

Digital constitutionalism in the new era of Internet governance

Giovanni De Gregorio* and Roxana Radu†

ABSTRACT

Digital technologies are profoundly intertwined with constitutionalism. They are not only a sum of material and immaterial architecture, but also provide infrastructures to exercise freedoms and powers. Even if digital technologies are likely to remain the key driver of global transformations in the next decades, the current evolution of Internet governance promises to affect this relationship. This article argues that Internet governance is evolving towards fragmentation, polarization and hybridization. These trends do not only concern the governance of the technical infrastructure. They also contribute to reshaping the architecture of freedom and power in the digital environment, giving impetus to a new role for constitutionalism in the digital age. Therefore, the primary question is how far does the evolution of Internet governance leads towards a new constitutional paradigm in the digital age? As digital spaces are governed at the crossroads of a new phase, these trends question the global paradigm at the basis of the Internet, thus opening a new research agenda. By examining the challenges raised by fragmentation, polarization and hybridization in the governance of digital technologies, this work examines emerging challenges to constitutional models protecting rights and limiting powers on a global scale.

KEYWORDS: digital constitutionalism, fundamental rights, power, digital sovereignty, Internet governance

INTRODUCTION

The Internet will likely change face in the next decade. In the form of a Web 3.0 or a Metaverse, established and new norm entrepreneurs are putting forward a new ordering of the Internet.¹ The rampant evolution of digital technologies, powered by 5G connectivity and artificial intelligence technologies, alters the current status of the infrastructure of the Internet and of its governance in unprecedented ways. Behind technical concerns, however, this tension hides an interest in reshaping Internet governance from the roots, affecting the overall distribution of power and

* Centre for Socio-Legal Studies, University of Oxford, Oxford, UK. E-mail: giovanni.degregorio@csls.ox.ac.uk

† Blavatnik School of Government, University of Oxford, Oxford, UK

1 R Radu and others, 'Normfare: Norm Entrepreneurship in Internet Governance' (2021) 45(6) *Telecommunications Policy* <<https://doi.org/10.1016/j.telpol.2021.102148>> accessed 14 February 2022.

the capacity to exercise rights and freedoms. The fragmentation of the global infosphere into national spaces of digital sovereignty,² the increased bifurcation of Internet-based technologies along ideological divides, and the complex dynamics at play for both public and private powers may not only raise questions about the protection of fundamental rights, but also pose broader challenges to established constitutional principles. As the Internet continues to be redefined due to the evolution of digital technologies, so is constitutionalism beyond the state.³

Replacing a unitary Internet with splinters has real implications that go beyond infrastructural governance. This trend of technical decoupling or fragmentation also alters the space(s) where freedoms and powers are exercised. On the one hand, states pose new threats: standards and protocols developed in and by illiberal regimes bring forward novel concerns about embedding control and surveillance in global technologies, at a time of growing technological polarization. On the other hand, private actors are exerting new forms of pressure and influence over digital technologies, impacting existing democratic processes and fundamental rights protections (ie hybridization).⁴ The gradual hybridization of Internet governance blurs the lines between the limits of power and makes it more difficult to uphold the public interest and necessary safeguards for the digital society.

Within this framework, our work scrutinizes how far the fragmentation, polarization and hybridization of Internet governance affect constitutionalism. The new phase of Internet governance challenges the current architecture of rights and freedoms available to digital citizens, thus opening a new research agenda. This article explores key Internet governance directions and the questions they raise for (digital) constitutionalism.⁵ It underlines that these developments not only lead to a shift in infrastructural governance, but also trigger a new paradigm in the social layer, where individuals exercise their rights and freedoms in various political regimes. By focusing on the evolution of a new phase of Internet governance, this work addresses a major gap in the current academic and policy debates, that of neglecting the intersection between Internet governance and constitutionalism. Showing how the politics and governance of the Internet influence constitutional values sheds light on current paths for constitutionalism in the digital age (ie digital constitutionalism).

The first section examines the trend of Internet fragmentation and its consequences on governing the technical and social layer. The second section, underlines how polarization increasingly characterizes the narratives of digital sovereignty that have become dominant in Internet governance. The third section focuses on the hybridization of the functional governance of spaces between public and private ordering, affecting both technical matters and content moderation. The final section discusses

2 L Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33 *Philosophy & Technology* 369; S Couture and S Toupin, 'What Does the Notion of "Sovereignty" Mean when Referring to the Digital?' (2019) 21(2) *New Media & Society* 2305.

3 N Krisch, *Beyond Constitutionalism. The Pluralist Structure of Postnational Law* (OUP 2010).

4 M Moore and T Damian (eds), *Digital dominance: The Power of Google, Amazon, Facebook, Apple* (OUP 2018).

5 G De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19(1) *International Journal of Constitutional Law* 41; N Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019); E Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) *International Review of Law Computers & Technology* 76.

the intersection between Internet governance and constitutionalism, specifically looking at three challenges: the fragmentation of fundamental rights and democratic values, the constitutional boundaries of digital sovereignty and the prevalence of hybrid powers in the digital environment.

FRAGMENTING THE INTERNET: BEYOND TECHNICAL CONCERNS

The potential fragmentation of the Internet is not a new apprehension.⁶ Over the years, several states—including China, Iran and Russia—have talked about separating themselves from the global network. Often referred to as ‘authoritarian’ splinters, such attempts have relied on the development of tight national controls and filtering of content, as well as online activity surveillance.⁷ Technical standards and resources are increasingly considered instruments of national control. While the deployment of Western software for repressing liberties in authoritarian countries has been in the focus of the media,⁸ the development and use of protocols by non-free countries has only recently started to be put in perspective. Standards, such as the Internet Protocol,⁹ or the Border Gateway Protocol,¹⁰ have been deeply entrenched in the architecture of the Internet since its early days, but these standards may change in the coming years. The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol was originally developed as part of the ARPANET programme funded by the US Department of Defense and later globalized by American companies implementing it on their services. As a decentralized network solution, it became the dominant means of Internetworking in the late 1980s. ‘Information wars’ between promoters of various technologies that could enable decentralized transmission of data packets took place in the mid-1980s, notably opposing established telephone oligopolies in favour of virtual circuits to scientists from the Advanced Research Projects Agency Network. Over the years, the most significant changes to this protocol included the transition from IP version 4 (IPv4) to IPv6, an increase to 128-bits addressing in order to respond to the growing number of devices connected to the Internet.

While the TCP/IP remains the backbone of today’s Internet, proposals for alternatives have started to be tabled and are likely to influence both the technical layer and the existing governance model associated with the development of standards. Recent proposals such as the Chinese ‘IP networking for Network 2030’ aim to provide an upgrade to the existing IP protocol to respond to the insufficiency of IPv6 for scalability in next generation networks, with a view to supporting future technologies, including quantum computing. The defining features of the Chinese protocol include: intrinsic security, robustness, determining forwarding, global reachability, best efforts and connection of heterogeneous networks. This project was put forward

6 M Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity Press 2017).

7 E Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs 2012).

8 R Deibert, ‘Authoritarianism Goes Global: Cyberspace Under Siege’ (2015) 26(3) *Journal of Democracy* 64; R Deibert, ‘What To Do About “Dual Use” Digital Technologies?’ (29 November 2016) <<https://deibert.citizenlab.ca/2016/11/dual-use/>> accessed 14 February 2022.

9 L de Nardis, *Protocol Politics: The Globalization of Internet Governance* (MIT Press 2009).

10 AJ Mathew ‘The Myth of the Decentralised Internet’ (2016) 5(3) *Internet Policy Review* <<https://doi.org/10.14763/2016.3.425>> accessed 14 February 2022.

in September 2019 by a representative of Huawei, the world's largest smartphone manufacturer and one of the biggest infrastructure providers. The new IP would connect physical entities of different sizes, from wearables to vehicles, as well as industrial control devices, while providing 'specific quality of service and security policies based on user identity, rather than mapping to something instead'.¹¹

Although the proposal remains vague in terms of technical details, the new IP appears to part ways with the existing architecture when it comes to addressing and forwarding.¹² While presented as a decentralized system, the Chinese proposal would move forward and access services away from the end users to centralized authorities, who would have the capability to block particular data flows if needed. In this scenario, the core of the network would have enhanced control over the end points. Critics note that the proposed 'single master plan' challenges the 'open and flexible system that is much more the result of decades of evolution'.¹³

Technology decoupling is a relatively recent phenomenon, predicated on the ability to expand performance or isolate and protect networks against emerging threats. While it can foster resilience, such decoupling can also introduce new risks on its own. Technologies for re-routing around damage in the case of outages, disruptions,¹⁴ circumventing censorship and network restrictions (eg at the level of DNS) are complemented by multi-level legal safeguards from international law, particularly human rights law, as well as regional and national constitutional safeguards that aim to protect freedom and limit powers.¹⁵ Technical fragmentation thus affects both the daily management of shared resources and their long-term governance, impacting the exercise of rights.

The 2019 Chinese proposal for a new IP has further exacerbated fears of moving away from the decentralized decision making for Internet standards, as the Chinese geopolitical influence over key technical infrastructures is constantly growing. In the case of 5G, building the next-generation wireless networks stirred numerous national controversies about the involvement of Chinese equipment manufacturers, leading to blocking or restricting the share of the Chinese giant Huawei in various markets around the world.¹⁶ In the elaboration of 5G standards, Huawei and China Mobile are leading in terms of contributions on designing standards in the 3GPP framework and own the majority of patents for implementation.¹⁷

11 S Jiang, 'New IP Networking for Network 2030' (2019), presentation delivered at the ITU. <<https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416>> accessed 14 February 2022.

12 S Hoffmann, D Lazanski, and E Taylor, 'Standardising the Splinternet: How China's Technical Standards could Fragment the Internet' (2020) 5(2) *Journal of Cyber Policy* 239.

13 M Hogewoning, 'Do We Need a New IP?' (*RIPE Labs*, 22 April 2020) <https://labs.ripe.net/Members/marco_hogewoning/do-we-need-a-new-ip> accessed 14 February 2022.

14 E Aben 'Does the Internet Route Around Damage? A Case Study Using RIPE Atlas' (*RIPE Labs*, 17 November 2015) <<https://labs.ripe.net/Members/emileaben/does-the-internet-route-around-damage>> accessed 14 February 2022.

15 R Radu, *Negotiating Internet Governance* (OUP 2019).

16 R Radu and C Amon, 'The Governance of 5G Infrastructure: Between Path Dependency and Risk-based Approaches' (2021) 7(1) *Journal of Cybersecurity* <<https://doi.org/10.1093/cybsec/tyab017>> accessed 14 February 2022.

17 IPLytics, 'Who Is Leading the 5G Patent Race? - A Patent Landscape Analysis on Declared SEPs and Standards Contributions' (*IAM*, February 2021) <<https://www.iam-media.com/who-leading-the-5g-pa>>

Standardization processes represent a new direction in the fragmentation of the Internet, as they generally seek to influence global deployments of technology but are not exempt from state influence. New patterns have emerged in the last two decades, since the Chinese government has strongly supported the development of new standards across various venues,¹⁸ not only to secure a first-mover advantage for its companies, but also as an ‘instrument of international power competition’.¹⁹ The 2018 Standards Law specifically encourages international participation of Chinese entities in global standardization processes and puts specific governance structures—such as the Standardization Administration—in charge of harmonizing standards capable of working nationally and internationally. In recent years, there has also been evidence of pressure on partner countries to adopt Chinese-origin standards.²⁰

Technological fragmentation proposals that put forward centralized approaches stand in contrast with the decentralization credo of Internet pioneers and pose new challenges to existing modes of governance. For example, the new IP project presented by Huawei representatives in front of international bodies came with a proposal for establishing a new formal structure to work on this within the International Telecommunications Union, moving the conversation away from the body that has traditionally handled the IP discussions, namely the Internet Engineering Task Force (IETF).

What has allowed the Internet to evolve into a global, decentralized network was the creation and upgrade of protocols and standards in a voluntary manner (although not necessarily in a disinterested fashion). In venues such as the IETF or the Internet Corporation for Assigned Names and Numbers (ICANN), the collaborative work of network engineers—in a personal capacity or as representatives of particular constituencies—meant that the basic standards and protocols underpinning the global Internet could be discussed openly and agreed by a community of experts, in which governmental pressure has always been minimal. This framework is starting to change as most draft proposals come from experts with a strong corporate backing and more attuned to state interests and participation of diverse voices is low.²¹ In the IETF, the standard-making process is currently led by US and Chinese engineers.²²

tent-race-patent-landscape-analysis-declared-seps-and-standards-contributions> accessed 14 February 2022.

18 J Seaman, *China and the New Geopolitics of Technical Standardization* (Ifri 2020).

19 M Kim, H Lee, and J Kwak, ‘The Changing Patterns of China’s International Standardization in ICT Under Techno-nationalism: A Reflection through 5G Standardization’ (2020) 54 *International Journal of Information Management* 102.

20 M Schneider-Petsinger and others, ‘US–China Strategic Competition: The Quest for Global Technological Leadership’ (*Chatham House*, 7 November 2019) <<https://www.chathamhouse.org/2019/11/us-china-strategic-competition>> accessed 14 February 2022; J Hillman, ‘China’s Belt and Road Initiative: Five Years Later’ (*Center for Strategic & International Studies*, 25 January 2018) <https://www.uscc.gov/sites/default/files/Hillman_USCC%20Testimony_25Jan2018_FINAL.pdf> accessed 14 February 2022.

21 C Cath, ‘The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force’ (2021) 45(6) *Telecommunications Policy* <<https://doi.org/10.1016/j.telpol.2021.102144>> accessed 14 February 2022; R Nanni, ‘The ‘China’ Question in Mobile Internet Standard-making: Insights from Expert Interviews’ (2021) 45(6) *Telecommunications Policy* <<https://doi.org/10.1016/j.telpol.2021.102151>> accessed 14 February 2022.

22 D Weyrauch and T Winzen, ‘Internet Fragmentation, Political Structuring, and Organizational Concentration in Transnational Engineering Networks’ (2021) 12 *Global Policy* 51.

The tradition of voluntary expert contributions delivered in the absence of state or business constraints is starting to fade away, making the work on standards a political contest.

The decentralized decision making for Internet standards and protocols that has prevailed so far faces major challenges from both governments and industry. First, new centralized architecture proposals discussed in multilateral venues make inclusive multi-stakeholder governance a lost ideal. Secondly, market leading companies might turn standardization into a private rule-making process implemented through obscure practices.²³ The interests at stake in this new phase of Internet governance might not always be aligned with the protection of fundamental rights, turning technical and information control into a new normative battleground, gravitating around two technospheres, as discussed below.

POLARIZING INTERNET GOVERNANCE: MODELS OF DIGITAL SOVEREIGNTY

The basic Internet infrastructure and the standards and protocols that form its technical backbone has long been considered a neutral foundation,²⁴ a layer separated from political struggles over content. Nonetheless, this perception no longer goes uncontested, considering the possibility to re-configure or manipulate the technical architecture to serve political purposes. Uses as diverse as combating pandemics and monitoring the work of dissidents have shown the dual nature of novel technologies with high potential,²⁵ and both liberal and illiberal regimes have started to adopt digital sovereignty discourses.²⁶ Alongside technical fragmentation, a decoupling engendered by social and legal values embedded in architectural design is likely to have a long-lasting impact on the Internet. The 'hands-off' approach of USA to the decentralized Internet and the state-controlled and centralized Chinese model are often contrasted as their technology giants become more powerful.

The rise in authoritarian splinters and the increased control of the Internet within national borders have eased the transition towards alternative models of digital sovereignty competing with neoliberal approaches. In countries where surveillance and information control are widespread, like the Arab States or China, the Internet has repeatedly been subject to public restrictions leading to the blocking of certain online services and/or the strict monitoring of data.²⁷ The case of Internet shutdowns is an

23 R Radu and M Hausding, 'Consolidation in the DNS Resolver Market – How Much, How Fast, How Dangerous?' (2020) 5(1) *Journal of Cyber Policy* 46.

24 T Wu, 'Network Neutrality, Broadband Discrimination' (2003) 2 *Journal of Telecommunications and High Technology Law* 141.

25 R Radu, 'Fighting the 'Infodemic': Legal Responses to COVID-19 Disinformation' (2020) *Social Media + Society* <<https://doi.org/10.1177/2056305120948190>> accessed 14 February 2022.

26 E Claessen, 'Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU' (2020) 5 *Journal of Cyber Policy* 140.

27 J Zittrain and others, 'The Shifting Landscape of Global Internet Censorship' (2017) Berkman Klein Center Research Publication No 2017-4; R Deibert and others, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press 2008).

extreme example of governments—mostly illiberal—relying on network architecture to express their sovereignty over the digital environment.²⁸

In the international discourse, the internal control paradigm dates back to a 2011 proposal made to the United Nations (UN) Secretary General for an ‘International code of conduct for information security’ (66/359) by the representatives of Russia, China, Tajikistan and Uzbekistan.²⁹ The document assessed that the signatories of the code endeavoured ‘[...] to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries [...] to independent control of information and communications technologies or to threaten the political, economic and social security of other countries’.

Nowadays, digital sovereignty is no longer invoked by authoritarian regimes only. More recent debates have crystallized around national prerogatives to control data flows within online sovereign spaces,³⁰ with the help of the home-grown tech industry. The European Union (EU) itself has adopted a strong technological sovereignty and strategic autonomy stance in the work of the Von der Leyen Commission,³¹ promoting a vision of digital sovereignty that focuses on the needs of Europeans and of the European social model. In this context, ‘digital sovereignty’ is understood as Europe’s ability to act independently in the digital world by implementing a mechanism to foster digital innovation.³² As Europe navigates its own internal tensions, governments around the world have to choose between American and Chinese technologies for their critical infrastructures and for providing their online services.

The bifurcation of the global Internet into American and Chinese technospheres, with their own sets of standards, is likely to reconfigure the current shape of the Internet. From the onset, Internet represented a step-change in communication technologies, presenting open protocols which allowed separately designed networks to interconnect and deliver services to their users under a unified architecture. The vision of the Internet pioneers was that of a global network on which bottom-up and top-down governance approaches co-exist. Current trends might harden the divide between these governance modes, polarizing the global discussions and further dividing this global domain of power.³³

28 G De Gregorio and N Stremlau, ‘Internet Shutdowns and the Limits of Law’ (2020) 14 *International Journal of Communication* 4226.

29 R Radu, ‘Negotiating Meanings for Security in the Cyberspace’ (2013) 15(6) *Info* 32.

30 J Pohle and T Thiel, ‘Digital Sovereignty’ (2020) 9(4) *Internet Policy Review* <<https://policyreview.info/concepts/digital-sovereignty>> accessed 14 February 2022.

31 U Von der Leyen, ‘A Union that Strives for More: My Agenda for Europe. Political Guidelines for the Next European Commission 2019-2024’ (16 July 2019) <https://ec.europa.eu/info/candidate-president_en> accessed 14 February 2022.

32 EPCS, ‘Rethinking Strategic Autonomy in the Digital Age’ (21 November 2019) <<https://op.europa.eu/it/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-118064052>> accessed 14 February 2022; T Barker, ‘Europe Can’t Win the Tech War It Just Started’ (*Foreign Policy*, 16 January 2020) <<https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/>> accessed 14 February 2022.

33 R Radu, JM Chenou, and R Weber (eds), *The Evolution of Global Internet Governance: Principles and Policies in the Making* (Springer 2014); M Kettemann, *The Normative Order of the Internet: A Theory of Rule and Regulation Online* (OUP 2020).

Importantly, this Internet governance schism does not concern only the different strategies adopted by different regimes, but also the role of the private sector, which plays a critical role in managing the infrastructure and the online services.

Historically, developing and using a communication infrastructure was a state prerogative. From the early telegraph times, exercising ‘infrastructural power’ has started to encompass much more than the expression of control over a given territory.³⁴ The communication technologies of the 20th century (radio, telephone, etc) challenged both sovereignty and territoriality, due to their transnational nature and their (almost exclusive) private ownership. The liberal state itself was no longer building and managing the networks. Instead, it entered agreements with private providers as it saw necessary, whether they were based in its national jurisdiction or not.

Under these circumstances, a handful of Western technology companies (Google, Apple, Facebook, Amazon, Microsoft, known as GAFAM) have consolidated their position in the market by building their own architecture and creating the technical means to operate in a self-sufficient manner.³⁵ Submarine cables are a case in point here. The shares of the GAFAM in cable building continue to grow exponentially from year to year.³⁶ In 2018, Google owned 8.5 per cent of the world’s undersea cables;³⁷ by 2019, it was the sole owner of three submarine cables and part owner of 10 more. Facebook also had part ownership in nine cables and was a major capacity buyer for a 10th, while Microsoft was contributing to four cables and Amazon helped to build three more. While a more nuanced discourse is emerging around digital sovereignty in democratic regimes, the influence of the American technosphere is ever so present. While motivated by different interests, American tech giants have in common a growing—and deliberate—push for a unilateral design of technical and behavioural rules and limited public oversight.³⁸

At the other end of the spectrum, illiberal regimes also adapted their strategies to work more closely with the industry to achieve their objectives, thus creating the Huawei model.³⁹ For Chinese authorities, cybersecurity has become a ‘new territory for national sovereignty’, as stated in their National Cyber Security Strategy,⁴⁰ and they have subsequently mandated the collaboration of companies headquartered in China with intelligence agencies in the National Intelligence Law passed in June

34 M Mann, ‘The Autonomous Power of the State: Its Origins, Mechanisms and Results’ (1984) 25(2) *European Journal of Sociology/Archives Européennes de Sociologie* 185.

35 Moore and Damian (n 4).

36 J Miller, ‘This Is What Our 2019 Submarine Cable Map Shows Us about Content Provider Cables’ (*Telegeography*, 19 March 2019) <<https://blog.telegeography.com/this-is-what-our-2019-submarine-cable-map-shows-us-about-content-provider-cables>> accessed 14 February 2022.

37 T Cooper, ‘Google Owns 63,605 Miles and 8.5% of Submarine Cables Worldwide’ (*BroadbandNow*, 12 September 2018) <<https://broadbandnow.com/report/google-content-providers-submarine-cable-ownership/>> accessed 14 February 2022.

38 G Huston, ‘The Death of Transit?’ (APNIC, 28 October 2016) <<https://blog.apnic.net/2016/10/28/the-death-of-transit/>> accessed 14 February 2022.

39 Y Wen, *The Huawei Model: The Rise of China’s Technology Giant* (University of Illinois Press 2020).

40 P Rosenzweig, ‘China’s National Cybersecurity Strategy’ (*Lawfare*, 27 December 2016) <<https://www.lawfareblog.com/chinas-national-cybersecurity-strategy>> accessed 14 February 2022.

2017.⁴¹ The Chinese impetus to develop a new approach on a global scale is straightforward in the largest infrastructure development project of the century, the Belt and Road Initiative, deploying fibre optic connectivity and upgrading technological infrastructures in more than 150 partner countries across four continents. The work is led by Huawei and ZTE and there is Chinese technical assistance offered alongside. This new form of ‘cyber power’ is predicated on a new vision of a digital pole, gravitating around standardization and economic influence over infrastructure building projects.⁴²

The recent attempts to challenge the decentralized Internet architecture have not only further consolidated the polarized areas of power. They have also pushed other states and many non-state actors in the Internet governance space to better define their positions. An important consequence of this process is the blurring of lines between traditional categories such as the public and the private sector. In illiberal countries, where such a distinction is already weak, this challenge leads to a hybridization of the relationship between governments and businesses developing their own model of infrastructural (public) governance. At the same time, in liberal countries, the public–private divide could be undermined with an increasing involvement of the public sector justified by a security and norms-driven ethos to protect the democratic side of the Internet.

However, states are still bound by the limits of national sovereignty. In the global arena, the Internet constantly tests the limits of traditional borders and legitimacy, but also the applicability of power checks and safeguards characterizing modern constitutionalism. The decay of national sovereignty is understood as resulting in ‘a world in which jurisdictional borders collapse, and in which goods, services, people and information “flow across seamless national borders”’.⁴³ Scholars have started to refer to the rise of ‘global law’ to define a meta-legal system where different organizations and entities produce and shape norms with extraterritorial implications.⁴⁴ Therefore, Internet governance can be seen as an expression of global governance, understood as ‘the exercise of authority across national borders as well as consented norms and rules beyond the nation state, both of them justified with reference to common goods or transnational problems’.⁴⁵ This definition acknowledges the role of state and non-state actors outside a given territory but falls short of capturing the extent to which global norm-making and policy processes have become hybrid, as discussed next.

THE HYBRID INTERNET: PUBLIC AND PRIVATE POWERS

Fragmentation and polarization do not tell the full story of the new phase of Internet governance. Another critical piece of the puzzle consists in the consolidation of a

41 MS Tuner, ‘Beijing’s New National Intelligence Law: From Defense to Offense’ (*Lawfare*, 20 July 2017) <<https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>> 14 February 2022.

42 D Broeders, L Adamson, and R Creemers, *A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace* (The Hague Program for Cyber Norms 2019).

43 R Hirschl and A Shachar, ‘Spatial Statism’ (2019) 17(2) *International Journal of Constitutional Law* 387.

44 G Ziccardi-Capaldo, *The Pillars of Global Law* (Ashgate 2008); C Prins and others (eds), *Digital Democracy in a Globalised World* (Edward Elgar Publishing 2017).

45 M Zürn, *A Theory of Global Governance: Authority, Legitimacy, and Contestation* (OUP 2018) 4–5.

hybrid framework characterized by the gradual blurring of lines between the public and the private sector, with long-term consequences on the institutional forms created and on actors' identities themselves. In the last 20 years, the state-centric model has decreased in importance in the face of global processes of convergence, dominated by intergovernmental organizations and transnational corporations.⁴⁶ The EU is one of the leading examples showing the constitutionalization of systems outside national boundaries.⁴⁷ As a result, the unitary state (and its law) is slowly replaced by supranational rules defined by new institutions based on principles and values that transcend territorial borders. In a similar vein, many other regional organizations, including the African Union and the Association of SouthEast Asian Nations, have started designing their own rules for digital matters, increasing the density and sources of authoritative decision making. Within this framework of international actors operating on a global scale, the compliance with international and supranational law is often contested, making constitutionalism global, but 'unbound'.⁴⁸ Its implementation relies increasingly on the participation of non-state actors in governing parts of the network.

Hybridization has brought about a new model of infrastructural (public) governance, where digital technologies are deployed to serve the converged political and economic interests of those in power. However, liberal regimes tend to nominally preserve the public-private divide as an important safeguard for freedom and protection,⁴⁹ but may, in practice, fear the growing involvement of private interests, whether in security-prone interventions or as part of a norms-driven ethos. Fragmenting the global technosphere to retain more control on a national level and centralizing the Internet around a few companies to enhance public enforcement represent two dangerous tendencies for the future use of technology, affecting both the protection of fundamental rights and the rule of law more generally.

China provides an interesting example of the hybridization of Internet governance. China has always monitored online activities,⁵⁰ while building a digital garden wall where national businesses had the time and space to grow outside any form of competition that allows for a partial opening up to digital globalization while maintaining control over the network architecture. This system has led to the creation of Chinese 'digital political economy',⁵¹ focused on increasing surveillance through its businesses, which can collect, use and share data while competing with other actors on a global scale. Nowadays, Huawei, Alibaba, Baidu and Tencent can increasingly compete with the dominant power of GAFAM, while seeing new services like

46 EC Ip, 'Globalization and the Future of the Law of the Sovereign State' (2010) 8(1) *International Journal of Constitutional Law* 635.

47 G de Búrca and JHH Weiler, *The Worlds of European Constitutionalism* (CUP 2012); JH Weiler and M Wind (eds), *European Constitutionalism Beyond the State* (CUP 2003).

48 A Wiener and others, 'Global Constitutionalism: Human Rights, Democracy and the Rule of Law' (2012) 1(1) *Global Constitutionalism* 1, 3.

49 M Goldmann, 'A Matter of Perspective: Global Governance and the Distinction between Public and Private Authority (and not Law)' (2016) 5(1) *Global Constitutionalism* 48.

50 J Zittrain and E Benjamin, 'Empirical Analysis of Internet Filtering in China' (2003), Harvard Law School Public Law Research Paper No 62.

51 Y Hong, *Networking China: The Digital Transformation of the Chinese Economy* (University of Illinois Press 2017).

TikTok getting introduced. Exporting this model abroad and the hybrid logic behind comes with global political aspirations implemented via the work of private intermediaries on a much larger scale.⁵² This is further globalized through infrastructural projects of scale, such as the Belt and Road Initiative, and new proposed standards—including the new IP networking for Network 2030, which provides an alternative protocol for next generation technology.

Liberal regimes, on the other hand, experience an increased hybridization due to private ordering in digital affairs. Starting with the private ownership of digital infrastructure as a key source of power in the information society,⁵³ technology giants enjoy a broad margin of discretion in deciding how to implement their services and their public policy functions. Online platforms are, *de facto*, free to define and interpret users' fundamental rights according to their legal, economic and ethical frameworks, since there are limited laws or regulations currently in place to prevent them from doing so. By virtue of the algorithmic architecture, online platforms can perform autonomous quasi-public functions in a split second, without relying on the oversight of a public authority. Setting the rules for enforcing and balancing users' fundamental rights by using automated decision-making processes moves us further away from constitutional safeguards. This balancing act in a hybrid governance setup is by no means easy. For instance, the decision of social media platforms to remove and consequently delete vast amounts of content, including political speech, is a clear interference with the users' right to freedom of expression on a global scale. At the same time, such content moderation activity could also preserve other fundamental rights such as privacy and protect users from harmful content online.

Historically, this tension dates back to the 1990s, when the USA, and then the EU, decided to follow a liberal approach with respect to regulating the Internet. Early proponents of a libertarian point of view looked at the Internet as a space without the influence of states' authority.⁵⁴ This approach was soon counterbalanced by scholars asserting the possibility to regulate the Internet,⁵⁵ arguing that the result that the international regulation of the Internet is feasible and legitimate,⁵⁶ as was confirmed in the following years.⁵⁷ In time, democratic states have chosen to rely more and more on tech intermediaries to enforce public functions online, as opposed to using direct forms of intervention via governmental means and public actors. This issue was pointed out more than 15 years ago, when the emphasis was placed on the

52 M Keane and H Yu, 'A Digital Empire in the Making: China's Outbound Digital Platforms' (2019) 13 *International Journal of Communication* 4624.

53 G De Gregorio, 'From Constitutional Freedoms to Power: Protecting Fundamental Rights in the Algorithmic Society' (2019) 11(2) *European Journal of Legal Studies* 65.

54 JP Barlow, 'Declaration on the Independence of the Cyberspace' (*EFF*, 8 February 1996) <<https://www.eff.org/cyberspace-independence>> accessed 14 February 2022; DR Johnson and D Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) *Stanford Law Review* 1367.

55 L Lessig, *Code: And Other Laws of the Cyberspace* (Basic Books 1999); JR Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997–1998) 76 *Texas Law Review* 553.

56 JL Goldsmith, 'Against Cyberanarchy' (1998) 65 *University of Chicago Law Review* 1199.

57 A Segura-Serrano, 'Internet Regulation and the Role of International Law' (2006) 10 *Max Planck Yearbook of United Nations Law* 191.

ways in which states could ensure the enforcement of public policies online by regulating network intermediaries, network engineering and technological instruments.⁵⁸

The rapid expansion of digital technologies, combined with the failure of public actors to promptly address digital challenges, has left important governance gaps, slowly filled by new private powers mirroring the exercise of (functional) sovereignty.⁵⁹ Looking at information platforms from a European constitutional standpoint, such entities are private actors. As a result, they can rely on their freedom to conduct business as recognized by the Charter of Fundamental Rights of the EU,⁶⁰ together with fundamental freedoms, especially, the freedom to provide services as set out in the Treaties.⁶¹ From a US constitutional perspective, platforms rely on a different constitutional basis to perform their businesses, in particular their freedom of speech as recognized by the First Amendment.⁶² In both cases, platforms enjoy a 'constitutional safe area' whose boundaries can be restricted only by the prominence of other fundamental rights. However, none of these processes embeds public safeguards to limit the extent to which profit maximization subjects fundamental rights to market logics, showing how the hybridization of governance works in practice.

Therefore, alongside the state expression of digital sovereignty, the ability of technology giants to govern infrastructures and digital spaces based on self-designed rules constitutes another form of power that is in urgent need of checks and balances considering that they perform public functions interfering with individual freedoms in 'black box', automatic processes with no accountability. The hybridization trend stems from state ambitions of tight control via private intermediaries in illiberal regimes, on the one hand, and the transfer of public functions to unregulated digital platforms in liberal regimes, on the other. The diversity of forms under which hybridization might present itself has consequences on the shape that constitutionalism itself might take in this new era of Internet governance, as discussed below.

CONSTITUTIONALISM IN THE NEW ERA OF INTERNET GOVERNANCE

Although it has been seen for a long time as a 'democratizing' platform, the Internet has never been a neutral ground for constitutionalism. Its own architecture and the values it embeds, as well as the way it is used, shape the space in which collective and individual rights and freedoms can be protected. Beyond technical considerations around the value of maintaining a unitary network, fragmenting the Internet would have trickle-down effects on the governance of the social layer, as rights are increasingly exercised online. Standards and protocols developed in/by illiberal regimes

58 MD Birnhack and N Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 *Virginia Journal of Law & Technology* 1; JR Reidenberg, 'States and Internet Enforcement' (2004) 1 *University of Ottawa Law & Technology Journal* 213.

59 F Pasquale, 'From Territorial to Functional Sovereignty: The Case of Amazon. Law and Political Economy' (*Open Democracy*, 5 January 2018) <<https://www.opendemocracy.net/en/digitaliberties/from-territorial-to-functional-sovereignty-case-of-amazon/>> accessed 14 February 2022.

60 Charter of Fundamental Rights of the European Union (2012) OJ C 326/391.

61 Treaty on the Functioning of the European Union (2012) OJ C 326/47.

62 JM Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 *University of California Davis Law Review* 1151.

bring forward concerns of centralization and embedded surveillance, as the use of digital technologies for political and economic control defines the digital space. Likewise, the consolidation of private powers in the digital environment raises questions about the collaboration and competition of these actors with traditional public powers.

This new era of Internet governance is thus intimately connected with (digital) constitutionalism. The project of digital constitutionalism is ‘to rethink how the exercise of power ought to be limited (made legitimate) in the digital age’.⁶³ The Internet serves a multitude of purposes: it is where individuals express their personal identity, where businesses (try to) maximize their profits and where governments increasingly perform their public tasks. In other words, the Internet is more than wires and data centres, it provides a societal foundation for connecting humans, advancing relationships and embedding social values. As both its technical underpinning and governance are about to change, the Internet faces a turning point: the values embedded in its governance model (including openness and interoperability) are likely to affect how constitutional rights and freedoms are exercised on a global scale.

At its core, constitutionalism serves two functions that are critical in relation to Internet governance. First, to ensure the protection of fundamental rights and, secondly, to limit the emergence of powers outside constitutional control. In this light, constitutionalism expresses values of key importance to the digital era. The individual may be subject to multilevel protection—state, regional and global—of public authorities, which are, in turn, legitimized by the people through democratic instruments of participation, as is the case of the EU.⁶⁴ Nonetheless, multilevel constitutionalism is not understood only as hierarchical system, but also as a plural and integrated set of values which, at least in the European framework, balances national identities and common constitutional traditions.⁶⁵

This relationship raises new questions about the role of constitutionalism in the digital age. What comes under scrutiny is the protection of rights and the exercise of power beyond traditional territorial boundaries in a digital ecosystem which is increasingly fragmented, polarized and subject to hybrid powers. The new Internet governance values derived from recent trends are likely to interact with constitutionalism, thus affecting the exercise of rights and limitation of powers coming from international, supranational and national constitutional law. The trends affecting the evolution of Internet governance become consequential for constitutionalism in three main respects: for the protection of rights and freedoms, for the extension of sovereign powers on a global scale, and for the consolidation of areas of unaccountable power.

The Fragmentation of Rights and Freedoms

Modern constitutionalism is built around the protection of a set of guarantees for all individuals, but the relative equilibrium of the constitutional ecosystem is regularly

63 Suzor (n 5).

64 I Pernice, ‘Multilevel Constitutionalism and the Crisis of Democracy in Europe’ (2015) 11 *European Constitutional Law Review* 541.

65 M Fichera and O Pollicino, ‘The Dialectics Between Constitutional Identity and Common Constitutional Traditions: Which Language for Cooperative Constitutionalism in Europe?’ (2019) 20 *German Law Journal* 1097.

tested by digital technologies. In the new era of Internet governance, more opportunities emerge to exercise fundamental rights, and equally, more threats of interference with them as well. Therefore, the safeguards in place for fundamental rights and freedoms need to be complemented by constitutional control and one cannot exist without the other. The fragmentation of the digital ecosystem as a result of new trends in Internet governance can affect the exercise of rights and freedoms. Network splintering, polarization and hybridization bring into sharper focus the extent to which applying different sets of norms and guarantees can undermine the protection afforded to the individual. Fragmentation and polarization can advance the illiberal agenda and further entrench a central authority, overshadowing personal freedoms and other constitutional values and principles such as the rule of law.⁶⁶

Back in 2011, the Council of Europe underlined the role of Internet governance in ensuring the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law.⁶⁷ A decade later, reality clashes starkly with this aspiration. The trend of fragmentation, already underway, spans both technical and socio-political domains. The fundamental interoperability of the global Internet facilitated the exercise of rights online, whether users connected from Argentina or from Russia, but that translated into an unequal protection of digital freedoms. While some countries and regions raised their standards and safeguards, including by imposing obligations on companies, as the EU has done with the General Data Protection Regulation,⁶⁸ others continued to leave the space unregulated. Under these circumstances, the full enjoyment of rights online remains contingent on how constitutionalism might be integrated into global digital policies moving forward.

Currently, the exercise of fundamental rights is challenged on multiple levels, from technical set-ups that allow for mass surveillance to the targeting of individual privacy and related breaches. The sources of concern also vary, depending on how advanced different Internet governance trends might be: on the governmental side, both illiberal and liberal regimes can and do limit, among others, free expression or the right to assembly, online and offline. Neighbouring countries can have different thresholds for respecting and ensuring fundamental rights online or may lean towards regional arrangements with different levels of empowerment for their citizens. Digital technologies have indeed provided new opportunities for public authorities to interfere with fundamental rights and democratic values. The case of Internet shutdowns is the paradigmatic example of how states are still a relevant source of risk for rights and freedoms in the digital age.

At the same time, digital platforms themselves might decide to censor particular types of content and sanction those who infringe their own community rules. When each platform designs its own rules, users are no longer comprehensively protected

66 T Ginsburg and A Simpsen (eds), *Constitutions in Authoritarian Regimes* (CUP 2014).

67 Council of Europe, *Declaration by the Committee of Ministers on Internet Governance Principles*, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6> accessed 14 February 2022.

68 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 (2016) OJ L 119/1.

against violations across services, nor can they benefit from equitable remedies. Access to remedy itself depends on corporate decisions about implementation, especially in the algorithmic society. Despite the regulatory thrust in the last decade, the exercise of rights and freedoms online remains limited to what platforms allow on a technical and ideological level.

The technical, legal and policy fragmentation can actively constrain or restrict certain uses of the Internet, with a direct impact on the enjoyment of rights. When the digital protection of rights and freedoms starts to resemble the splinternet, based on jurisdictional and Internet architecture choices, polarization poses an additional challenge. In a move away from constitutionalism, the separation into two technospheres is becoming more visible via technical standardization processes and group positioning and voting within international organizations. The recent discussions on a global cybercrime treaty are a case in point here. A negotiation to agree a new global convention on cybercrime has been proposed in 2019 by Russia and subsequently started receiving support from a number of developing countries. What is at stake in this negotiation is the degree of control over transnational cooperation and exchange of information on the misuse of the Internet, although the terms are vaguely defined. The resolution that started the process was entitled 'Countering the use of information and communications technologies for criminal purposes' (74/247) and, as of late 2021, the process is co-sponsored by China, alongside Russia. Compatibility with existing arrangements such as the Council of Europe Convention on Cybercrime remains unclear, potentially indicating competition between two sets of norms, divided along political cleavages.

Lastly, the hybridization of Internet governance is consequential for the constitutional equilibrium needed in the digital age. What might even look like a legitimate ground for state actors to expand their authority online, by restricting the reach of the private sector, has a reverse: the public-private ordering in which economic, political and technological functions are impossible to disentangle. This makes it increasingly difficult to navigate islands of protection, ultimately undermining the full enjoyment of rights, whether this affects the digital access to education or the global flow of information. In the information society, the worst-case scenario features decentralized and unaccountable entities exercising unbounded power in new hybrid forms.

Digital constitutionalism is currently at a crossroads, where the exercise of rights is also affected by the projection of digital sovereignty on a global scale and the consolidation of hybrid powers in unaccountable ways, as explained below. Alterations in Internet governance are both drivers and reflections of changes in the world order, where constitutional values and principles no longer define the spectrum of liberal and illiberal interactions.

The Constitutional Boundaries of Digital Sovereignty

Territory is the natural limitation of sovereign powers. The power of the state to regulate its citizens is usually limited to a certain territory; outside this physical space, citizens are subject to the influence of other sovereign powers. Within this framework, constitutionalism plays a critical role in shaping the boundaries of sovereign

powers and this is particularly evident when constitutionalism meets transnational phenomena. From these exchanges rules emerge to protect freedoms and limit powers that are not subject to national logics but are shaped by external norms and models of governance. The different paths taken by states to regulate the Internet are more than political choices, as they are also driven by the constitutional peculiarities of different legal systems in interaction with transnational phenomena. In what follows we discuss the example of freedom of expression to illustrate the complexity of constitutional protections for global data flows.

In the USA, the First Amendment still provides a shield against any public interference with freedom of speech, enabling US companies to extend their powers and standards of protection beyond the American territory in the services they provide abroad. Despite multiple attempts and proposals to regulate platform power at the federal level,⁶⁹ and even at the local level—for example in Florida,⁷⁰ private ordering remains embedded in the dominant liberal approach, which also hides an indirect and ommissive way to extend constitutional values beyond territorial boundaries. Rather than intervening in the market, the US government has opted for consolidating the space for a liberal hub in which American technology giants can thrive on a global scale.

Under these circumstances, it is certain that the failure to limit the power of platforms in the USA does not only stem from an entrenched constitutional protection of free speech, but also from a clear lack of incentives. Regulating platforms that run services for billions of users worldwide could affect the global position of these leading tech companies, while revealing the so-called ‘invisible handshake’⁷¹ between the government and industry in sensitive areas of cooperation, such as security. The 2013 Snowden revelations have proven how far public authorities rely on Internet companies to extend their surveillance programmes and escape accountability.⁷² In other words, this model of American digital sovereignty has been successful and the USA will continue to build on private ordering and the invisible cooperation between public and private actors as the way to move forward in the algorithmic society.

The EU, on the other hand, has already shown its ability to influence global dynamics via the so-called ‘Brussels effect’.⁷³ It should not come as a surprise that the EU has also started to build its narrative about digital sovereignty based on ensuring the integrity and resilience of the data infrastructure, networks and communications, aimed at mitigating dependency on other parts of the globe for critical technologies.⁷⁴ The EU has also started to discuss protective mechanisms and tools to foster

69 M Kelly, ‘All the Ways Congress Is Taking on the Tech Industry. Every Bill, Every Plan, Every Threat’ (*The Verge*, 3 March 2020) <<https://www.theverge.com/2020/3/3/21153117/congress-tech-regulation-privacy-bill-coppa-ads-laws-legislators>> accessed 14 February 2022.

70 D McCabe, ‘Judge Blocks Florida Law Regulating Social Media Companies’ (*The New York Times*, 30 June 2021) <<https://www.nytimes.com/2021/06/30/technology/florida-law-social-media-desantis.html>> accessed 15 February 2022.

71 MD Birnhack and N Elkin-Koren, ‘The Invisible Handshake: The Reemergence of the State in the Digital Environment’ (2003) 8 *Virginia Journal of Law & Technology* 1.

72 D Lyon, *Surveillance after Snowden* (Polity Press 2015).

73 A Bradford, *The Brussels Effect. How the European Union Rules the World* (OUP 2020).

74 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Shaping Europe’s digital future [2020] COM (2020) 67 final.

digital innovation (including in cooperation with non-EU companies). As observed by the European Council, '[t]o be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure.'⁷⁵ However, in this case, the ECJ has underlined the constitutional limits of digital sovereignty in at least in two cases. In *Google v CNIL*,⁷⁶ the ECJ observed that freedom of expression does not enjoy the same degree of protection at the international level and, in Europe, it can vary from one Member State to another. Therefore, it is not possible to provide a general obligation to delist links and information applying to all Member States. Likewise, in *Glawischign-Piesczek v Facebook*,⁷⁷ the ECJ specified that Member States should take into consideration their international obligations given the global dimension of content circulation, without specifying which rules of international law would apply in this case.

Meanwhile, China and Russia offer multiple examples of how illiberal regimes propose alternative models of Internet governance based on their own values.⁷⁸ Particularly, China has always controlled its market from external interferences and used extensive censorship on free expression, rather than using a liberal or laissez-faire approach. More recently, though, China has adopted some liberal strategies and is currently promoting outside its borders a Western conception of Internet economy, while maintaining control over content and over its businesses on a national level. Baidu, Alibaba and Tencent are increasingly competing with the dominant power of GAFAM, but remain accountable to Beijing. The international success of TikTok—a social networking service where users post their short videos—is an example of how China aims to attract a global audience of users while supporting innovation in its business sector.⁷⁹ However, polarization shows the limits of competition. Sustained efforts by the US government to ban TikTok and WeChat are a case in point here.⁸⁰

China is a global player in digital affairs, including in the building of the core infrastructure, as the Belt and Road Initiative shows.⁸¹ The Huawei model is based on exporting technological power supplying digital infrastructure even in peripheral areas.⁸² China is therefore partially opening up to digital globalization while maintaining control over the network architecture and over content within its national

75 European Council, 'Special meeting of the European Council (1 and 2 October 2020) – Conclusions' (*European Council*, 2 October 2020) <<https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>> accessed 14 February 2022;

76 Case C-507/17, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)* (*Google v CNIL*) [2019] ECLI:EU:C:2019:772.

77 Case C-18/18, *Eva Glawischign-Piesczek v Facebook Ireland Limited* [2019] ECLI:EU:C:2019:821.

78 D Broeders and others, 'Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace' (*The Hague Program for Cyber Norms Policy Brief*, November 2019) <<https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace>> accessed 14 February 2022; Claessen (n 26);

79 Keane and Yu (n 52).

80 K Rogers and C Khan, 'Biden Revokes and Replaces Trump Order That Banned TikTok' (*The New York Times*, 9 June 2021) <<https://www.nytimes.com/2021/06/09/us/politics/biden-tiktok-ban-trump.html>> accessed 15 February 2022.

81 J Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (OUP 2021).

82 Wen (n 39).

borders. This two-fold approach has been called the Beijing effect and provides an alternative model to the American and European approaches to the protection of constitutional rights.⁸³ Besides the deliberate attempts by China to extend its technological influence across African countries,⁸⁴ the Chinese Internet governance model also transpires in global international organizations such as the UN.⁸⁵

This framework underlines how constitutional values shape the expression of digital sovereignty, and its manifestations outside national borders. As opportunities to escape constitutional obligations grow and become more difficult to contest in a polarized world, the hybridization of Internet governance outlines the limits of accountability.

The Consolidation of Hybrid Powers

The new era of Internet governance is characterized by a clear consolidation of hybrid powers, which makes the distinction between public and private authority more difficult to disentangle. This consolidation is the main result of the neoliberal approaches followed by constitutional democracies at the end of the last century. The Internet was perceived as a crucial infrastructure to foster fundamental rights and freedoms, especially through the services offered by private actors. Among these were social media platforms and search engines, facilitating access to information and individual expression, as well as offering new means to mobilize online. Intervening in this market was understood both as a drawback for innovation and as a potentially disproportionate interference with economic freedoms and fundamental rights. Therefore, under the guise of protecting democratic values, public intervention has been considered a risk, rather than a safeguard, for the protection of rights and freedoms. Besides, the digital liberal approach was also built on the interest of public actors to maintain the cooperation with the private sector in strategic sectors such as security, in a so-called invisible handshake between states and technology giants.⁸⁶

The liberal framework driving the digital policies of constitutional democracies has mitigated public interference in the digital environment and encouraged a pervasive hybridization between state and private interests. Directly and indirectly, this approach has helped the consolidation of private powers in governing the flow of information online and developing new instruments of surveillance based on the processing of vast amount of personal data.⁸⁷ The spread of disinformation and the misuse of data have repeatedly made the headlines since the start of the COVID-19 pandemic, pinpointing once more the enormous control exercised by private actors in the new digital ecosystem.⁸⁸ From the Arab Spring to the Cambridge Analytica

83 MS Erie and T Streinz, 'The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance' (2021) 54(1) *New York University Journal of International Law and Politics* 1.

84 I Gagliardone, *Africa, and the Future of the Internet* (ZED 2019).

85 G Negro, 'China's perspective on Internet governance: a more integrated role in global discussion?' (2022) *Journal of Chinese Political Science* (forthcoming).

86 MD Birnhack and N Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 *Virginia Journal of Law & Technology* 1.

87 JM Chenou and R Radu, 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' (2019) 58(1) *Business & Society* 74; R Radu and M Hausding, 'Consolidation in the DNS Resolver Market – How Much, How Fast, How Dangerous?' (2020) 5(1) *Journal of Cyber Policy* 46.

88 P Pitruzzella and O Pollicino, *Hate Speech and Disinformation: A European Constitutional Perspective* (Bocconi University Press 2020).

scandal and to online hate speech inflaming the genocide in Myanmar,⁸⁹ numerous examples from the last decade show that the contestation of democratic processes and human rights has moved online.

A *fil rouge* connects these examples. The power of private actors, mainly large corporations, to determine the protection of fundamental rights and shape democratic values on a global scale is mediated via the network's architecture. *Inter alia*, modern constitutionalism aims, on the one hand, to protect fundamental rights, and, on the other, to limit the emergence of powers outside constitutional control. This issue is intimately connected with the role of constitutional law in the information society. The predominant role of decentralized and unaccountable entities exercising powers mirroring public authority would look like a legitimate ground for state actors to expand their authority online. The challenges raised by private powers would appear as a legitimate ground to increase powers by restricting the freedoms of the private sector. This trend leads to increased surveillance and control. In this light, attempts by state actors to regain authority by impacting the architecture of the Internet represent powerful ways to regulate the digital environment.

In the European framework, a new wave of (digital) constitutionalism is rising as a shield against the discretionary exercise of power by online platforms in the digital environment. As pointed out by Vestager, a few online platforms play a critical role for democracy since 'they define our public space – and the choices they make affect the way our democracy works'. As also underlined, '[t]hey affect the ideas and arguments we hear – and the political choices we believe we can make. [...] So we can't just leave decisions which affect the future of our democracy to be made in the secrecy of a few corporate boardrooms.'⁹⁰ That is why one of the main objectives of the proposed Digital Services Act is to protect democracy by mandating that platforms start being (more) transparent about how their algorithms work and (more) responsible for their decision-making processes.⁹¹ In response to recent challenges raised by platforms in the EU, the Commission intends to use the Digital Services Act as a legal instrument in order to better control the space of private power and reduce the impact of private decisions on European democratic values.

Moving from the European example to global Internet governance trends, the primary challenge for digital constitutionalism is to ensure not only that public interferences online are minimized, but also that the public–private cooperation is brought in line with the constitutional values underpinning fundamental rights and democracy. As more divergent paths are chosen for digital governance and more efforts are put into splintering the Internet, the role of constitutional principles is repeatedly called into question.

89 Human Rights Council, 'Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar' (12 September 2018) <https://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf> accessed 14 February 2022.

90 M Vestager, 'Algorithms and Democracy' AlgorithmWatch Online Policy Dialogue (30 October 2020) <https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/algorithms-and-democracy-algorithmwatch-online-policy-dialogue-30-october-2020_en> accessed 14 February 2022.

91 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM (2020) 825 final.

CONCLUSION

This article explored a new phase of Internet governance characterized by fragmentation, polarization and hybridization. It underlined how these recent trends are affecting more than the technical governance of the infrastructure, impacting the core architecture of power and freedoms in the digital environment. These dynamics give impetus to a new role for global constitutionalism in the information society, showing how different orders and types of authority interact on a global scale and why we need to better define checks and balances. They demonstrate that constitutional questions are increasingly scrutinized beyond the state, and thus require public policy approaches that acknowledge political, technological and economic interests.

As liberal and illiberal regimes are increasingly involved in governing digital spaces, establishing rules for how the Internet evolves is intrinsically intertwined with constitutionalism, providing opportunities for exploring a new research agenda. This work shows that key challenges to digital constitutionalism come from multiple expressions of power clashing along several dimensions, including jurisdictional and ideological ones. Discussing the recent trends of fragmentation, polarization and hybridization of Internet governance, we note that two core constitutional functions are put to test: first, the protection and exercise of fundamental rights and secondly, the limitation of unaccountable power. These functions depend on the regulation of both the technical and the social layers. While illiberal regimes might benefit from extending their powers online and blocking the expression of legal pluralism, liberal systems face a major impasse between accelerating the move towards mass-surveillance and entrusting the private sector to safeguard individual liberties and freedom using regulatory incentives.

Looking at attempts to fragment the Internet, a shift in its technical governance towards integrating control-prone standards and centralized enforcement could undermine the multi-level protection of rights coming from international, supranational and national constitutional law. Polarization poses an additional challenge: the American and Chinese technospheres expand beyond standardization processes into global governance dynamics, whether it is for the establishment of international conventions or for normative efforts. Lastly, the hybridization of Internet governance is achieved through the continuous blurring of private-private ordering in the exercise of public interest functions, in democratic and authoritarian systems alike. When technology giants and digital platforms exercise unbounded power, at stake is the full enjoyment of individual and collective rights and freedoms guaranteed by constitutionalism.

This new research agenda holds a lot of promise. A clear examination of the challenges faced by our political and legal systems when infrastructural shifts occur is both timely and much needed. In the new era of Internet governance, digital constitutionalism can provide a new research angle to study how rights and powers are exercised and to what extent the traditional functions of constitutionalism are reframed in the digital age. The challenges raised by the evolution of Internet governance underline how digital constitutionalism does not lead to a single answer but encourages us to examine how different models address the question of rights and powers embedded in different institutional and cultural logics across global and local dimensions in the digital age.