the SPANISH YEARBOOK of INTERNATIONAL LAW

The normative dimension of platform governance: big tech and digital platforms as normative actors

Josep IBÁÑEZ MUÑOZ *

Abstract: Big tech and digital platforms are not only market players or even political agents, but also normative actors and sources of authority for users, consumers and even governments. Virtual communities shape a global public domain and transcend the private nature of the services and spaces of interaction provided by private corporations. In the global public domain of cyberspace, States appear as dysfunctional and heterogeneous entities for the regulation of content, whereas global platforms have become normative actors effectively shaping the behavior of individuals and groups of all sorts through code, algorithms and business models. The relevance of this normative dimension of platform governance deserves a normative acknowledgement as well as a critical consideration.

Keywords: Virtual communities – big tech – digital platforms – normative actors – platform governance

(A) INTRODUCTION

Recent years have seen an increasing tension between States and non-state actors in relation to the establishment of norms for the use and functioning of internet around the globe. Since the first decades of the creation and expansion of cyberspace, its universal, transnational and decentralized nature favoured the development of cyberlibertarian conceptions stressing the democratic potential of networks; digital citizens, netizens, would enjoy freedom and creativity in spaces beyond the limitations of territories shaped by political geography and geopolitics. However, the reality of cyberspace in the 21st century has been partly shaped by States, and the so-called return to geopolitics[1] has entailed a remarkable wave of regulation with the aim of controlling internet users within state borders, even beyond them, as well as the projection of state power with cyberoperations, in what can be seen as the emergence of cybergeopolitics.[2]

Between these two coexisting trends, big tech companies and digital platforms have become central players for the articulation of communication on the internet. The notion of platform adopted here is a broad one, "a programmable architecture designed to organize interactions between users — not just end users but also corporate entities and public bodies" on the internet, as defined by Dijck, Poell and Waal.[3] Such digital constructs have created the virtual spaces where users, consumers and

* Associate Professor of International Relations, University Pompeu Fabra. Email: josep.ibanez@upf.edu.

1 S. Guzzini (ed), *The Return of Geopolitics in Europe?: Social Mechanisms and Foreign Policy Identity Crises* (Cambridge University Press, Cambridge, 2012), and W. R. Mead, 'The Return of Geopolitics', 93(3) *Foreign Affairs* (2014) 69-79.

2 R. J. Deibert, 'The geopolitics of internet control: Censorship, sovereignty, and cyberspace', in A. Chadwick, Ph. N. Howard (eds), *Routledge Handbook of Internet Politics* (Routledge, New York, 2009) 323-336; Ch. C. Demchak and P. Dombrowksi, 'Rise of a Cybered Westphalian Age', 5 *Strategic Studies Quarterly* (2011) 32-61; R. Nieto Gómez, 'Cybergéopolitique: de l'utilité des cybermenaces', 152-153(1-2) *Hérodote* (2014) 98-122; J. Sheldon, 'Geopolitics and Cyber Power: Why Geography Still Matters', 36(5) *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy* (2014) 286-293; C. Cuihong, 'Geopolitics in the Cyberspace: A New Perspective on U.S.-China Relations', 39(1) *The Journal of International Studies* (2018) 9-37.

3 J. van Dijck, T. Poell and M. de Waal, *The Platform society. Public Values in a Connective World* (Oxford University Press, Oxford, 2018), at 4. In this volume the anatomy of platforms is depicted by stressing the relevance of some elements: "a platform is fueled by *data*, automated and organized through *algorithms* and *interfaces*, formalized

 DOI: 10.17103/sybil.25.8

citizens interact according to both the rules of digital platforms and the rules of states. The normative settings of these interactions online are more complex and diverse than the public norms that states adopt and enforce in their fragmented territorial spaces. On the internet, a diversity of public and private actors and authorities cooperate and compete in the management of the public interest with overlapping or conflicting norms, shaping so the behaviour of individuals, groups and organizations of all sorts.

The following pages overviews some of the features of digital platforms and the normative challenges they pose to States, characterized as dysfunctional polities to govern the global public domain of cyberspace. In light of the complexity of platform governance, a conceptual framework is suggested to depict normative processes in terms of normative flows or streams running along normative courses or channels, which are shaped according to the normative action by both public and private actors and authorities.

(B) GLOBAL PUBLIC SPACES, DYSFUNCTIONAL POLITIES AND NORMATIVE CODE

Interactions among users of platforms, applications and services on the internet are at the origin of virtual communities, defined by H. Rheingold back in 1993 as "social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace."[4] The nature of such Computer-mediated communities (CMC) or electronic communities has extensively been debated, and with the experience of recent decades we can assume by now not only that they are versions of real communities, but also that they affect 'real life' communities and, actually, they are themselves real communities, as suggested by B. Wellman and M. Gulia.[5] They may be conceived as 'communities of practice', 'virtual arenas', 'virtual networks' or 'networked virtual communities',[6] but in most cases these social interactions online take place in public spaces constituted by millions of users, and transcend territorial, social, functional boundaries. Such communities are transnational in their scope, heterogeneous in terms of participation, and very diverse in their functionality and interests.

Although private corporations articulate this social reality with their digital services, the sheer dimension and scale of virtual communities make them public spaces of interaction, well beyond the private nature of the platforms hosting, facilitating and reproducing them. Like in many areas of social and economic life, industry self-regulation effectively grants private companies a public role in terms of governance.[7] Thus, big tech companies and digital platforms have assumed and performed with their private means functions of global governance in the transnational public spaces where virtual communities exist.

Since they are shaped and organized according to patterns and rules designed and embedded in the

---

through *ownership* relations driven by *business models*, and governed through *user agreements*." *Ibid.*, at 9.

[4] H. Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Addison-Wesley, Reading, MA, 1993), at 5.

[5] Wellman, B., & Gulia, M., 'Net surfers don't ride alone: Virtual communities as communities', in M. Smith & P. Kollock (eds), *Communities in cyberspace* (Routledge, London, 1999), at 167-194.

[6] A comprehensive discussion of these conceptions can be found in D. Ellis, R. Oldridge and A. Vasconcelos, 'Community and Virtual Community', in B. Cronin (ed), *Annual Review of Information Science and Technology*, (information Today, Medford, 2004), at 145-186, doi: 10.1002/aris.1440380104.

[7] V. Haufler, *Public Role for the Private Sector: Industry Self-Regulation in a Global Economy* (Carnegie Endowment for International Peace, Washington, DC, 2001).

software of apps and platforms hosting them, they are not spontaneous or unlimited spaces of interaction, but social arenas with some degree of institutionalization. They are, therefore, part of the global public domain, understood by J. G. Ruggie as "an increasingly institutionalized transnational arena of discourse, contestation, and action concerning the production of global public goods, involving private as well as public actors."[8] And there is, therefore, a global public interest, an interest with a communitarian dimension (qualitatively different from the aggregate interests of States), arising from rational deliberation and open participation, and the beneficiaries of which are not only States, but humankind (individuals and peoples of present and future generations).[9]

In cyberspace States have not always been able nor willing to assume and perform the provision of public goods such as regulation of interactions in virtual communities. These difficulties, or reluctance, to control the internet derive from a variety of factors, such as the pace of technological innovation, the lack of awareness about the depth of transformations brought about by the revolution of Information and Communication Technologies (ICTs), the plurality of governmental approaches and policies (from democratic to authoritarian), or the calculated strategies by some powerful States to enjoy their technological advantage in the digital world. But the essential issue at stake is the dysfunctionality of territorial entities to deal with trans-border functional realities, especially if from a liberal democratic perspective fundamental rights and freedoms of citizens are to be preserved. As in other areas of international life, connectivity in cyberspace severely disrupts political geography and modern territoriality.[10] States, and notably democratic governments, appear as dysfunctional political entities to manage the coexistence of spaces-of-flows with spaces-of-places and the challenges of unbundled territoriality.[11]

For States the regulation of cyberspace has been extremely difficult due to the architecture of the internet, but this un-regulation of the Net is a feature of the past, as noted by L. Lessig.[12] During the 21st century, both States and technological companies have 'tamed' the cyberspace, although through different means and for different purposes. For most governments, the internet has eventually been understood as a domain that can and must be controlled, just like other more familiar domains of modern territoriality. But for ICT companies, this possibility was clearly understood since the beginning of electronic markets. The policy of commercialization and privatization of the Net completed by the United States government by 1995 represented for ICT companies the opening of huge business opportunities, and these commercial activities entailed the design and implementation of software products and business models which effectively shaped the way users, consumers, and virtual communities at large would behave in the cyberspace.

The normative dimension of software was eloquently stressed by L. Lessig in 1999: "In real space we recognize how laws regulate -through constitutions, statutes, and other legal codes. In cyberspace we must understand how code regulates —how the software and hardware that make cyberspace what

---

[8] J. G. Ruggie, 'Reconstituting the Global Public Domain — Issues, Actors, and Practices', 10 *European Journal of International Relations* (2004) 499–531, at 504.

[9] O. Casanovas and J. Rodrigo, *Compendio de Derecho internacional público* (3rd ed., Tecnos, Madrid, 2014), at 341-342, and N. Bouza, C. García and A. J. Rodrigo, '¿Hacia *Worldfalia*? La gobernanza política y jurídica del interés público global', in N. Bouza, C. García and A. J. Rodrigo (eds), *La gobernanza del interés público global* (Tecnos, Madrid, 2015), at 43-44.

[10] P. Khanna, *Connectography. Mapping the future of global civilization* (Random House, Madrid, 2016).

[11] J. G. Ruggie, 'Territoriality and Beyond: Problematizing Modernity in International Relations', 47 *International Organization* (1993) 139-174.

[12] L. Lessig, *Code and other laws of cyberspace* (Basic Books, New York, 1999) and L. Lessig, *Code version 2.0* (Basic Books, New York, 2006).

 DOI: 10.17103/sybil.25.8

it is *regulate* cyberspace as it is… Code is law."[13] And it was through code that some companies explored and exploited the opportunities of using software and system design to make money on the internet. As early as the 1990s AOL adopted a 'walled garden' strategy embracing advertising campaigns with sponsored content and service for its captive audiences. And in the early 2000s Larry Page and Sergei Brin at Google took a strategically decisive path: in spite of their aversion for advertising, in order to solve the company's lack of revenue, they decided to resell the attention gained by its search engine. Basically, they enabled a brilliant algorithm to be used for commercial purposes. In the following years many other websites and platforms hosting blogs, videos and all sorts of information rushed into commercial activities enabled by code. The transparency of advertising tactics like the clickbait was absent and most users totally unaware of the advent of the model of the attention merchant, as named by Tim Wu.[14] This same reality has been depicted as 'platform capitalism' by Nick Srnicek, who explains how advertising platforms appropriate data as a raw material and their revenue results "from the extraction of data from users' activities online, from the analysis of those data, and from the auctioning of ad space to advertisers."[15] The argument is further pushed by Shoshana Zuboff in her explanation of the 'extraction architecture', according to which digitalization and datafication (the application of software that allows computers and algorithms to process and analyze raw data) have resulted in 'surveillance capitalism', in which "software programs and their algorithms that function automatically, continuously, ubiquitously, and pervasively to achieve economies of action."[16]

Such business models, sustained and enhanced by software code, effectively shaped the behaviour of internet users in a sophisticated and rapidly changing environment which was beyond the reach of legal norms and regulation. Code and algorithms of digital platforms started to operate as mechanisms of control by establishing the technical conditions of user's activities and interactions online: cookies, content filtering, user's identification, geo-localization, and many other automated technical 'solutions' enabling or disabling choices for users, just like regulation allows or bans behaviours for citizens.

(C) NORMATIVE FLOW, NORMATIVE CHANNELLING, AND PLATFORM GOVERNANCE

A proper understanding of the normative dimension of decisions adopted by software engineers and digital platforms requires a conceptual framework which is complementary or alternative to theories about norm creation, diffusion and transformation in international relations and international law.[17]

---

[13] L. Lessig, *Code and other laws of cyberspace… supra* n. 9, at 6. The 'code is law' argument was originally inspired by W. J. Mitchell, *City of Bits: Space, Place and the Infobahn* (MIT Press, Cambridge, MA, 1995), at 111. The idea that technological capabilities and system design act as rules for participants had already been formulated in L. Lessig, 'Reading the Constitution in Cyberspace', 45 *EMORY L.J.* (1996) 896-97, at 869; and it was also stressed soon after by J. R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' 76 *Texas Law Review* (1998) 553-593. In Reidenberg's words, "the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage", *Ibid.*, at 555.

[14] T. Wu, *The attention merchants. The epic scramble to get inside our heads* (Alfred A. Knopf, New York, 2016).

[15] N. Srnicek, *Platform Capitalism* (Polity, Cambridge, 2017), at 30.

[16] S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power* (Public Affairs, New York, 2019), at 305.

[17] On the notion of norm entrepreneur and the adoption of such role by companies and other private actors in the normative process, see C. R. Sunstein, 'Social Norms and Social Rules', 96 *Columbia Law Review* (1996) 903-929; H. H, Koh, 'Why Do Nations Obey International Law' (106) *The Yale Law Journal* (1997) 2599-2659; M. Finnemore and

The regulation of platforms illustrates processes which may be different to those conveyed through the notion of norm entrepreneurship, norm diffusion as 'cascades'[18] or 'cycles',[19] or the role of 'contestation' in global governance,[20]

As a complementary explanation, rather than as an alternative, we suggest here that normative processes take the form of *normative flows* or *streams*: dynamic and heterogeneous sets of norms evolving within *normative courses* or *channels* which effectively affect social and economic practices, policies and even technologies. These analogies of water flows, streams, courses and channels offer a convenient image for the kind of fluid interaction between public and private norms resulting from the intervention of public and private actors in domestic, international, transnational and global environments.

Following A. Wiener's typology of norms,[21] a plurality of fundamental norms, organizing principles, and standardized procedures and regulations coexist and interact dynamically within normative channels created by normative actors, as well as by the same norms. In contrast with the image of cycles, the metaphor of channels conveys an idea that normative flows can retake previously existing courses (as in a cycle) or can open new ones. Normative processes may be affected by new technological means, by the participation of new actors or by the evolving prevalence of some normative tools, and the resulting channels drive norms towards areas previously unknown. Such normative channelling will vary in different States, in different regions and in transnational and global contexts, and these contextual differences account for the diversity and asymmetry of normative flows, always subject to dynamic forces of change and adaptation.

Normative flows and normative channelling seem a suitable conceptual framework to understand platform governance, defined by R. Gorwa as "layers of governance relationships structuring interactions between key parties in today's platform society, including platform companies, users, advertisers, governments, and other political actors."[22] At least three variables seem particularly relevant to account for the variations in normative flows and normative channelling of platform governance: the type of normative actors, the public-private nature of norms, and the type of regulatory tools.

(1)Normative actors

The plurality of actors creating, implementing and enforcing norms in digital platforms can be organized along three basic relevant distinctions. The first one would stress how differently States and companies have approached the regulation of platforms. As suggested above, some prominent

K. Sikkink, 'International Norm Dynamics and Political Change', 52 *International Organization* (1998) 887-915; A. Acharya, 'How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism' 58 *International Organization* (2004) 239-275; W. Sandholtz, 'Dynamics of International Norm Change: Rules against Wartime Plunder', 14(1) *European Journal of International Relations* (2008) 101–131, doi: 10.1177/1354066107087766; S. E. Goddard, 'Brokering Change: Networks and Entrepreneurs in International Politics', 1 *International Theory* (2009) 249-281; M. Finnemore and D. Hollis, 'Constructing Norms for Global Cybersecurity', 110(3) *American Journal of International Law* (2016) 425-479, doi:10.1017/S0002930000016894.

[18] M. Finnemore and K. Sikkink, *supra* n. 12.

[19] W. Sandholtz, *supra* n. 12; A. Wiener, *A Theory of Contestation* (Springer, Berlin, 2014).

[20] *Ibid.*, and A. Wiener, 'A Theory of Contestation — A Concise Summary of Its Argument and Concepts', 49(1) *Polity* (2017) 109-125.

[21] A. Wiener, *The Invisible Constitution of Politics: Contested Norms and International Encounters* (Cambridge University Press, Cambridge, U.K., 2008), at 66.

[22] R. Gorwa, 'What is platform governance?', 22(6) *Information, Communication & Society* (2019) 854-871, at 854 doi: 10.1080/1369118X.2019.1573914.

companies played a leading role in shaping the behaviour of users and consumers on the internet. The pace of technological and business innovation offered them a privileged position to decide through code, business practices and private regulation how individuals, groups and institutions would use their services, what information would be exchanged and how asymmetrically power would be allocated in the Net.

During the last two decades this 'platform ecosystem'[23] has become dominated by five high-tech companies with headquarters on the West Coast of the United States: Apple, Microsoft, Alphabet (Google), Amazon and Meta (Facebook). This 'Big Five' groups concentrate ownership and control of key platforms, apps and digital services from North America, and in some industries and activities they share the market with platform companies like Salesforce, Netflix, Paypal, Shopify, ServiceNow, Airbnb, Booking.com, Uber or Twitter. In Europe few and smaller software companies and platforms can compete with their American rivals, like SAP or Spotify do. In Asia, excluding China, only tech companies like Samsung or Sea (Garena) would rank among the top players. And the peculiar Chinese platform ecosystem is dominated by giants like Tencent, Alibaba, Meituan, Jingdong Mall, Pinduoduo, Baidu, East Money Information or Kuaishou Technology. Thus, worldwide a reduced group of corporations concentrate the economic activity and market value of the platform ecosystem.[24] Such oligopoly results from the new dominant surveillance capitalism's logic of accumulation,[25] and in the normative process gives big tech companies an upper hand to design, create, implement and enforce private regulation on users/consumers. In platform governance they are central actors, 'global governors' who effectively manage the public interest according to their private interests[26]; as noted by T. Gillespie, "while part of the question must be how platforms are governed, an equally important question is how platforms govern".[27]

The ecosystem is shared with some normative actors from outside the private sector, such as governments, NGOs and other actors of civil society. But only States and intergovernmental organizations have truly nourished the normative flow of platform governance with regulation, and they have done it rather recently and in very dissimilar ways. This is actually the second important

---

[23] J. van Dijck, T. Poell and M. de Waal, *supra* n. 1, at 12.

[24] Largest tech companies by market cap and Largest internet companies by market cap, 2022.

[25] S. Zuboff, *supra* n. 14.

[26] On the notion of 'global governors' to include private actors and authorities, D. D. Avant, M. Finnemore and S. K. Sell (eds), *Who governs the globe?* (Cambridge University Press, New York, 2010), at 1-2.

[27] T. Gillespie, 'Regulation of and by platforms', in J. Burgess, A. Marwick and T. Poell (eds), *The SAGE Handbook of Social Media* (SAGE, London, 2018) 254-278, at 262. This same argument is shared by a number of scholars when analyzing specific practices by platfoms in diverse issue areas: D. K. Citron, *Hate crimes in cyberspace* (Harvard University Press, Cambridge, MA, 2014); L. DeNardis and A. M. Hackl, A. M., 'Internet governance by social media platforms', 39(9) *Telecommunications Policy* (2015) 761–770; J. Grimmelmann, 'The virtues of moderation', 17(42) *Yale Journal of Law and Technology* (2015); S. Humphreys, 'Predicting, securing and shaping the future: Mechanisms of governance in online social environments', 9(3) *International Journal of Media & Cultural Politics* (2013) 247–258; R. MacKinnon, E. Hickok, A. Bar, H. Lim, *Fostering freedom online: The roles, challenges and obstacles of Internet intermediaries* (United Nations Educational, New York, 2014); J. A. Obar and S. Wildman, 'Social media definition and the governance challenge: An introduction to the special issue', 39(9) *Telecommunications Policy* (2015) 745–750; J. Reagle, *Reading the comments: Likers, haters, and manipulators at the bottom of the web* (MIT Press, Cambridge, MA, 2015); S. T. Roberts, 'Commercial Content Moderation: Digital Laborers' Dirty Work', 12 *Media Studies Publications* (2016); Y. Roth, 'No overly suggestive photos of any kind': Content management and the policing of self in gay digital communities' 8(3) *Communication, Culture & Critique* (2015) 414–432; L. Stein, 'Policy and participation on social media: The cases of YouTube, Facebook, and Wikipedia', 6(3) *Communication, Culture & Critique* (2013) 353–371; B. Wagner, 'Governing Internet expression: How public and private regulation shape expression governance' 10(4) *Journal of Information Technology & Politics* (2013) 389–403; J. van Dijck, *The culture of connectivity: A critical history of social media* (Oxford University Press, Oxford, 2013).

 DOI: 10.17103/sybil.25.8

distinction announced above: democratic States and authoritarian States have adopted very different approaches to platform governance. In an international legal system where human rights have been interpreted and implemented in very disparate ways, domestic political systems retain a high degree of discretion in deciding how digital platforms will be regulated, with more or less constraints for big tech companies, with more or less freedom for users. Although this is an obvious observation, the 'global' scope or regulatory mechanisms both by public and private actors and authorities is in reality 'regional' (North American, European or Western) or 'domestic' (China, Russia and many other non-democratic countries).

Likewise, and this is a third distinction, the lack of uniform platform governance is also the result of huge disparities between powerful and weak States. Some great powers and regions can regulate the transnational operations of big tech companies because of their leverage in front of these giant private entities, but the public authorities of lesser States can hardly cope with the complex platform ecosystem and cede larger room of manoeuvre to foreign corporations with the means and expertise to exploit opportunities in peripheral markets. It is easy to understand that public regulation in OECD countries, Russia, China, India and some other great and middle powers has been adopted (or could have been adopted) with less difficulties than in many African, South American or Asian countries. The result, again, is a highly asymmetric and dysfunctional platform governance from an international or global perspective.

(2)Public-private nature of norms

The public-private distinction in platform governance is crucial to understand the nature of normative flows. But such attempt is somehow blurred by some empirical paradoxes: public authorities are not the sole regulators of public spaces and issues of public interest online; private actors and authorities often regulate interactions in the public domain of virtual communities; in many occasions, public norms fail to properly serve the public interest; and self-regulation by private companies organize the public sphere where the interests of platform users lie.

Who determines the public interest in digital platforms? Actually, what is the public interest of virtual communities on the internet? Our initial assumptions about the existence of a global public domain in cyberspace and the need to protect the global public interest of internet users are confronted to the reality of normative flows inconsistently nourished by both domestic public actors (States) and transnational/global private actors (digital platforms). The dysfunctionality of States to properly regulate the global public interest lies to a large extent on the basic distinctions considered in the previous section about normative actors. Differing domestic approaches to regulation are now obvious in the light of three ideal types. First, the more liberal stance of United States public authorities and Silicon Valley's companies, reluctant to State intervention, which was crucial for the emergence and expanse of big tech companies and digital platforms. Second, the more conservative approach of European countries and the EU, where public authorities tend to rely on regulation to ensure the protection of public interests; the democratic pillars of these States tend to limit the intrusion of public policies to areas of data protection, privacy, user's rights, etc. Thirdly, there is the radical interventionist stance of authoritarian governments, where the notion of public interest is discretionary defined and both internet users and digital platforms obey public authorities in a more

 DOI: 10.17103/sybil.25.8

controlled and restricted version of the internet.[28]

These three models offer some insights about the diverse normative courses taken by platform governance in different regions of the world. But beyond these differences, recent trends are unequivocal in pointing at growing state intervention and regulation. Freedom House's annual reports illustrate a continuous decline in global internet freedom and increased governmental restraints on free expression, being China the most radical case of abusive State intervention to curtail human rights and freedom on the Net. However, these observations coexist with other relevant remarks in relation to the spread of misinformation favoured (or at least tolerated) by digital platforms, as well as systematic abuses of users' and consumers' rights by corporate and market practices.[29] Wherever they can, big tech companies adopt and implement normative tools aimed at expand their profits through data harvesting at the expense of data protection, privacy, consumer rights, non-discrimination, truthfulness of information, etc. Private normative courses make their way in transnational and global environments whenever States fail to protect the public interest. Thus, hybrid normative flows shape the behaviour of users, sometimes with prevailing public regulation, and often with prevailing self-regulation mechanisms and private regulation of virtual communities.

There is a growing awareness about the dark side of the internet -the 'Net delusion', as Mozorov calls it,[30] and concerns about the authoritarian drift in cyberspace seem well founded. Their origin is not only the expanding cyber capabilities of authoritarian non-Western powers like China and Russia —digital authoritarianism, as some call it—,[31] but the vulnerability of democratic systems vis-à-vis misinformation campaigns eroding basic political institutions and consensus.[32] Such harmful use of information and digital platforms is exacerbated, promoted, facilitated or allowed by software code, algorithms, artificial intelligence and machine learning algorithms embedded in digital platforms; they can all be used according to, and depending on, the norms created and implemented by these companies, which effectively shape the behaviour of their users.[33] The Capitol attack in January 2021 illustrate how far some dangers can go when the use and abuse of ICTs is unrestrained by public authorities.[34]

This is one of the reasons why both the European Union and the United States under the Joe Biden Administration are exploring their own paths to curtail some privileges and practices of big tech

---

[28] These three models are partially inspired by K. O'Hara and W. Hall, 'Four Internets. The Geopolitics of Digital Governance', 206 *CIGI Papers* (2018), although O'Hara and Hall distinguish up to five models: Silicon Valley's Open Internet, Brussels' Bourgeois Internet, Beijing's Authoritarian Internet, DC's Commercial Internet, and Moscow's Spoiler Model. A similar argument about the fragmentation of cyberspace is defended with the concept of 'Splinternet' in S. Malcomson, *Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web* (OR Books, New York/London, 2016). And the 'Balcanization' of the internet is a similar idea suggested by C. Sunstein, *#Republic: Divided democracy in the age of social media* (Princeton University Press, Princeton, NJ, 2017).

[29] *Freedom on the Net 2021. The Global Drive to Control Big Tech* (Freedom House, Washington, DC, 2021).

[30] E. Mozorov, *The Net Delusion. The Dark Side of Internet Freedom* (Public Affairs, New York, 2011).

[31] J. Sherman, 'Digital Authoritarianism and Implications for US National Security', 6(1) *The Cyber Defense Review* (2021) 107–118.

[32] B. R. Allenby, 'The Age of Weaponized Narrative, or, Where Have Your Gone, Walter Cronkite?', 33(4) *Issues in Science and Technology* (2017). Allenby defines 'weaponized narrative' as "the use of information and communication technologies, services, and tools to create and spread stories intended to subvert and undermine an adversary's institutions, identity, and civilization, and it operates by sowing and exacerbating complexity, confusion, and political and social schisms".

[33] A critical view on the harmful role played by tech companies in society and politics in the United States is deployed unambiguously in J. P. Steyer (ed), *Which side of history? How technology is reshaping democracy and our lives* (Common Sense Media, San Francisco, 2020).

[34] K. Hao, 'How Facebook got addicted to spreading misinformation', MIT Technological Review (2021).

 DOI: 10.17103/sybil.25.8

companies and digital platforms. In the case of the European Union, after the General Data Protection Regulation (DGPR) of 1996, new legislative efforts are under way to regulate big tech practices through the Digital Markets Act, and to create a safer digital space through the Digital Services Act, two pieces of legislation expected to change the digital landscape.[35] In the case of the United States, the turn in public policy seems clear: in March 2021 Tim Wu, a champion of antitrust policies in the digital economy, was appointed as special assistant to the President for technology and competition policy in March 2021; the President's chief science advisor, Eric Lander, started to work in an 'AI bill of rights' by November 2021; and the reform of Section 230 of the Communications Decency Act is in sight of the Administration -this law protects online platforms ('interactive computed services') from liability for information and content posted by their users, and allows them to moderate users' content without being treated as publishers.[36]

(3)Regulatory tools in normative channelling

As previously suggested, normative courses are shaped by both public and private actors and authorities in platform governance. A relevant issue when considering the diversity of normative tools is their legal or non-legal nature, since such distinction will trigger (or not) the legal consequences arising from their enforcement. As Pauwelyn, Wessel and Wouters have stressed, there is a universe of norms larger than the universe of law, and in such universe of normativity is where international and domestic normative flows are nourished and mixed.[37]

On the one hand, following policy strategies for the digital environment, States issue legislation, regulation, rules, and also join international legal initiatives in the form of international treaties, customary law, general principles of law, resolutions of international organizations, judgements by international courts, etc. This is the kind of traditional approach that public authorities used to guide the behaviour of citizens, companies, organizations of all sorts, as well as public administration itself. In recent years, the number of such public regulatory mechanisms seems to have significantly increased to govern the internet. Most of these instruments are *legal* norms, and a plethora of soft law mechanism without binding character, although States have also resorted to other norms in the form of standards, guidelines, declarations, codes of conduct, etc.

On the other hand, following profit maximization strategies, big tech companies and digital platforms guide their users' and consumers' behaviour through all sorts of contracts, conditions of use, terms of service, declarations of compliance, privacy policies, data policies and all kinds of standards and guidelines, community rules, codes of conduct, codes of practice, etc. All these regulatory mechanisms and self-regulation have no legal effects themselves, but in the absence of public legal norms, private regulation may attain equivalent effects in terms of actual shaping of users' behaviour.

These two normative flows coexist and mix in both cooperative and conflicting ways in numerous countries where digital platforms conduct their activities. They share the grey area or normativity

[35] 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, and Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.

[36] Section 230 of the Communications Decency Act (1996).

[37] J. Pauwelyn, R. A. Wessel, and J. Wouters (eds), Informal International Lawmaking (Oxford University Press, Oxford, 2012), at 6.

 DOI: 10.17103/sybil.25.8

between the channels of legal and non-legal norms for two reasons. First, because the turn to informality in international law-making has entailed the proliferation of soft-law and informal (legal) norms adopted by states as convenient tools with a view to effective compliance without the burden of other binding and formal instruments.[38] Second, because hybrid and multistakeholder initiatives have gathered public and private actors around shared normative efforts, such as the Safer Social Networking Principles (2009), the Dynamic Coalition on Platform Responsibility (2014), the EU Code of Conduct on Terror and Hate Content (2017), the EU Code of Practice on Disinformation (2018) or the Christchurch Call (2019); these are examples of what R. Gorwa calls 'co-governance' in the 'platform governance triangle'.[39]

But the normative flows also share the little-known area of normative enforcement, where public efforts coexist with platforms compliance operations. Some remarkable research efforts illuminate the relative weight of public and private authorities in specific enforcement and compliance activities like platform content removal and takedowns in the European context. But public understanding of these operations remains limited, and more easily accessible information is needed to properly assess them.[40]

(D) CONCLUDING REMARKS

The restrictions imposed by Facebook on Donald Trump's accounts on 6 January 2021, when he still was President of the United States, represent a powerful illustration of the normative weight and power of digital platforms. To put it clear: A private corporation denied the exercise of freedom of expression to the highest public authority of the most powerful country of the world. We must have missed something when such a decision affecting the public interest of societies is left in the hands of private individuals and organizations. Mark Zuckerberg admitted in September 2019: "We are responsible for enforcing our policies every day and we make millions of content decisions every week. But ultimately I don't believe private companies like ours should be making so many important decisions about speech on our own."[41]

Digital platforms should act consistently with the beliefs of their CEO, but before that, they should cease to disturb and distort the global public domain and leave the defense of the global public interest to more legitimate actors and authorities. Civil society organizations continue to be the weak stakeholders in platform governance, and together with (democratic) governments and other public actors and authorities, they could substantially enhance the legitimacy of policies and norms in cyberspace. Big techs continue to be key normative players, but many have demonstrated their inability and failure to properly serve the public interest. Their normative role may be substantially reduced in the near future, at least in the United States and the European Union.

---

[38] J. Pauwelyn, R. A. Wessel and J. Wouters, 'When Structures Become Shackles: Stagnation and Dynamics in International Lawmaking', 25(3) *European Journal of International Law* (2014) 733-763.

[39] R. Gorwa, 'The platform governance triangle: conceptualising the informal regulation of online content', 8(2) *Internet Policy Review* (2019), doi: 10.14763/2019.2.1407.

[40] D. Keller and P. Leerssen, 'Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation', in N. Persily and J. A. Tucker (eds), *Social Media and Democracy. The State of the Field and Prospects for Reform* (Cambridge University Press, Cambridge, 2020) 220-251.

[41] 'Facebook unveils charter for its 'Supreme Court,' where users can go to contest the company's decisions', *Washington Post* (17/09/2019).