance of their technical role (which at the time still did not have any oligopolistic features and was thus unaffected by competition law) in relation to operations impinging on user activity and behaviour.

Today we are witnessing a kind of "code reloaded", in light of the metamorphosis referred to above, whereby digital intermediaries have transformed from economic operators into full-blown private powers, in competition with public authorities. Indeed, these operators are distant relatives of the operators that were (not) regulated under European law during the era of digital liberalism. They are much less neutral, much less passive and yet much more sophisticated and much more capable (whilst not, however, taking on the role of traditional publishers) of altering the content hosted within their virtual spaces.

[56]L. Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

[57]M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali* (Aracne, 2019).

On the other hand, whilst Lessig had well understood and described an initial shift from the political decision-maker to the IT expert, some years later, from the start of the 2010s, algorithmic power and the resulting machine-learning capability shifted decision-making from humans—whether politicians or IT experts—to machines. These algorithms formed part of the automation architecture of the new ecosystem rooted in AI which, along with the exponential growth of the data available, completed the new intermediaries' transformation from economic operators into political forces. It should be added that in many cases the algorithm is opaque and non-transparent, thereby further enhancing the power of platforms. As the following sections will argue when considering the reactions by public authorities to the consolidation of algorithmic power, the most recent round of digital constitutionalisation in Europe appears to have identified appropriate countermeasures in relation to this aspect (lack of transparency).

5 | REMEDIES. HOW TO LIMIT ABUSES OF POWER IN THE ALGORITHMIC SOCIETY: TOWARDS A DIGITAL CONSTITUTIONALISM?

Having illustrated the pitfalls within the gradual yet inexorable process by which economic operators within cyberspace metamorphose into private powers, as well as the spatial and value characteristics that acted as a backdrop to that metamorphosis, it is now necessary to ask, according to the initial framing of this study, and looking in particular to the fourth element of our quadrangular shape, how digital sovereignty is expressed by the concerned legal orders. More generally, we must consider what appropriate instruments are available to modern constitutionalism in order to counter or limit the expansion of private digital power.

The current question is still the same as the one that Goldsmith and Wu posed in 2006—namely, "Who controls the Internet?"[58]—to which another equally relevant question should now be added: How can liberal democracies exercise their own "digital" sovereignty over private powers that are competing on an increasingly equal footing with public authorities?

The major differences between the respective value frameworks that characterise US and European law (although here one could obviously mention other competing models such as the Chinese model) also explain the issues at stake within the debate on digital sovereignty under which different legal systems, which may make specific claims in relation to the governance of cyberspace, apply different "visions" of the same rights and different standards of protection.

Remaining true to the trans-Atlantic focus sketched out at the start, these reactions must be illustrated—also in the light of the extremely different value framework, which this study has sought to present—by focusing first on the US system and then on the EU. First however, it is necessary to make a preliminary note concerning one aspect that unites the two sides of the Atlantic.

5.1 | The US perspective: The primacy of the state action doctrine

If we start by considering the US context, American constitutional law does not provide for the horizontal application of the rights contained in the Bill of Rights, in contrast to the position in Europe. Or rather, as far as the application of the rights contained in the constitutional amendments introduced from 1791 onwards are concerned, including in particular the First Amendment, their horizontal effect (*inter privatos*) is precluded by the "state action doctrine".[59] According to this doctrine, the guarantees provided by the rights enshrined in the federal Bill of Rights can only be invoked against public authorities and not against private individuals.

[58]See T. Wu and J.L. Goldsmith, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006); see also Goldsmith, above, n. 8.
[59]See, most notably, S. Gardbaum, 'The "Horizontal Effect" of Constitutional Rights', (2003) 102 *Michigan Law Review*, 388; M. Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law', (2003) 1 *International Journal of Constitutional Law*, 79; W.R. Huhn, 'The State Action Doctrine and The Principle of Democratic Choice', (2006) 84 *Hofstra Law Review*, 1380.

The reason underlying the resistance towards acceptance of a general horizontal effect for the rights contained in the federal Constitution can be found in the fertile ground in which US constitutionalism took root, based on the values of liberty and individual freedom, which constitute the bedrock for private autonomy.

In other words, as Mark Tushnet has observed, 'the judicialisation of relations between private persons [is] an intolerable intrusion of the state into the sphere of private autonomy'. This leads naturally into the question, with specific reference to our field of enquiry, as to whether such an intrusion could be considered to be intolerable even in cases involving private powers that often *de facto* exercise public or para-constitutional functions, which can hence be considered to be state actors *latu senso*? The Supreme Court's answer has been sufficiently clear and confirms that such an intrusion would be intolerable. In the only substantial decision to be considered newsworthy,[60] the Court held that a private person could not be regarded as a state actor, despite the massive size of the platform YouTube.

Moreover, as has rightly been pointed out, 'according to the interpretation embraced by the Court of Appeal, there is absolutely no potential similarity between a service provider such as YouTube and the notion of state actor within US constitutional law: there is no involvement in that specific range of functions that have been traditionally reserved on an exclusive basis to the state';[61] on the contrary, they are nothing other than private operators that make decisions relating to the governance of their own respective spaces.

Given the insuperable nature of the obstacles presented by the state action doctrine, the reference to governance of the space managed by the platforms represented a second attempt by US constitutional law—here too, substantially without any success—to more effectively (de)limit the emerging digital power. This involved, in particular, the interpretative option that sought to establish equivalence between the spaces offered by digital platforms providing social network services, on the one hand, and a public forum, on the other. The aim of this was to apply the "public forum doctrine", which allows extremely limited scope—largely content-neutral—for interference with the exercise of free speech rights in locations, such as parks, roads and squares, that are considered to be naturally designed to host exchanges of ideas and opinions between different people.

It has been pointed out in the literature[62] that this assertion is often made metaphorically with the aim of describing social networks as the new public forum; however, to vest it with a normative effect would be something entirely different. The US case-law has endorsed this account to date solely in relation to social network accounts used by state officials, i.e. persons acting in a public capacity, holding that measures such as the blocking or removal of comments effectively violate freedom of expression.[63] It is important to note that the case-law does not consider private ownership to preclude classification as a public place, noting that there may indeed be "designated public forums"; these are spaces that, whilst being private, "become" essentially public in nature, being subjected to the same process of metamorphosis that we have seen to apply in relation to private cyberspace operators.

The attempts referred to above to reclassify the role of platforms, and in particular social networks, have a variety of implications with regard to the values at stake within digital space, with which the new "powers" must inevitably engage. To state that a social network is equivalent to a public service or a state is not a neutral act as it entails subjection to a range of guarantees that are normally associated with the actions of public operators. Although on paper such a development might mark progress in the sense of providing greater guarantees, on the other hand it may entail some pitfalls. In particular, to subject private operators to the same standard of protection as that imposed on public bodies could have difficult consequences in terms of some of the strategies that have been developed at the European level. This is relevant above all in relation to content that is not unlawful but may need to be removed or to be subject to technical action according to strategies to combat certain content developed within the ambit of self-regulation or co-regulation. Disinformation is a particularly striking example of this. This is a warning which, as

[60] *Prager University v. Google LLC*, n. 18–15,712 (9th Cir. 2020).
[61] Bassini, above, n. 57, 22.
[62] Ibid., 68.
[63] *Knight First Amendment Inst. at Columbia Univ. v. Trump*, n. 1:17-cv-5205 (SDNY); *Knight First Amendment Inst. at Columbia Univ. v. Trump*, n. 18–1691 (2d Cir.); *Biden v. Knight First Amendment Institute at Columbia University* 593 U.S. (2021); *Davison v. Randall*, n. 17–2002 (4th Cir.).

has been acknowledged in the literature,[64] was previously given by Justice Alito in his concurring opinion in *Packingham v. North Carolina*,[65] in which he criticised the excessively relaxed way in which the Supreme Court's opinion had suggested that the Internet—and social networks in particular—constituted new "public forums" within the digital reality, without considering the normative implications of this dictum. This is not all: any requirement that content moderation by social networks must comply with the "public" standard would risk entirely frustrating the promise of freedom inherent within these platforms, jeopardising their possible use as instruments of protest or for combatting propaganda or public censorship. This would result in social networks being steered by state authorities. Although the authorities may in some cases operate for virtuous purposes, in some cases they may be inspired by less commendable goals, especially within immature democracies or during armed conflict, as we are already sadly aware of.

In any case, the attempt (or the interpretative mistake) that appears to be apparent within *Packingham* of attributing normative and prescriptive value to the spatial metaphor[66] of cyberspace as a public forum was definitively blocked (or clarified) in a relatively recent judgment of the District Court for the Northern District of California,[67] in which it was clearly held that, '[a]lthough *Packingham* spoke of "cyberspace" and "social media in particular" as "the most important places … for the exchange of views" in modern society, […] *Packingham* did not, and had no occasion to, address whether private social media corporations like YouTube are state actors that must regulate the content of their websites according to the strictures of the First Amendment'.

Metaphorically speaking, as has been rightly stressed, 'this represented a *coup de grâce* for any claim to establish equivalence that might have been based on that nonetheless important judgment, the significance of which must not therefore be misconstrued'.[68] Once again, metaphors have to be taken seriously.

5.2 | The European perspective: From the ECJ's judicial activism to the first phase of digital constitutionalism

We turn now to the ways in which sovereignty has been expressed in Europe in response to, and in order to "contain", the new digital power, with emphasis placed on how these actions contrast with the approach in the United States. It is posited that actions taken in Europe, in contrast to what has occurred in the United States, are feasible on the grounds of being consistent with the constitutional traditions common to the Member States. The option involves the possibility of recognising European charters of rights as having horizontal effect against private operators, thereby applying the German doctrine of *Drittwirkung* established in the famous *Lüth* judgment.[69]

For its part, the ECJ has demonstrated the potential for horizontal application of provisions of the Treaties, even when they were directed exclusively at the Member States. A particularly clear example of this is its decision in *Defrenne II*,[70] which held that a Treaty provision was capable of horizontal direct effect—namely, the Article 157 TFEU (then Article 119 of the EC Treaty) on equal pay for men and women—even though it was addressed exclusively to the Member States and required national legislators to adopt provisions at national level that are most appropriate to ensure the efficacy, and hence justiciability, of the right to equal pay for men and women for equal (or equivalent) work.

[64]See, also, Bassini, above, n. 57, 78. On the possible consequences of such re-qualifications, see especially the work of D.C. Nunziato, 'From Town Square to Twittersphere: The Public Forum Doctrine Goes Digital', (2019) 25 *Boston University Journal of Science & Technology Law*, 1.
[65]*Packingham v. North Carolina*, in 582 U.S. ___ (2017).
[66]A. Morelli and O. Pollicino, 'Metaphors, Judicial Frames, and Fundamental Rights in Cyberspace', (2021) 68 *American Journal of Comparative Law*, 616.
[67]*Prager University v. Google LLC*, n. 18–15,712 (9th Cir. 2020).
[68]Thus Bassini, above, n. 57, 88
[69]BVerfGE, 7, 198, Jan 15, 1958.
[70]Case 43/75, *Gabrielle Defrenne v. Société anonyme belge de navigation aérienne Sabena*, ECLI:EU:C:1976:56. The decision has been the subject of much debate within academia. Amongst the first relevant comments, see O. Stocker, 'Le second arrêt Defrenne. L'égalité de rétribution des travailleurs masculins et des travailleurs féminins', (1977) *Cahiers de droit Européen*, 180.

A number of cases have subsequently resulted in the horizontal application of general principles of EU law[71] and, albeit in a line of case-law that is not always entirely transparent, also of some provisions of the Charter of Fundamental Rights.[72]

However, within this context there is a singular aspect of the ECJ's reaction to the emergence of digital power, which during those years was not, moreover, being resisted by a neo-liberal legislature, which took the view that digital operators should not be regulated, or simply remained inactive, as is apparent from the extremely long gestational period necessary in order to adopt the General Data Protection Regulation (GDPR) in 2016. This aspect was the surreptitious, and by all means not expressed, horizontal application of Articles 7 and 8 of the Charter of Fundamental Rights (concerning, respectively, the respect for private life and data protection) within the case-law adopted in 2014 and 2015 (*Google Spain* and *Schrems* in particular) concerning the enforcement of digital privacy rights against the emerging power of algorithms.

This period of judicial activism by the ECJ, which can in some sense be accounted for both with reference to the threat of global surveillance originating from the United States and the inertia of European lawmakers,[73] having repeatedly kicked the long-awaited GDPR into the long grass, evidently amounted to a clear rejection by the ECJ of the previous approach characterised by digital liberalism. This approach prevailed on both sides of the Atlantic and favoured the transformation of private entities from economic operators into full-blown powers.

Although the period of creative reaction from the ECJ is certainly understandable and even consistent (at least as regards the specific level of protection afforded to data protection) with the values embraced by the constitutional traditions common to the Member States, there were nonetheless some downsides which forced a rethink of the way in which European digital sovereignty was expressed in the face of the digital "threat". This led to a new approach that saw a reaction by European constitutional law to the consolidation of private power.

The first evident downside was the amplification of an imbalance, in terms of the separation of powers, between the judicial branch and the political/legislative branch.

This point is quite significant and needs to be considered in more detail. The phenomenon of "judicial globalisation" was already being debated at the end of the last century[74] in terms of the growing, and ultimately preponderant role, of courts within (power) dynamics with the legislature and the executive. However, as noted elsewhere,[75] this role has been even more significant within the new digital world. There are at least two reasons for this. The first is due to the failure to act by lawmakers, which has become chronic in a field (i.e., the regulation of cyberspace) that is at an extremely high risk of obsolescence. This has given rise to a vicious circle in which the legislature and the executive prefer to remain inactive, rather than constantly falling behind technological developments, thus leaving it to the courts to make choices, which are in some cases tragic,[76] on balancing operations concerning a technology that, far from being neutral, is subject to a strong axiological-substantive matrix.

The second reason (as stressed in Section 2 when commenting on the first rulings issued by US courts in response to the anarchical perspective that saw cyberspace as being immune to influence by public authorities) is related to the exercise of rooting jurisdiction, which is typical of Internet law, and which further amplifies the role of courts within the digital ecosystem.

[71]See, among others, Case 26/62, *Van Gend en Loos v. Administratie der Belastingen*, ECLI:EU:C:1963:1; Case 2/74, *Reyners v. Belgian State*, ECLI:EU:C:1974:68; Case 33/74, *Van Binsbergen v. Bestuur van de Bedrijfsvereniging voor de Metaalnijverheid*, ECLI:EU:C:1974:131; Case 41/74, *Van Duyn v. Home Office*, ECLI:EU:C:1974:133.

[72]Case 414/16, *Egenberger*, ECLI:EU:C:2018:257; Case 569/16, *Bauer*, ECLI:EU:C:2018:871; Case 684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften*, ECLI:EU:C:2018:874; Case 68/17, *IR v. JQ*, ECLI:EU:C:2018:696; Case 193/17, *Cresco Investigation*, ECLI:EU:C:2019:43; Case 55/18, *CCOO*, ECLI:EU:C:2019:402. See E. Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle', (2020) 22 *Cambridge Year Book of European Legal Studies*, 208; V. Piccone and O. Pollicino (eds), *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività* (Editoriale Scientifica, 2018).

[73]De Gregorio, *Digital Constitutionalism in Europe*, above, n. 1.

[74]A.M. Slaughter, 'Judicial Globalization', (2000) 40 *Virginia Journal of International Law*, 1103.

[75]Pollicino, above, n. 1.

[76]G. Calabresi and P.C. Bobbitt, *Tragic Choices* (W.W. Norton & Co., 1978).

In light of these considerations, it is clear within the European context that it was necessary, if not to rebalance, then at least to mitigate the imbalance referred to above in terms of the separation of powers, ensuring that decision-making mechanisms involved also and in particular the democratic-representative input from the legislative process.

This imbalance is not the only drawback to the expression of digital sovereignty through case-law. It is also compounded by a process of fragmentation, also at the national level, of the rules developed through case-law for specific individual scenarios, thereby significantly undermining the principle of legal certainty. More specifically, given the lack of legislative action, having failed to regulate, amongst other things, the liability exemptions (or rather limitations) provided for under Directive 2000/31, both European and national courts have established new roles and definitions for Internet service providers. These have been both active and passive roles,[77] although also "sophisticated" roles,[78] thereby resulting in the creation of a variety of new figures (despite the legislation remaining unchanged) corresponding to the different levels of responsibility for the private gatekeepers of the digital ecosystem, which have not only become much larger but have also changed fundamentally in terms of their essence. All of this has obviously played out against a backdrop characterised by a significant level of fragmentation within the case-law, and consequently the weakening of the principle of legitimate expectations.

A third downside to this period of judicial activism has been the—certainly unintended but extremely risky—consequences of the decisions discussed, including in particular *Google Spain*. In fact, one of the effects of the creation within the case-law of the right to be forgotten has been for the ECJ to vest a search engine (i.e., a private operator/power) with the task of striking the delicate balance between a user's right to be forgotten and the right to be informed of the majority of Internet users. Where an operation that should fall within the exclusive purview of a judicial or para-judicial authority is delegated to a private operator vested with almost complete discretion and without adequate procedural guarantees, this inevitably ends up enhancing that operator's power.

These issues have resulted in the emergence of a new approach, which has been defined as "digital constitutionalism",[79] in which political actors have reasserted control over the expression of digital sovereignty with a view to containing the new private powers. Leaving aside specific labels and the potential conceptual confusion that has been associated with them (not always rightly) due to the alleged (although in fact unfounded) resemblance between theories of global constitutionalism[80] and the different manifestations of digital constitutionalism, one thing is certain. This new approach has been characterised by the re-appropriation of European legislators' role as lawmakers. This time, in contrast to the initial phase during the early 2000s, which was characterised by digital liberalism and in which antitrust law reigned supreme, they have been fully mindful of the need to inject a constitutionally informed viewpoint that is capable of limiting the influence of, and preventing abuses by, any powers that have transformed from private economic operators to powers in a strict sense. It is clear that, from this point of view, any *ex post* intervention such as that provided for under competition law, cannot be sufficient. It is by contrast necessary to use the toolkit of constitutional law, which must be reconfigured (but not entirely disrupted) in the face of the new technological environment.

The first somewhat concentrated dose of this "injection" came with the entry into force of the GDPR in 2016, which, moreover, codified many of the rules that had previously been developed within the case law of the ECJ. It elevated the right to data protection from an economically informed interest under Directive No 95/46 into a right to privacy inherent to the constitutional framework, which had in the meantime been codified in the Charter of Fundamental Rights, in both its static (Article 7) and dynamic (Article 8) manifestations.[81]

[77]See, among others, Joined Cases 236/08, C-237/08 and 238/08, *L'Oréal and others*, ECLI:EU:C:2010:159; Case 18/18, *Glawischnig-Piesczek*, ECLI:EU:C:2019:821. With respect to Italian case-law, see, most notably, Cass. Pen. 19 marzo 2019, n. 7708.

[78]See Tribunale di Roma, sez. IX, 27 aprile 2016, n. 8437.

[79]De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, above, n. 1; De Gregorio, *Digital Constitutionalism in Europe*, above, n. 1; Pollicino, above, n. 1; O. Pollicino, 'Data Protection and Freedom of Expression Beyond EU Borders: EU Judicial Perspectives', in F. Fabbrini, E. Celeste and J. Quinn (eds.), *Data Protection Beyond Borders* (Bloomsbury, 2021).

[80]M. Betzu, 'I poteri privati nella società digitale: oligopoli e antitrust', (2021) 3 *Diritto Pubblico*, 745.

[81]See G. Martinico, 'Art. 7. Rispetto della vita privata e della vita familiare', in R. Mastroianni et al. (eds.), *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè, 2017); O. Pollicino and M. Bassini, 'Art. 8. Protezione dei dati di carattere personale', in Mastroianni et al. (eds.), *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè, 2017).

As has been argued elsewhere,[82] the GDPR has acted as a model for various jurisdictions, giving rise to a form of legal "colonisation", or, as it has also been defined, a "Brussels effect"[83] that is almost global in reach, extending from California[84] to China.[85]

Despite the attempted transplanting and the apparent success of these operations,[86] it is clear that the GDPR has a strong axiological-substantive vocation, embracing a framework of values inherent to the constitutional traditions common to the Member States, starting from the privacy-dignity couplet as the undisputed lodestone. In this sense, leaving aside the relative perspective involving the migration of the European constitutional mindset to other countries, the GDPR has in fact helped to make fortress Europe even more impregnable in defence of the value paradigm referred to above, which has been jeopardised by the amplification of private digital power.

This enhancement of fortress Europe has been a common feature of the various legislative changes introduced in recent years: from the reform of copyright law[87] through the changes to the law governing the provision of audiovisual media services[88] to European legislation on the prevention of terrorism.[89] This could be regarded as the initial phase of digital constitutionalism, which has *de facto* emerged as a response by European political representatives to the considerably high judicial power of the previous era, the processes and pitfalls of which have been described above.

A defining feature of this first phase has been a strong axiological-substantive configuration, which in turn, however, suffers from two underlying drawbacks, despite being fundamentally consistent with European constitutional roots. Due to the variety of sectoral legislation, the first drawback concerns the risk (as seen during the phase of judicial activism) of triggering a process of internal fragmentation. This would result in the application of different rules, also in relation to the different liability models for the major digital platforms, depending upon the specific relevant legislation, subject, moreover, to a not insignificant margin for the Member States, considering the extremely large number of open clauses contained in the relevant regulations, which are often tantamount to masked directives.[90]

It is clear that, although this obviously buttresses fortress Europe against possible external attacks, it also risks causing an implosion, or in any case an internal weakening, due to the excessive sectoral specialisation within the relevant provisions. This has evident repercussions, once again, on the principle of legal certainty.

The second drawback results from the risk that, in focusing exclusively on a regional value framework—the characteristic features of which are extremely specific—in order to regulate the digital ecosystem, which is by definition transnational, fortress Europe may end up becoming seriously isolated due to a lack of bridges connecting it with other significant regional hubs.

This clearly raises the possible risk that European rules may not be enforced, and more generally that Europe and the United States may drift further apart, thereby undermining the solidity of the trans-Atlantic bridge. However, maintaining that bridge is crucially important in order to ensure the effective containment by modern constitutionalism of the now consolidated private digital power.

[82] O. Pollicino and K. Kowalik-Bańczyk, 'Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information', (2016) 13 *German Law Journal*, 315.

[83] A. Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).

[84] See California Consumer Privacy Act 2018 (CCPA).

[85] See Personal Information Protection Law 2021 (PIPL).

[86] See the Brazilian General Law on Data Protection, Lei Geral de Proteção de Dados (LGPD), of 2018.

[87] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.

[88] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69.

[89] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L172/79.

[90] See, among others, G. De Gregorio, 'Democratising Online Content Moderation: A Constitutional Framework', (2020) 36 *Computer Law & Security Review*, 105,374.

5.3 | The horizontal approach as response to the risk of fragmentation: An analysis of the Digital Services Act and the Digital Markets Act

The drawbacks illustrated in the previous section have resulted in a second phase (which is currently ongoing and is set to continue into the near future) within digital constitutionalism in Europe. This phase is characterised not only by an axiological-substantive approach but also by a procedural dimension as well as its "horizontal" scope, as it is not focused on individual sectors, precisely in order to avoid the fragmentation mentioned above.

More precisely, in light of the above indications, the European Commission has recently intervened to give tangible effect at a normative level to its methodological guidelines. It has done so specifically through the Digital Services Package,[91] which includes two regulations aimed at addressing the two greatest problems associated with the exercise, holding and concentration of digital power by these intermediaries. The DMA and the DSA, proposed by the Commission in December 2020, were finally adopted in 2022 respectively as Regulation (EU) No 2022/1925 and Regulation (EU) No 2022/2065. Thanks to these two normative acts, the European Union is now seeking to redesign the normative framework, and hence the obligations and responsibilities of online digital platforms, in an attempt to counter the consolidation of private digital power, within a perspective that is more procedural than axiological-substantive. The two regulations are complementary and are significant in that they address the greatest problem affecting the digital market,[92] namely the concentration of resources, data and information, which gives rise to concentrations of market power.[93]

On the one hand, the objective of the DMA is to take action to correct market failures, attempting to limit the power of the major digital platforms, which are referred to within the proposed regulation as "gatekeepers"; on the other hand, the EU aims to address the social harm caused by the dissemination of content—whether legal or illegal—on platforms. In particular, the DSA addresses issues such as the responsibility of online intermediaries for content uploaded by third parties, online user safety and asymmetric due diligence obligations for the various providers of information society services, thereby amending the original provisions on e-commerce set out in Directive 2000/31/EC.[94]

The lowest common denominator of both proposals is the focus placed on the quantitative dimension to platforms, including, in particular, "very large online platforms and very large search engines". This choice is naturally dictated by an awareness that, within a digital context, it is often the quantitative dimension that has qualitative implications in terms of the enhanced capacity of platforms, thanks also to the massive volumes of data collected, to put in place surgical profiling mechanisms, although also to predict preferences.[95]

Also, the DSA has "very large online platforms" and "very large online search engines" as its principal objective,[96] i.e. those digital platforms that, taking account of the number of users and the volume of data to which they have access, are considered to be particularly influential and to wield power on the digital market. Adopting a risk-based approach,[97] the regulation will subject providers of (digital) intermediation services to proportionate duties and obligations that are commensurate with the specific risks that may potentially result from the provision of their services.[98]

[91]The Digital Services Act package (*European Commission*, 2020), available at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed 12 June 2023).

[92]See, among others, J. Laux, S. Wachter and B. Mittelstadt, 'Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA', (2021) 43 *Computer Law & Security Review*, 105,613.

[93]M. Colangelo and M. Maggiolino, 'Manipulation of Information as Antitrust Infringement' (2018) 26 *Columbia Journal of European Law*, 63.

[94]See Recitals 4 ff. of the DSA, as well as arts. 4–6 amending rules on the exemption of liability of intermediary as previously regulated within the e-Commerce Directive.

[95]Zuboff, above, n. 6.

[96]Very large online platforms, pursuant to art. 33, paras. 1 and 4, are defined as those platforms providing their services to a monthly average of 45 million recipients within the European Union.

[97]A method which, in fact, is not completely new to the European institutions, as explained in G. De Gregorio and P. Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age', (2022) 59 *Common Market Law Review*, 473, 483–488.

[98]Thus recital 76 of the DSA: 'Very large online platforms and very large online search engines may cause societal risks, different in scope and impact from those caused by smaller platforms. Providers of such very large online platforms and very large online search engines should therefore bear the highest standard of due diligence obligations, proportionate to their societal impact'.

Accordingly, whereas on the one hand the main objective of the DMA is to counter the digital power of platforms on an economic level, the DSA aims to contain that power on another front. This will entail a whole range of transparency obligations with a view to balancing the information asymmetry of users and that of providers.[99]

As has been demonstrated within a considerable body of literature,[100] platforms have radically altered the way in which information is used and also how it is shared by users who in turn contribute to the dissemination of fake news or online hate speech. In this sense, therefore, it is desirable to provide users of these instruments both with information and also with procedures that can rebalance the unilateral asymmetries of the power of platforms. Coupled with the obligations aimed at achieving a greater acknowledgement of the responsibility of platforms and especially of their accountability (the true watchword of the new bodies of rules, which has evidently been borrowed from the GDPR framework), the aim will be to reinforce the position of users, but also in a certain sense the discretion available to major platforms.

It is impossible to predict what the tangible effects of these provisions will be and whether they will be capable of rebalancing the exercise and control of digital power. It is possible to clarify at this stage that the new legislation—the contents of which have been briefly described here—will have the task of redefining the reach of the law as regards platforms' obligations and responsibilities, not only within the internal market but also on a global scale. The aim is to revive the "Brussels effect", mentioned above in relation to the export of the GDPR, although this time based more on a procedural than an axiological-substantive foundation. For these reasons, it ought to be less susceptible to crises of rejection.

6 | CONCLUDING REMARKS: DUE DATA PROCESS AND THE PROCEDURAL DIMENSION (THE SECOND SEASON OF EUROPEAN DIGITAL CONSTITUTIONALISM)

The analysis emerging from the previous section might be synthesised as a new manifestation of digital constitutionalism that seeks to resolve the problems in terms of non-transparency that frequently come to light when it come to the algorithms used by the new powers. In other words, after a first phase of reaction to the emerging digital powers by the European constitutional powers (firstly, the European Court of Justice with its "wild" judicial activism and, secondly, starting with the adoption of the GDPR, the EU lawmaker with its hypertrophic approach) focusing (only) on the substantive values at the heart of European constitutional law, a change of strategy has taken place with the adoption of the DSA and DMA. The focus has been not (only) on the mentioned values, in the light, it should be added, of a sectorial vertical approach, but rather, as has been described by commenting on the new EU legislation's added value, on a horizontal and procedural application thereof, which might be seen as the main features of the second season of European digital constitutionalism.

In particular, the mentioned legislation does so by providing procedural guarantees to remedy the absence of substantive guarantees comparable to those applicable to relations with public bodies. However, it is important to note that, whilst focusing much more on the procedural dimension than the previous exclusively axiological-substantive approach did, this new manifestation of digital constitutionalism must not be confused with a radicalisation of that approach that would risk transforming the state into what Forsthoff would have called 'a macro-administration shorn of political capacity'.[101] Moreover, one must not be so naive as to overlook the possibility that any attempt at proceduralisation that is detached from a reference value foundation is destined to degenerate into a sterile exercise of "procedural fetishism".

In order to tease out the (at least potential) added value that the procedural guarantees mechanisms can attribute to the level of protection for the fundamental rights at stake, it may be helpful to consider an example.

[99]For an in-depth account of the two texts, see M. Eifert, A. Metzger, H. Schweitzer and G. Wagner, 'Taming the Giants: The DMA/DSA Package', (2021) 58 *Common Market Law Review*, 987.
[100]See, among others, Balkin, above, n. 2.
[101]Betzu, above, n. 80, 747.

Consider the right to be forgotten, which is a new right created within case-law, or rather an existing right that has been recycled for the digital world. Its elaboration by the ECJ has certainly added a new right to the array of rights available to users against major platforms. However, it may be the case that it will not raise effectively the level of protection for the rights at stake. This is not only because the inflation in substantive rights (which has now become fashionable, if one considers the number of declarations of rights on the Internet[102]) risks increasing the scope for constitutional collisions, and hence conflicts, but also because—and this is the key point for our present purposes—the ECJ has vested a private operator, a search engine, with the task of striking a balance between the right to be forgotten, on the one hand, and the right to be informed, on the other, without adopting any procedural guidelines to structure the relations between the search engine and the users as regards the specific arrangements for exercising that right. Without being subject to procedural safeguards of any type, it is the private operator that decides what arrangements should apply, which obviously undermines the rights of the individual on both a procedural and a substantive level.

Just as procedural obligations that are not rooted in a specific value framework can give rise to an empty exercise in terminology, similarly the creation of new substantive rights without the appropriate procedural safeguards can risk producing rights that only exist on paper.

The great benefit of stressing the procedural dimension, which may be defined as a European application of *due (data) process*[103] on a horizontal level between private parties, is that it is potentially able to consolidate that trans-Atlantic bridge. This is because it is a dimension (and a principle, i.e., due process applied in the digital realm) that is absolutely not alien to US constitutionalism.[104] Moreover, the particular focus on the valorisation of the principle of transparency points towards another benefit that is often not visible: that of ensuring that the actions of "private powers" are open to control where they implement strategies or measures that have been adopted by public authorities, which may have threatened major financial sanctions in the event of non-compliance.

The final reflections have tried to answer one of the research questions identified in the introduction: what arsenal is available to constitutionalism, considered from a trans-Atlantic perspective, to counter the exponential expansion of private powers? The remainder of the analysis has tried to respond to all of the remaining research questions. What has been proposed, for the first time, is a quadrangular shape in relation to the geometry of digital powers, corresponding to four constitutive dimensions: 1. space; 2. values; 3. actors; and 4. remedies (with the fourth focusing on the responses of constitutionalism to the consolidation of that power). Each constitutive element has been analysed in depth in order to show the specific feature of these new powers and why they are different from the previous ones. The analysis has also focused on the reasons related to the consolidation and changing nature of such powers, targeting in particular the algorithmic factor as the main consequence of such transformation.

As is clear from the investigation carried out, the classic categories of constitutional law—sovereignty, territory, people and power—far from being outdated in the new digital context, are very much contemporary and indeed crucial in order to understand and contextualise the new threats to constitutionalism which must be, at the same time, able to show the needed flexibility to address such threats and remain faithful to its genetical code: limiting power(s).

ORCID

Oreste Pollicino https://orcid.org/0000-0002-8521-3050

How to cite this article: Pollicino O. The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism. *Eur Law J*. 2023;1-21. doi:10.1111/eulj.12472

[102]See Redeker et al., above, n. 1, 302.

[103]K. Crawford and J. Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms', (2014) 55 *Boston College Law Review*, 93; D.K. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions', (2014) 89 *Washington Law Review*, 1.

[104]See, among others, M.H. Redish and L.C. Marshall, 'Adjudicatory Independence and the Values of Procedural Due Process', (1986) 95 *Yale Law Journal*, 455.