Revista **Direito e Praxis**

Amplified voices, limited change? Rethinking the complex relationship between Democracy, Regulation, and the Internet

Vozes amplificadas, mudanças limitadas? Repensando a complexa relação entre Democracia, Regulação e Internet

Lucas Sena[1]

[1]University of São Paulo (USP), São Paulo, São Paulo, Brazil. E-mail: lucas.sena@alumni.usp.br. ORCID: https://orcid.org/0000-0002-1444-1347.

Guilherme Otaviano Soares[2]

[2]University at Albany, Albany, New York, United States. E-mail: gotavianosoares@albany.edu. ORCID: https://orcid.org/0009-0001-5313-9466.

Abstract

This study's central question is: how does the internet impact political participation and democracy? The internet has reconfigured the dynamics of democracy, enabling more direct dialogue between representatives and civil society. It also imposes new challenges, particularly regarding the limits of digital platform usage and their increasing appropriation for illicit purposes. Given this scenario, this article analyzes the complex relationship between the internet, regulation, and democracy, emphasizing the role of digital platforms in political participation and the emerging regulatory challenges. For this purpose, besides the introduction and concluding remarks, this study also has five sections: the first contextualizes the intersection of democracy, participation, and the internet; the second addresses the phenomenon of cyberactivism and digital social movements, analyzing their potentialities and limitations; the third delves deeper into themes such as control, access to information, and the participatory pathways enabled by digital media; the fourth discusses aspects of internet regulation and governance, with a comparison between the European Union's General Data Protection Regulation (GDPR) and Brazil's proposed Fake News Bill (PL 2630/2020); and the fifth examines empirical challenges to digital democracy by analyzing concrete cases of online manipulation and disinformation and discussing the urgent need for more robust regulatory responses. The concluding remarks point to a scenario of increasing tension between state regulation and the resistance of digital platforms to complying with judicial orders, highlighting a new chapter in this complex relationship and prompting reflections on the future of democracy in the digital age.

Keywords: Internet; Democracy; Regulation; Digital Platforms; Political Participation.

Resumo

A questão que norteia este estudo é: como a internet impacta a participação política e a democracia? A internet reconfigurou a dinâmica da democracia, pois possibilitou um diálogo mais direto entre representantes e a sociedade civil, mas também impôs novos desafios, especialmente em relação aos limites do uso das plataformas digitais. Diante desse cenário, este artigo analisa a complexa relação entre internet, regulação e democracia, com ênfase no papel das plataformas digitais na participação política e nos desafios regulatórios emergentes. Além da introdução e das considerações finais, este estudo apresenta cinco seções de desenvolvimento: a primeira contextualiza a

intersecção entre democracia, participação e internet; a segunda aborda o fenômeno do ciberativismo e dos movimentos sociais digitais, suas potencialidades e limitações; a terceira aprofunda a análise em temas como controle, acesso à informação e os caminhos participativos propiciados pelas mídias digitais; a quarta discute aspectos da regulação e da governança na internet, com uma comparação entre o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia e o Projeto de Lei das *Fake News* (PL 2630/2020) em tramitação no Brasil; e a quinta examina desafios empíricos à democracia digital, analisando casos concretos de manipulação e desinformação online e discutindo a premência de respostas regulatórias mais robustas. As considerações finais apontam para um cenário de crescente tensão entre a regulação estatal e a resistência das plataformas digitais em se submeterem a ordens judiciais, o que evidencia um novo cenário nessa complexa relação e suscita reflexões sobre o futuro da democracia na era digital.

Palavras-chave: Internet; Democracia; Regulação; Plataformas Digitais; Participação Política.

1. Introduction

Democracy, at its core, enables individuals to participate in decisions that shape the collective future actively. Over time, however, the concepts of democracy and participation have evolved, moving beyond the traditional view that confined participation merely to the act of voting. Today, democratic participation is expanding through the internet, which facilitates interaction among citizens, businesses, institutions, and governments, thereby overcoming temporal and spatial barriers. From the perspective of "digital democracy," the internet is increasingly seen as an alternative public sphere where networked communication allows for the formation of decentralized public opinion—a feature Habermas (1996) identifies as crucial for democratic legitimacy.

Consequently, the internet fosters a more profound democratic experience, as opinions expressed in the digital realm cultivate a sense of knowledge emancipation (Faria, 2010). The network not only diminishes hierarchical control over information but also provides access to a variety of alternative content platforms, promoting a greater equilibrium in the informational flow (Farranha, 2016; Castells, 2017). Similarly, the internet's decentralized structure encourages a broader plurality of information, though not always in ways that are exclusively beneficial for democracy. According to Tufekci (2017), this plurality is evident in networked protests, where the digital environment facilitates the swift and widespread mobilization of individuals around common causes, even as such movements grapple with long-term challenges stemming from a lack of formal organizational structures.

"Networked power" (Castells, 2017) offers a lens through which to understand how decentralized communication can both bolster democracy and, conversely, widen social and political fragmentation when platforms for debate become polarized. Digital social networks provide a new infrastructure for participatory democracy, while also giving rise to "connective actions" wherein coordination can unfold with less hierarchy, guided by a logic of flexible individual and collective endeavors (Loader & Mercea, 2011).

The proliferation of news sites, data platforms, social media, and other digital avenues enhances an individual's ability to bypass traditional systems of information control. Moreover, the digital environment has emerged as a vital arena for social mobilization, concurrently enabling research not only into political participation but also into governance and regulation. Contemporary movements, often characterized by

hashtags and digital petitions, have become prominent new forms of expressing support for or opposition to political issues, agendas, and actors. This highlights how mobilization is, in part, driven by the engagement of actors within the virtual sphere. These new dynamics align with Olson's (1965) "theory of collective action," which posits that both material and non-material incentives shape political engagement—a phenomenon potentially amplified by connectivity within social networks.

In this context, the present study aims to investigate digital democracy as a tool in constant dialogue with political participation. This evolving form of participation reshapes communication, which is now digitized and networked (Faria, 2012). The central question guiding this research is: How does the internet impact political participation and democracy? This inquiry stems from escalating debates surrounding access to information and the boundaries of participation on digital platforms, issues intertwined with themes of accountability, governance, and regulation. This study does not endeavor to propose regulatory directives for these networks. Instead, it seeks to explore, drawing on specialized literature, the ongoing debate concerning political participation, democracy, and internet regulation.

This paper commences with this introduction, which forms the first part of its overall structure. Subsequently, the article's development is organized into five sections: the first contextualizes the intersection of democracy, participation, and the internet; the second delves into the phenomenon of cyberactivism and digital social movements, analyzing their potential and limitations; the third section offers a deeper analysis of themes such as control, access to information, and the participatory pathways afforded by digital media; the fourth part discusses aspects of internet regulation and governance, featuring a subsection dedicated to a comparative analysis of the European Union's General Data Protection Regulation (GDPR) (EU 2016/679) and Brazil's Fake News Bill (PL 2630/2020), currently progressing through the National Congress; and the fifth development section further explores the urgency of regulation in light of empirical challenges to digital democracy, by examining emblematic cases of online manipulation and disinformation in Brazil and from an international perspective, alongside legal responses and the imperative for a more robust regulatory framework for the digital sphere. The article concludes with final remarks that highlight a potential escalation in tensions between state regulation and the reluctance of digital platforms to consistently adhere to judicial orders in their countries of operation, signaling a new phase in this

intricate relationship. Finally, the methodology employed is qualitative, articulated through the interrelation of concepts and theoretical approaches germane to the central themes under analysis. Furthermore, to illustrate and enrich the discussion on contemporary challenges and institutional responses, this study incorporates an analysis of emblematic cases and pertinent normative documents, such as those examined in the fourth and fifth sections.

2. Democracy, Internet, and Participation

Popular sovereignty is frequently understood as a foundational concept for understanding democracy. According to part of the literature, majority rule constitutes a central democratic principle as it underpins representation. However, liberal democracy often curtails civil society's involvement to the mere act of voting, a characteristic of a representative model that limits popular participation primarily to governmental transitions.

Conversely, with the informational revolution, the internet has solidified its role as a crucial tool for bringing public visibility to various demands (Castells, 2017). Political participation has intensified within the digital environment, with new means of engagement gaining traction, especially over the last two decades. Concepts such as electronic democracy, cyberdemocracy, digital democracy, and e-democracy have emerged to define popular participation via the internet. Broadly, these terms highlight the new democratic opportunities afforded by the technological infrastructure of computer networks (Gomes, 2005).

Wilson Gomes (2005) identified three fundamental assumptions for digital democracy. The first pertains to the internet's capacity to address participation problems in liberal representative democracies by offering an easy, agile, and convenient channel for engagement. The second assumption suggests that the internet obviates the need for intermediaries between the civil and political spheres, thereby fostering a more continuous flow of information. The third assumption views the internet as a space where civil society not only consumes but also produces political information, thus breaking from the traditional logic of passive content consumption (Gomes, 2005).

The expansion of democracy into the online environment represents a conceptual broadening. Lusoli (2013) highlights the term e-democracy as a way to integrate digital and interactive media into democratic practice. This concept acknowledges the importance and centrality of digital technologies (Coleman & Blumer, 2009; Faria, 2012).

These concepts have gained prominence in recent cases, such as the #BlackLivesMatter movement, which leveraged social networks to organize protests and influence legislative changes in the United States, and the "Arab Spring," where digital platforms enabled popular mobilization and the sharing of information beyond state control. Such examples illustrate how digital democracy can forge new pathways for political participation, allowing citizens to organize, share information, and exert pressure on governments, even in contexts of severe repression or censorship (Howard & Hussain, 2013). Furthermore, Fuchs (2014) argues that the role of social media in the public sphere should be critically understood, considering its potential to colonize the social sphere and the importance of governance mechanisms that ensure the autonomy of public participation amidst the economic and political interests of large platforms.

Around the world, other examples can be found, and a striking one demonstrating the democratic potential of the internet and Information and Communication Technologies (ICTs) in the constituent process was Iceland's collaborative construction of its new constitution, initiated in 2011. Following the 2008 financial crisis, the Icelandic populace demanded a constitution that was more representative and aligned with their needs and culture. In response, the government established a Constitutional Council composed of 25 citizens from diverse backgrounds and, for the first time, enabled direct public participation through social networks and digital platforms like Facebook and Twitter. This process, known as the "Crowdsourcing Constitution," allowed any citizen with internet access to contribute suggestions and opinions, exemplifying the use of ICTs to promote broader inclusion and strengthen the relationship between the people and the constitutional text. The Icelandic experience demonstrates how mass collaboration can transform constitutionalism, fostering an "open society of interpreters" and reinforcing the citizen's role as a protagonist in the democratic process (Marinho, Cançado, & Iwamoto, 2021).

Digital democracy can thus be categorized into five degrees. The first two are elementary, representing a flow of communication from the government to the citizen, intended to gather feedback from civil society. The first degree concerns access to public

services and administrative efficiency, while the second relates to popular consultation to shape the public agenda. The third degree emphasizes state transparency, with the government providing information to society but without directly depending on public opinion for decision-making (Gomes, 2005). The fourth degree approaches deliberative democracy, combining representative and participatory models, whereas the fifth degree is characterized by direct democracy, in which civil society directly controls and validates political decisions.

These varying levels of digital democratic engagement, which range from government-led information sharing and consultation to direct citizen control over political decisions, reflect the institutional and social theoretical strands of digital democracy. The institutional perspective scrutinizes the relationship between the political system and the citizenry, aiming to observe how the state fosters opportunities for interface between democratic interests and established institutions. The social perspective, conversely, centers on civic engagement and online political deliberation (Gomes, 2007). Nevertheless, these frameworks do not entirely encompass the multifaceted complexity of this topic.

Also, Peter Dahlgren (2005) identifies three fields of democracy via the internet: the liberal-individualist, the communitarian, and the deliberative. The first emphasizes individual autonomy to express preferences and act politically; the second values common bonds and a sense of belonging; and the third concentrates on citizen participation in shaping public opinion and political decisions. The deliberative model attempts to reconcile popular sovereignty with the rule of law, aiming to use consensus as a mechanism for legitimacy (Habermas, 1987). Finally, the participationist current of digital democracy seeks to increase direct political participation by citizens through the internet, with the purpose of promoting greater effectiveness in political decisions (Almeida, 2016).

2.1. Cyberactivism and Digital Social Movements

Cyberactivism and digital social movements have increasingly played a central role in contemporary politics, establishing new forms of citizen participation and mobilization. With the advancement of information and communication technologies, political activism has expanded into the online environment, enabling individuals and

groups to organize awareness campaigns, coordinate demonstrations, and influence public debates in unprecedented ways. The concept of cyberactivism refers to the use of the internet as a tool for collective action and political activism, characterized by the creation of support networks, information dissemination, and engagement in the struggle for social rights (Castells, 2012; Shirky, 2008).

According to Manuel Castells (2012) in his work *Networks of Outrage and Hope*, the internet has transformed the dynamics of social movements by offering a horizontal communication space that allows for decentralized, real-time organization and information sharing. This organizational model is fundamental to digital social movements like #BlackLivesMatter and #MeToo, which emerged in response to social injustices and rapidly became global mobilization phenomena. These movements are notable not only for denouncing systemic problems such as racism and gender violence but also for their capacity to sensitize public opinion and influence public policies by creating a "digital public sphere" where ideas and demands can gain visibility and support.

The #BlackLivesMatter movement, for example, originated in the United States in 2013 following the acquittal of George Zimmerman in the killing of Trayvon Martin, an unarmed Black youth. Created by three Black activists (Alicia Garza, Patrisse Cullors, and Opal Tometi), the movement used the hashtag #BlackLivesMatter to amplify denunciations of police violence and systemic racism against the Black population. This movement grew rapidly, gaining support and organizing protests in various American cities and around the world. The internet was essential for organizing these actions, allowing the movement's messages to spread beyond national borders and transform into an international civil rights campaign. The digital campaign also pressured local governments and organizations to adopt public safety reforms, demonstrating the effectiveness of cyberactivism in prompting changes in offline politics (Jackson, Bailey, & Welles, 2020).

Another significant example is the #MeToo movement, which gained momentum in 2017 after public allegations of sexual abuse and harassment involving influential figures in the entertainment industry. The movement was propelled by posts from women who shared their personal stories with the hashtag #MeToo, exposing the extent and severity of sexual harassment in workplaces. The global reach and visibility generated by the movement not only fostered cultural shifts but also contributed to the creation of

policies for preventing and combating harassment in various organizations and governments.

The efficacy of digital social movements can also be analyzed from the perspective of collective action theories. Mancur Olson (1965) argues that the mobilization of groups around common interests faces the "free-rider" problem—individuals who benefit from collective efforts without actively contributing. Digital movements, however, confront this challenge differently; social networks allow anyone to engage minimally by sharing content, thereby broadening the reach of messages and lowering participation barriers. Indeed, the digital environment can boost collective action by providing new means of coordination and message amplification, although this virtual mobilization also presents organizational and sustainability challenges (Tufekci, 2017).

In this regard, Veronese and Capela (2017) draw attention to the complex relationship between digital tools and the strengthening of democracy in the Brazilian public sphere. The authors question the effectiveness of "slacktivism," also known as armchair activism, which refers to activist practices demanding little concrete engagement and typically occurring online. Veronese and Capela (2017) explain that while platforms like AVAAZ, which promotes global digital activism, and Change.org - one of the largest active virtual petition platforms - exist, a duality must be observed. While they attempt to democratize access to political participation via the internet, thereby allowing citizens to express themselves and opine, especially through the collective signing of digital petitions, there is a risk of individualizing political action. This dynamic, present in armchair activism, by facilitating superficial adherence to causes detached from concrete and in-person collective engagement, could, in the authors' view, actually weaken the building of ties and the articulation of robust social movements, which are crucial for achieving lasting political transformations and demands connected to social reality (Veronese & Capela, 2017).

In this sense, although digital social movements have demonstrated efficacy in mobilizing public attention to social justice issues and influencing the political agenda, they face considerable challenges and limitations. The ephemeral nature of social media, marked by the rapid obsolescence of content and the constant renewal of topics, can hinder the continuity of advocated causes. Vulnerability to disinformation campaigns and informational manipulation represents another obstacle, destabilizing credibility and confusing the movements' messages. Furthermore, the decentralized nature of

cyberactivism, which favors spontaneous adherence and a diversity of voices, can complicate the formulation of cohesive demands and the construction of sustainable long-term political strategies. Despite these limitations, the importance of cyberactivism for democratizing public space and strengthening social causes is undeniable. Digital technologies emerge as powerful catalysts for social transformation, capable of broadening the reach of demands and creating new forms of civic engagement and participation.

3. Control, Access to Information, and the Participatory Pathway of Social Media

Discussions about access to information and social participation directly relate to accountability, which, in its vertical form, involves mechanisms for oversight and sanction of elected representatives, as well as their responsiveness to the electorate (Teixeira, Sena, & Silva, 2024). Digital media, particularly social networks, have created new opportunities for horizontal accountability, through which ordinary citizens can monitor and pressure public authorities and corporations in a more dynamic and accessible manner, thereby challenging the hegemony of traditional media (Loader & Mercea, 2011). In a democratic context, the concept of accountability intertwines with the control exercised by civil society in participatory institutions, where representatives are agents who must account for their actions and mandates (Almeida, 2016; Mainwaring, 2003).

The traditional concept of accountability unfolds into two components: answerability (the obligation to explain or justify actions) and enforcement (the assurance of sanctions in cases of improper conduct) (Schedler, 1999). Peruzzotti and Smulovitz (2002) broaden this discussion by introducing social accountability, a control mechanism that extends beyond the electoral cycle, aiming to allow associations, social movements, and civil society in general to continuously scrutinize political authorities, without solely depending on the vote to hold them responsible.

Current digital media are transforming these conceptions, as social network platforms enable constant observation of political agents, allowing the public to actively participate in discussions previously confined to formal institutional settings. The internet and social media act as catalysts for a form of accountability that permits real-time information dissemination while simultaneously creating a space for public debate and

civic engagement. However, the fragility of networked movements, often lacking leadership and strategic planning, can compromise their long-term effectiveness (Tufekci, 2017).

In recent years, the internet has become an essential platform for exercising accountability, a domain previously restricted to traditional media such as radio, television, and newspapers. The growing availability of online information provides new forms of transparency and more dynamic control over public acts (Farranha & Santos, 2016). In this scenario, online participation is characterized by its active and continuous nature, with mobilizations like hashtags demonstrating the capacity for rapid, global articulation and expression of public demands (Castells, 2001; 2017).

Social media foster a "dialogic accountability," in which the dialogue between representatives and public opinion intensifies (Almeida, 2016). Platforms such as Facebook, X (formerly Twitter), WhatsApp, and the recent BlueSky allow for the swift and effective mobilization of ideas, interests, and people, something unprecedented compared to traditional forms of activism (Almeida, 2016; Baccarin, 2019, 2023; Farranha, 2012, 2016). On this topic, Bennett and Segerberg (2013) discuss the emergence of connective action, a form of collective action organized via the internet, exemplified by the *Los Indignados* and *Occupy Wall Street* movements. In Brazil, the 2013 demonstrations also serve as an example, as they showed how social networks can be channels for amplifying mobilizations and, consequently, significantly impacting public debate and political and regulatory actions.

Another example, this time from August 2024, concerns the suspension of the X platform and its consequences for both political participation and the debates arising from this discussion. Although X was not the first virtual environment to be blocked by the Brazilian judiciary[1], the case is emblematic because the decision came from the Supreme Federal Court in response to non-compliance with judicial orders and represented an escalation of tension between the platform and the Brazilian Supreme Court. The orders requested the appointment of a legal representative in the country, demanded the removal of profiles promoting hate speech, fake news, and actions against the democratic rule of law in Brazil, and imposed fines. The platform resisted the orders and, in response, went as far as withdrawing its representation from Brazilian territory

---

[1] Since 2007, there have been instances of digital platform suspensions by the Brazilian judiciary, such as WhatsApp, which was blocked between 2015 and 2016 (Falegatti, 2024).

and refusing to pay the fines. The imbroglio lasted from August to October 2024 and was only resolved when the platform complied with the determinations of the Brazilian justice system[2].

Succinctly, the decision demonstrates two central aspects: the need for more effective regulation of the virtual environment and the complex, challenging debate about the limits of online participation. Regarding these aspects, the position that has been strengthening is that digital platforms cannot be used for committing crimes. In a speech upon taking office as president of the Superior Electoral Court (TSE) in 2022, Justice Alexandre de Moraes declared that "(...) freedom of expression is not freedom to destroy democracy, to destroy institutions, to destroy the dignity and honor of others." (Migalhas, 2022). Therefore, a challenge arises in ensuring that political participation via the internet does not merely represent a desire to attack legal rights and the institutions that structure democracy. Despite advances, the blocking of platforms, though controversial, also brings to the fore the debate on the responsibility of technology companies and the limits of freedom of expression, making it important to question the extent to which such actions limit or guarantee the protection of political participation in a democratic context.

This context makes evident the need for effective regulation that not only restricts the dissemination of harmful content but also encourages more informed and responsible political participation in the virtual environment (Carvalho, 2020). Despite its potential, there is another debate regarding the limitations of digital media in fostering inclusive political discussions. According to Almeida (2016), although digital tools facilitate mobilization and reduce costs, they tend to attract individuals who are already politically active, and anonymity can hinder the deepening of discussions. Thus, even if the internet expands access to information, it does not necessarily alter the dynamics of collective action nor promote more robust interaction between representatives and the represented (Almeida, 2016), and it may also create obstacles stemming from the existing reluctance in public debate concerning the limits of freedom of expression.

The deterioration of the public sphere on social media is aggravated by the proliferation of fake news and extremist discourses, driven by an economic model that incentivizes viral and controversial content, thereby contributing to polarization and

---

[2] The blocking of the X platform was ordered on September 30, 2024, by Brazilian Supreme Court Justice Alexandre de Moraes, after the platform itself announced its non-compliance with the Court's orders (Agência Brasil, 2024).

harming democratic communication (Carvalho, 2020). This decentralization, while broadening access to information, results in a lack of accountability in the verification and dissemination of shared information.

The Access to Information Law (Law No. 12,527/2011), the Marco Civil da Internet (Internet Civil Framework - Law No. 12,965/2014), and the General Personal Data Protection Law (LGPD - Law No. 13,709/2018) are important milestones in the Brazilian context, as they seek to expand transparency, privacy, freedom, and regulate internet use. These legislative instruments represent attempts to formalize the rights and duties of users and companies but still face challenges in practical application, especially concerning the implementation of effective measures against the spread of false information and the responsible use of personal data (Oliveira, 2013). The LAI guarantees the right to access public information; the MCI establishes principles, guarantees, rights, and duties for internet use; and the LGPD encourages discussions on privacy and freedom in the virtual environment. Although there have been advances, as Lemos (2019) points out, civil society participation in the internet regulation process in Brazil is still limited, with greater prominence given to the government and the technical community, as observed in the Marco Civil debate. Currently, the focus has primarily been on the companies that create and manage the main online participation tools.

These challenges highlight the complexity of controlling the digital environment, which, despite offering new possibilities, still faces regulatory hurdles that are constantly renewed and become more intricate.

4. Regulation, Internet, and Governance

Lawrence Lessig (2006) introduces the concept of "regulation by code," a distinct form of internet regulation where the legal architecture of cyberspace interacts with both government and market forces. Lessig differentiates the internet from cyberspace, positing that the internet primarily serves as a tool for everyday transactions like payments and news access. In contrast, cyberspace comprises interactive communities that reshape social interaction. Consequently, digital media enable individuals from diverse locales to establish online groups and networks with self-regulatory capacities. This, Lessig (2006) argues, opens up new arenas for action by both governmental control

mechanisms and the communities themselves. These digital communities are emerging as platforms for asserting democratic rights and values, underscoring a scenario where technology helps articulate demands for social justice and inclusion, thereby broadening avenues for networked public deliberation and participation (Silva & Paiva, 2013).

Self-regulation is a testament to the flexibility of cyberspace, where groups can spontaneously form networked communities via social media, capable of instituting their own norms for conduct and interaction. Lessig (2006, p. 88) contends that "codes constitute cyberspaces; these spaces enable or disable individuals and groups." This is reflected in the internal dynamics of these communities, which are governed by member-defined rules that can span from discourse standards to internal markets.

As network technologies have proliferated, internet regulation has necessarily extended beyond mere access to information laws. Initially envisioned as conduits for transparency and public data, cyberspace now hosts autonomous and intricate platforms such as Facebook, X, and WhatsApp. While not initially intended for political engagement, these platforms have evolved into crucial hubs for political organization and deliberation across the political spectrum. Faria (2012) notes that this shift, dubbed the "open parliament," has effectively transformed digital platforms into influential channels for shaping laws and public policies. However, the deployment of these tools has also given rise to challenges concerning disinformation and interference in democratic processes, as exemplified by the X platform case. The internet has empowered citizens to transition from passive information consumers to active protagonists in the public sphere, granting them the ability to directly mold social and political narratives through the creation and dissemination of digital content (Fuchs, 2014).

In Brazil, the discourse surrounding digital media regulation has gained significant traction in recent years. This is particularly due to heightened public debate over the limits of free expression and the exploitation of these platforms for criminal activities, actions undermining the democratic state, and the organization of illicit enterprises. The spread of "fake news" and the amplification of hate speech through social networks pose an escalating threat to democratic integrity, exacerbated by economic incentives that favor the dissemination of sensationalist and polarizing content, thereby hampering constructive dialogue and mutual understanding (Carvalho, 2020).

A current empirical illustration is the case of the X platform. As detailed in the preceding section, its operations were suspended in Brazil following its refusal to adhere

to national laws, its role as a conduit for extremist ideologies, and its mobilization of resources to defy Brazilian judicial orders. This incident underscores the emergent regulatory challenges: how to ensure that political participation occurs legitimately and responsibly, preventing virtual spaces from becoming havens for crime, disinformation, or assaults on the democratic order. Intrinsically linked is the question of how, and by what means, decisions to block internet participation can be legitimately made and upheld. It is a stark fact that the absence of robust regulation not only jeopardizes democratic integrity but also cultivates an environment ripe for the propagation of discourses that threaten the rule of law and fundamental democratic interests.

Although digital platforms connect individuals globally, they can also be weaponized to intensify criminal activities, disseminate hostile messages targeting groups, individuals, or organizations, and derail crucial societal agendas. Such impediments can deepen political and social polarization, facilitated by the algorithmic design of these platforms, which often prioritizes user engagement (Tufekci, 2017). In many instances, this contributes to an adverse, potentially hazardous digital milieu conducive to counter-activism (Baccarin, 2023). Moreover, anonymity and the lack of immediate repercussions tend to encourage the proliferation of such harmful discourse, frequently in an environment devoid of effective regulations or boundaries (Carvalho, 2020).

In this sense, emerging technologies invariably impact legislation. Friedman (2001), for instance, suggests that novel technologies like artificial intelligence necessitate new regulatory frameworks. The advent of devices that supplant human labor or sway public opinion, such as bots that propagate false news, raises significant concerns regarding democratic integrity and labor rights.

By functioning as hybrid arenas for interaction and propaganda, social platforms reshape the concept of the public sphere, giving voice to a diverse array of actors. However, they also provide fertile ground for information manipulation and the algorithmic control of social behavior (Tufekci, 2017). Cohen (2012) similarly explores the impact of digital technologies on the formation of "connected citizenship," proposing that these technologies have the potential to alter individual subjectivity and political culture. Information networks fundamentally shape how individuals discover and interpret the world, thereby intensifying processes of mediation and the naturalization of functions previously undertaken by humans.

As the regulatory debate matures, discussions around a new model of democratic governance are also coming to the fore. Internet governance aims to integrate government and society, enhance participation, and establish mechanisms for e-governance (Hofmann et al., 2017). For digital governance to be genuinely democratic, it is imperative that all stakeholders have equitable access to, and control over, the data and algorithms that define online interactions. This requires fostering a digital infrastructure that serves as a public good, capable of withstanding commercial and political pressures (Loader & Mercea, 2011). Consequently, internet governance can manifest participatively, with decentralized collaboration among all actors, or through a "governed network" model, where a lead agent directs the organization (Provan & Kenis, 2013).

Another crucial element is network governance, which presents both opportunities to strengthen and challenges to overcome for democracy (Denhardt, 2011). Effective governability hinges on collaboration among governments, civil society, and the private sector to forge political agendas that uphold democratic legal norms. The core challenge, however, lies in discerning how regulation can effectively underpin internet governance and broaden online participation spaces without succumbing to the perils of illegal, discriminatory, and anti-democratic practices (Patrício, 2017; Hofmann et al., 2017; Epstein et al., 2016).

4.1. A Comparative Analysis of the GDPR and Brazil's Fake News Bill

The digital transformation has introduced new challenges for democratic governance and the protection of rights in the virtual environment, prompting different regions to adopt specific regulations to safeguard their citizens. Two notable examples of such regulations are the European Union's General Data Protection Regulation (GDPR) (EU 2016/679) and Brazil's Fake News Bill (PL 2630/2020), which is currently progressing through the National Congress. While the GDPR primarily focuses on personal data privacy, the Fake News Bill centers on combating disinformation and promoting transparency on social media and messaging platforms.

Table 1. Comparison between GDPR and the Fake News Bill

Criterion	GDPR (EU)	Fake News Bill (Brazil)
Main Objective	Data protection and privacy	Combating disinformation and informational manipulation
Focus	Personal data and individual control	Information, transparency, and accountability
Penalties	Fines up to 4% of annual global revenue	Fines, platform and user liability
Examples of Critiques	Costs for SMEs, extraterritorial application	Risk to freedom of expression, privacy
Global Impact	Inspired privacy regulations globally	May influence policies against disinformation

Source: compiled by the authors.

The GDPR, in effect since 2018, principally aims to protect the privacy and control of personal data for citizens of the European Union (EU). It establishes stringent rules for data collection, storage, and processing, applicable to all organizations operating within the EU or processing data of European citizens, regardless of their location. In contrast, the bill aiming to institute Brazil's Fake News Law seeks to mitigate the spread of disinformation and foster transparency in online content management. Furthermore, it proposes a series of measures to combat fake news, such as mandatory stricter content moderation and the identification of those responsible for widely disseminated information.

While the GDPR prioritizes citizens' rights to privacy and control over their data, the Fake News Bill primarily focuses on combating disinformation and protecting the integrity of public debate, aspects commonly addressed in STF decisions (Migalhas, 2024). The GDPR imposes robust guarantees ensuring that personal data are used with explicit consent and for legitimate purposes, providing for the "right to be forgotten" and the rectification of incorrect information. The Fake News Bill, conversely, promotes transparency in the dissemination of information on networks and aims to inhibit the creation and sharing of false or manipulated content, especially within political and electoral contexts.

Thus, the GDPR requires organizations to clearly explain to users how their data is processed and grants them the right to request the deletion of their information if they do not agree with platform guidelines. Brazil's Fake News Bill, on the other hand, mandates that social media platforms implement mechanisms to identify potentially false

content and inform users about sponsored content. Additionally, it seeks to compel platforms to take responsibility for content moderation and, in doing so, to label potentially manipulative content.

Regarding penalties, the GDPR imposes rigorous fines, which can reach up to 4% of a company's annual global turnover, thereby ensuring an enforcement mechanism that compels platforms to prioritize compliance with the legislation. The Brazilian proposal, still in the approval phase, envisages fines and sanctions for platforms that fail to meet transparency and moderation requirements. The commonality is that both regulations establish financial sanctions and incentives for compliance. However, the GDPR stands out for the global impact of its penalties and the effectiveness of its application, whereas the Brazilian Fake News Bill still faces challenges in terms of regulation and operationalization. Despite resistance from platforms in Brazil—the most notorious example being the statement issued by Google[3] between April and May 2024—the Bill still needs to advance on this topic.

The GDPR is widely respected and serves as a benchmark for privacy legislation in other regions. Nevertheless, it faces criticism related to compliance costs for small and medium-sized enterprises (SMEs) and the complexity of its extraterritorial application. Conversely, as mentioned, the Fake News Bill encounters resistance from sectors concerned about potential restrictions on freedom of expression, the risk of censorship, and the complexity of monitoring content without violating user privacy.

Therefore, the GDPR is a global landmark for privacy regulations and has inspired similar laws in various parts of the world, as well as strengthening the concept of data protection as a fundamental right. The Fake News Bill, although still under development, could establish important precedents for digital content governance in other democracies facing similar problems and could complement the General Personal Data Protection Law (LGPD - Law No. 13,709/2018) to enhance the protection of personal data on digital platforms. Furthermore, by addressing disinformation and promoting transparency, the Bill broadens the debate on digital information governance beyond privacy.

Another shared aspect is the concern of both initiatives to respond to contemporary challenges of the digital environment and to offer distinct approaches for

---

[3] In late April 2024, Google displayed a link on its Brazilian search engine homepage (google.com.br) to a statement expressing its opposition to Brazil's Fake News Bill. The statement was subsequently removed after Brazil's Ministry of Justice intervened. (CNN Brasil, 2024)

protecting citizens' rights. The GDPR has consolidated itself as a global reference in data protection, having established privacy as a fundamental right and promoted rigorous standards that empower individuals over their personal information in the face of large big tech companies. Its influence transcends EU borders, as it has become a model for the spread of privacy legislation in various regions and has reinforced the role of companies in preserving digital privacy.

In contrast, the Fake News Bill, still under discussion in Brazil, addresses the issue of disinformation and the impact of social media on the public sphere. It seeks a balance between freedom of expression and mitigating the negative effects of informational manipulation, assigning specific responsibilities to digital platforms regarding content moderation and transparency. This proposal, though controversial, responds to concerns about the influence of social media on democratic processes and suggests a content governance model adapted to the Brazilian context, albeit one still in need of further legal refinement.

These initiatives highlight the diversity of strategies required to tackle the complex challenges of the digital environment. While the GDPR provides a solid foundation for privacy protection, the Brazilian Bill represents an effort to safeguard informational integrity in the public space. Together, they illustrate that effective digital governance must consider both the protection of personal data and the quality and veracity of information conveyed online.

5. Regulatory Urgency in the Face of Empirical Challenges to Digital Democracy

The discussion of the internet as a sphere for expanding political participation and strengthening democracy, a central theme of this article, cannot dispense with a critical analysis of the risks inherent in its architecture and use. While the digital environment offers unprecedented channels for civic engagement and the formation of a digital public sphere (Habermas, 1996; Fuchs, 2014), it has also become fertile ground for disinformation, the manipulation of public opinion, and coordinated attacks that threaten the stability of democratic institutions. This duality reflects the tension between the emancipatory potential of the network (Faria, 2010) and its appropriation for dynamics of control and social fragmentation (Castells, 2017; Han, 2022). Amidst this complex

arrangement, the need for effective regulatory mechanisms emerges not merely as a technical or legal issue, but as an imperative for safeguarding democracy itself. Emblematic cases, both in Brazil and internationally, help to illustrate existing vulnerabilities and the intricate task of constructing digital governance that balances freedom, responsibility, and the protection of public interest, thereby challenging the notion that platforms' "code" alone would suffice for their regulation (Lessig, 2006).

This understanding is further reinforced by studies such as Persily's (2017), which argues that the contemporary informational ecosystem is structured to reward polarizing and emotionally appealing content, to the detriment of factual and balanced information. This algorithmic logic contributes to the radicalization of political discourse and the fragmentation of the digital public sphere.

In the Brazilian context, investigations and debates surrounding the so-called "Hate Cabinet"[4] have exposed the capacity of organized groups to use digital media and messaging applications to execute systematic disinformation and defamation campaigns against political adversaries (Poder 360, 2023). The dynamics of these actions—characterized by the massive and rapid production of often false or distorted content, and its coordinated dissemination through networks of profiles, including the use of bots to simulate support and artificially amplify the reach of untrue narratives—aimed not only to tarnish individual reputations but also to erode qualified public debate and potentially influence electoral outcomes, as suggested in analyses of the 2018 and 2022 elections (Nobre et al., 2019; Bittencourt & Rosa, 2022). Such phenomena demonstrate how dialogic accountability (Almeida, 2016) can be subverted and how the space for interaction in digital communicative arenas has been transformed in the face of coordinated attack networks.

Consequently, the fallout from these disinformation networks has laid bare the difficulties within the Brazilian legal framework to contend with the speed and scope of such campaigns, as well as to effectively identify and hold accountable all links in the chain of production and distribution of illicit and harmful content. The very decentralized structure of the internet, which theoretically fosters plurality (Castells, 2017), here

---

[4] The expression "Hate Cabinet" (Gabinete do Ódio) refers to an informal structure alleged to have operated in Brazil, primarily during Jair Bolsonaro's administration (2019-2022). This network's objective was reportedly to coordinate the mass production and dissemination of disinformation, false news, and defamatory attacks against political opponents, democratic institutions, and members of the Judiciary through digital media and instant messaging applications. (Poder 360, 2023)

presents itself as a challenge to law enforcement and timely accountability. In response to this increasingly challenging scenario, significant institutional efforts are observable. Noteworthy examples include inquiries conducted within the Supreme Federal Court (STF), such as Inquiry 4781[5], and the continuous action of the Superior Electoral Court (TSE) in issuing resolutions[6] aimed at regulating electoral propaganda and combating disinformation. The complexity of adapting the legal framework to new technologies is also highlighted in studies like the Technical Note "Building Consensuses: Deep Fakes in the 2024 Elections" (Junquilho et al., 2024). This study, by analyzing decisions of the Regional Electoral Courts (TREs) on the use of deepfakes following TSE Resolution No. 23,732/2024, reveals a diversity of interpretations and persistent challenges in classifying and regulating these new forms of manipulation in the electoral context. This aspect illustrates the ongoing efforts to adapt legal and institutional responses to technologies that evolve more rapidly than legislative cycles.

Furthermore, it is pertinent to recall that the Brazilian legal system, through Art. 323 of the Electoral Code (Law No. 4,737/1965), already criminalized the dissemination of knowingly false facts in electoral propaganda. However, its wording was amended by Law 14,192/2021 to include the commission of virtual electoral crimes and crimes against women[7]. However, the dynamics of online disinformation campaigns—often operated by diffuse actors employing tactics that exploit legislative gray areas—and the difficulty in swiftly assigning responsibility underscore the need for constant legislative

---

[5] Inquiry (INQ) 4781, also known as the "Fake News Inquiry," was initiated ex officio by the then-president of the Supreme Federal Court (STF), Justice Dias Toffoli, in March 2019, through Administrative Order GP No. 69/2019. Its stated objective was to investigate "fraudulent news (fake news), slanderous accusations, threats, and other offenses that affected the honorability and security of the Supreme Federal Court, its members, and their families" (Brasil, 2019). INQ 4781 gained notoriety in Brazilian public debate due to its conduct by Justice Alexandre de Moraes, who was designated to lead it by the order itself.

[6] The resolutions of the Superior Electoral Court (TSE) that seek to regulate electoral propaganda and combat disinformation, with a recent focus on technologies such as Artificial Intelligence (AI) and deepfakes, notably include TSE Resolution No. 23,732, of February 27, 2024. This resolution amended TSE Resolution No. 23,610, of December 18, 2019, which provides for electoral propaganda, to incorporate specific rules on the use of AI, the prohibition of deepfakes intended to harm or favor candidacies, and the mandatory labeling of synthetic content in electoral propaganda for elections (Brasil, 2024).

[7] Law No. 14,192, enacted in 2021, established as its central objective the prevention, repression, and combat of political violence against women (Brasil, 2021). To achieve this protective aim, the law amended several legal provisions, including the Electoral Code (Law No. 4,737/1965). In this context, one of the relevant modifications occurred in Art. 323 of said code, which addresses the crime of disseminating, in propaganda or during an electoral campaign, knowingly false facts about parties or candidates that could influence the electorate. Law No. 14,192/2021 updated the wording of this article and, consistent with its scope, added qualifying circumstances that increase the penalty if the crime of electoral disinformation is committed via the internet or social media, or, significantly, if it involves disparagement or discrimination based on a woman's status, color, race, or ethnicity. This amendment aligned the repression of electoral disinformation with the protection of women in politics.

enhancements. In this regard, proposals such as Bill No. 2630/2020 (the Fake News Bill), previously mentioned in this study as an effort to create a specific legal framework, seek to establish more robust mechanisms for platform accountability and combating illicit content, within a debate that reiterates the complex relationship between regulation, freedom of expression, and the limits of state intervention in the digital environment.

Moreover, the use of generative artificial intelligence and natural language models for large-scale disinformation production is emerging as a recent and growing concern. Research, such as that by Weidinger et al. (2021) from the Alan Turing Institute, demonstrates that AI models can be employed both to automate the creation of false narratives and to amplify the reach of manipulation campaigns. Such technical advancements, not yet fully addressed by existing legislation, make the formulation of adaptable, democratically anchored regulatory frameworks urgently necessary.

On the international stage, the Cambridge Analytica scandal[8], which gained global notoriety in 2018, remains a paradigmatic case of electoral manipulation facilitated by the exploitation of personal data on digital platforms. The collection of information from millions of Facebook users, without explicit consent for the purposes for which it was used, enabled the creation of detailed profiles and the targeting of personalized political messages aimed at influencing voter behavior in political processes such as the 2016 U.S. presidential elections and the Brexit referendum (McGaughey, 2018; Hu, 2020). This case highlighted not only citizens' vulnerability to data-driven manipulation but also the disproportionate power of digital platforms to compile and manage user data, and the inadequacy of then-current privacy and political advertising regulations (Henriksen, 2019). The global repercussions of the scandal spurred a movement for greater data protection, culminating in landmarks like the General Data Protection Regulation (GDPR) in the European Union (Raccagni, 2023). The GDPR established new standards for personal data processing and inspired legislation in various countries, including Brazil's General Personal Data Protection Law (LGPD – Law 13,709/2018) (Costa et al., 2022). Nevertheless, even with these advancements, the ability of political and commercial

---

[8] The Cambridge Analytica scandal involved the British political consulting firm of the same name, which improperly obtained and used personal data from tens of millions of Facebook users. The information was employed to build detailed profiles aimed at targeting political advertising and influencing voter behavior in democratic processes (Henriksen, 2019). In her master's thesis, Ellen Emilie Henriksen (2019) points out that this scandal demonstrates how the collection and misuse of personal data for political microtargeting can manipulate individual vulnerabilities, polarize societies, and threaten the governability of liberal democracies. The author highlights the impacts on democratic stability, the data economy, and individual autonomy, in addition to exposing tensions between state and corporate practices in the use of big data.

actors to exploit data for microtargeting, and the opacity of algorithms governing information distribution, continue to be sources of profound concern, still jeopardizing citizens' informational autonomy and the fairness of political competition.

Another relevant example comes from India, where the use of WhatsApp in electoral campaigns has been the subject of numerous allegations of disinformation and hate speech, particularly in the 2019 general elections. The country, with over 400 million active users on the platform, witnessed the massive circulation of false messages, leading to measures such as limiting message forwarding and tracing content origins. However, these measures face criticism regarding privacy and freedom of expression (Arun, 2019).

In this context, a joint analysis of the "Hate Cabinet" case—which highlights disinformation and coordinated attacks for domestic political interference—and the Cambridge Analytica scandal—exposing algorithmic manipulation via data on a transnational scale with implications for informational sovereignty—helps to understand some of the empirical challenges inherent to democracy in the digital age. These examples demonstrate that there is no single or simple solution; rather, building a safer and more democratic digital environment demands a complex regulatory and social strategy, which must rest on several fundamental pillars.

Firstly, the pursuit of greater transparency from platforms themselves regarding their recommendation and content moderation algorithms, as well as their use of data for advertising and political purposes, is essential. Secondly, accountability—a democratic mechanism whereby companies with access to large-scale data can be diligent in mitigating systemic risks such as the spread of disinformation and hate speech—needs to be better defined and applied. In the Brazilian case, this aspect still lacks sufficient legal modulation and regulatory design to help overcome the hesitation frequently observed in discussions like that of PL 2630, and the resistance of platforms themselves to fully submit to national legislation, as seen in the X suspension case. This involves a careful debate about the role of platforms, not as arbiters of truth, but as actors with significant responsibilities for the communicative and civic processes occurring on their services.

Furthermore, continuous and in-depth investment in critical media and digital literacy for the population remains an indispensable tool. It is important to note that this remedy requires concerted actions, whether through more responsive regulation or criteria that can hinder the mass dissemination of false information. Citizens who are more aware of how platforms operate and the tactics of manipulation are better

equipped to exercise their right to information and to participate in democracy more autonomously and attentively, which contributes to a more resilient society.

Finally, given the intrinsically global nature of the internet, international cooperation among regulators, researchers, and civil society organizations is also of paramount importance for developing standards and best practices that can be adapted to local realities, without stifling innovation or imposing disproportionate barriers to freedom of expression. The unwavering defense of human rights in the digital environment must permeate all these initiatives and ensure that the quest for security and informational integrity does not result in excessive surveillance or undue curtailment of freedoms (Kaufman, Junquilho, & Reis, 2023). In this sense, internet regulation is configured less as a final destination and more as an ongoing process of adaptation, negotiation, and democratic construction in the face of challenges posed by a constantly evolving technological environment—a process that demands constant vigilance and a renewed commitment to democratic values so that the voices amplified by the network result in changes that strengthen, rather than limit, democracy.

6. Concluding Remarks

Lawrence Lessig's (2006) concept of "regulation by code" illuminates the interplay between cyberspace's architecture, governmental oversight, and market dynamics, a synergy that empowers online communities to establish their own self-governing norms. While the internet primarily streamlines everyday transactions, cyberspace fundamentally reshapes social interaction, thereby generating regulatory challenges that escalate in complexity in tandem with these evolving digital arenas. Furthermore, the notion of code-based regulation highlights how digital platforms not only mold user behavior but also dictate the parameters of permissible interaction. This underscores the critical need to scrutinize who controls these underlying codes and the vested interests driving their implementation (Fuchs, 2014).

The internet stands as one of the most pivotal instruments for bringing societal issues, and their inherent contradictions, to the forefront. Unsurprisingly, political participation mediated through cyberspace has given rise to concepts such as "digital democracy" and "e-democracy," which underpin new modalities of social engagement.

Such engagement proves particularly potent in movements that confront established political structures, exemplified by Occupy Wall Street and the Arab Spring protests. In these instances, social networks facilitated swift, large-scale mobilizations. Yet, they also exposed the inherent fragility of these networks, which, lacking robust organizational frameworks, often struggle to sustain their long-term agendas (Tufekci, 2017).

Equally compelling is the broadening understanding of accountability, which increasingly turns to the virtual sphere to comprehend evolving forms of control, oversight, and social engagement as digital networks redefine them. The facility afforded by the internet has thus intensified scrutiny through digital media, fostering more active and global participation. This is evidenced by mobilizations like hashtags and connective actions that transcend geographical boundaries and compel legal systems to grapple with transnational discourse. This cross-border dimension of digital flows lends credence to Balkin's (2018) assertion that platform regulation must function as a novel form of constitutional governance, guided not only by national statutes but also by public norms anchored in democratic rights and principles. This new paradigm of participation, however, inherently challenges existing legal frameworks and interrogates the limits of national sovereignty, particularly when hate speech and "fake news" proliferate rapidly across jurisdictions without effective regulatory mechanisms to curtail such practices (Carvalho, 2020).

Despite these complexities, regulatory initiatives have emerged. Europe has responded with the General Data Protection Regulation (GDPR) (EU 2016/679), a global standard-setter in this domain, while Brazil is currently debating its Fake News Bill (PL 2630/2020) in the National Congress, a proposal that continues to face considerable resistance. It is undeniable that online political participation introduces challenges increasingly manifest in democracies, notably through the escalating spread of disinformation and the perpetration of crimes against individuals, institutions, and the democratic state itself. This situation underscores the urgent necessity for appropriate regulation of the virtual environment, a need starkly illustrated by the suspension of the X platform in Brazil.

The urgency for such regulation is amplified by empirical cases demonstrating the direct impact of the internet's instrumentalization against democratic processes. Investigations into the so-called "Hate Cabinet" in Brazil, for example, offer insights into the potential for organized structures to systematically disseminate disinformation and

launch coordinated attacks aimed at influencing public debate and eroding institutional trust. Similarly, the international Cambridge Analytica scandal revealed further dimensions of how personal data manipulation on digital platforms can be leveraged to interfere in elections and steer voter behavior on a massive scale. Both instances not only highlight potential regulatory lacunae but also underscore the repercussions of absent or insufficient specific and effective digital environment regulation.

Institutional responses to these phenomena—such as the Superior Electoral Court's development of resolutions to combat disinformation and regulate new technologies like deepfakes in campaigns, and the existing legal provisions like Art. 323 of the Electoral Code addressing the dissemination of falsehoods in propaganda—are significant strides. Nevertheless, the velocity of technological transformation and the sophistication of manipulative tactics online demand more than reactive, piecemeal solutions. The ongoing debate surrounding PL 2630/2020 in Brazil, much like the discussions in Europe regarding the GDPR's efficacy and limits, reflects a persistent quest for equilibrium between safeguarding democracy, upholding freedom of expression, and protecting user rights.

Addressing this intricate landscape necessitates a principled and adaptive approach to crafting durable solutions. Rather than merely pursuing specific laws that risk rapid obsolescence, it is crucial to foster democratic governance of the digital ecosystem, anchored in continuous multi-stakeholder dialogue. Key pathways forward include promoting algorithmic transparency and platform accountability, sustained investment in critical media and digital literacy, and bolstering international regulatory cooperation. It must be emphasized that the proactive defense of human rights within the virtual sphere should form the bedrock of any regulatory endeavor, ensuring that technology serves to fortify democracy rather than undermine it.

The fragmentation of the digital public sphere and the emergence of information bubbles intensify political polarization and diminish trust in democratic institutions, as social networks tend to foster interactions that reinforce confirmation biases and impede dialogue among diverse groups (Gomes, 2005). Consequently, while digital media expand access to information and democratize political participation, critical discussions are needed regarding the boundaries of free expression and the impact of these platforms on political engagement. An exigent question is whether established regulatory frameworks—such as the Access to Information Law, the Marco Civil da Internet, and the

General Personal Data Protection Law—are equipped with the tools and instruments necessary to promote greater transparency and control while simultaneously checking the advance of practices that, under the guise of democracy, repeatedly harm democratic institutions and fundamental rights.

Therefore, state regulation of digital platforms must strike a delicate balance between protecting freedom of expression and the necessity of limiting the circulation of content that threatens public safety and institutional integrity. This represents a formidable challenge, demanding effective digital governance that, rather than solely emphasizing collaboration (Loader & Mercea, 2011), acknowledges and prepares for inherent tensions among various actors. This transformation points toward a "digital public sphere" wherein citizens assume a more proactive role in information production and distribution, thereby configuring new dynamics of power and collective participation (Fuchs, 2014). Particular attention must be paid to the impact of fake news and algorithmic manipulation on public opinion formation, which compromise users' informational autonomy and exacerbate inequalities in access to reliable, high-quality information (Carvalho, 2020).

The principal challenge lies in ensuring that cyberspace operates as a genuinely pluralistic democratic space—one where a multiplicity of voices is not only guaranteed but valued, and where regulatory criteria and imposed limitations are delineated with rigor and transparency, in adherence to human rights fundamentals and the principles of equity and social justice (Tufekci, 2017).

If, in a prior era, cooperation among governments, digital media platforms, and civil society was viewed as the most straightforward path to establishing effective regulation and moderation for a secure and respectful virtual environment, the current landscape reveals escalating tensions among these stakeholders. The suspension of the X platform, for example, while not an isolated incident, signals a potential rise in disputes between democratic states and major digital platform companies (big tech), potentially undermining the feasibility of harmonious or responsive self-regulation.

Conversely, media literacy and public awareness regarding the detrimental effects of hate speech remain vital tools for preventing such phenomena, though their effectiveness and reach are also under scrutiny. The posture of platforms concerning judicial mandates or legislative proposals for internet regulation suggests that a singular focus on enhancing internal technologies and self-regulatory policies may prove

insufficient. The present situation indicates a critical need for digital platforms to refine their technologies and moderation policies in the future, striving for an equilibrium between protection from harmful content and the preservation of free expression, even as the precise demarcation between these poles remains elusively defined.

In this regard, political participation via the internet constitutes both a profound challenge and an undeniable advancement for democracy. Broadly, the internet significantly contributes to a deeper democratic experience by enabling citizens to engage more actively and dynamically in public sphere discussions. However, as has been demonstrated, it is imperative to reflect on other factors that influence this participation, such as the appropriation of cyberspace by various social groups, ideological and political contests, impediments arising from its use, and the overarching control of this domain.

Thus, the future of digital democracy depends on the effective articulation of state regulation, corporate platform responsibility, and the cultivation of an informed, participatory digital citizenship, all within an adaptive, multilevel regulatory model (De Gregorio, 2022). Such a model presupposes that different tiers of governance—local, national, and international—operate in a coordinated and responsive fashion to the global dynamics of the digital environment. This approach should be underpinned by a "constitutionalization of the internet"—that is, the establishment of a new normative pact capable of constraining the power of big tech and safeguarding fundamental rights, including when exercised in private, algorithmically-mediated environments. This entails, for instance, recognizing public service obligations for platforms, even as private entities, particularly concerning transparency, algorithmic non-discrimination, and protection against systemic abuses.

Furthermore, this adaptive approach acknowledges the futility of static solutions in an era of relentless technological innovation. Instead of relying solely on traditional legal norms, it advocates for flexible regulatory mechanisms, such as regulatory sandboxes, co-regulation initiatives between state and platforms, independent audits, and the development of participatory public deliberation forums on automated decision-making (Cohen, 2019; Suzor, 2019). The objective extends beyond merely preventing abuses to proactively structuring digital communication infrastructure in alignment with democratic values.

Finally, fostering robust digital citizenship requires more than mere media literacy; it necessitates the institutionalization of participatory practices that actively

involve citizens in debates surrounding digital policies and algorithmic regulation. Digital social movements already function as de facto regulatory actors, pressuring platforms and governments for greater informational justice, transparency, and ethical moderation. To disregard these emergent forms of civic power would be to reduce digital democracy to a mere technical recalibration between state and corporate interests (Milan & Treré, 2020).

The ongoing confrontation between state regulation and the frequent resistance of digital platforms to comply with judicial orders in their countries of operation heralds a new chapter in this intricate relationship, with implications for the future of democracy in the digital age that are still far from certain. This suggests that the internet not only transcends conventional limitations of time and space but also exerts profound effects on democratic practice. The potential for escalating conflicts between states and big tech renders this landscape all the more unpredictable.

Referências bibliográficas

AGÊNCIA BRASIL. Liberação do X: confira cronologia da suspensão da rede social. Agência Brasil, Brasília, 10 out. 2024. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2024-10/liberacao-do-x-confira-cronologia-da-suspensao-da-rede-social. Acesso em: 5 jan. 2025.

ALMEIDA, Débora Rezende. Instituições participativas, accountability e mídias sociais: o Conselho Nacional de Assistência Social. In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso. Democracia digital, comunicação política e redes: teoria e prática. Rio de Janeiro: Folio Digital: Letra e Imagem, 2016. p. 41-59.

ARUN, Chinmayi. On WhatsApp, Rumours, and Lynchings. Economic & Political Weekly, v. 54, n. 6, 2019.

BACCARIN, Matheus. "Não é sobre a vacina, é sobre liberdade": o ativismo contra a obrigatoriedade das vacinas para a covid-19 no Brasil. 2023. 178 f., il. Dissertação (Mestrado em Ciência Política) - Universidade de Brasília, Brasília, 2023.

BACCARIN, Matheus. #EleiçãoSemLulaÉFraude x #MoluscoNaCadeia: Memes no julgamento do Lula e o confronto de enquadramentos por meio do humor. 2019. Monografia (Bacharelado em Ciência Política) – Instituto de Ciência Política, Universidade de Brasília, Brasília.

BALKIN, Jack M. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. UC Davis Law Review, v. 51, n. 3, p. 1149-1210, 2018.

BENNETT, W. L.; SEGERBERG, A. The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. Cambridge: Cambridge University Press, 2013.

BITTENCOURT, Geraldo; ROSA, Jorge Martins. Bots, Ciborgues e WhatsAppers: Atores Humanos e Não-Humanos em Grupos Políticos Digitais Brasileiros. Revista Comunicando, v. 11, n. 2, p. e022017-e022017, 2022.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 nov. 2024.

BRASIL. Lei nº 14.192, de 4 de agosto de 2021. Estabelece normas para prevenir, reprimir e combater a violência política contra a mulher; e altera a Lei nº 4.737, de 15 de julho de 1965 (Código Eleitoral), a Lei nº 9.096, de 19 de setembro de 1995 (Lei dos Partidos Políticos), e a Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), para dispor sobre os crimes de violência política contra a mulher. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14192.htm. Acesso em: 15 maio 2025.

BRASIL. Supremo Tribunal Federal. Inquérito (INQ) nº 4.781-DF. Relator: Ministro Alexandre de Moraes. Instaurado pela Portaria GP nº 69, de 14 de março de 2019.

BRASIL. Supremo Tribunal Federal. Presidência. Portaria GP nº 69, de 14 de março de 2019. Gabinete da Presidência do Supremo Tribunal Federal, Brasília, DF 14 mar. 2019.

BRASIL. Tribunal Superior Eleitoral. Resolução nº 23.732, de 27 de fevereiro de 2024. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 10 maio 2025.

CARVALHO, Lucas Borges de. A democracia frustrada: fake news, política e liberdade de expressão nas redes sociais. ILAB. Revista de Direito e Políticas Públicas, v. 1, n. 1, p. 172-199, 2020.

CASTELLS, Manuel. O poder da comunicação. São Paulo: Paz e Terra, 2017.

CASTELLS, Manuel. Redes de indignação e esperança. Movimentos Sociais na era da internet. São Paulo: Zahar, 2012.

CNN BRASIL. Ministério da Justiça notifica Google para ajustar página inicial. CNN Brasil, São Paulo, 9 maio 2023. Disponível em: https://www.cnnbrasil.com.br/politica/ministerio-da-justica-notifica-google-para-ajustar-pagina-inicial/. Acesso em: 10 jan. 2025.

COHEN, Julie E. Configuring the Networked Citizen: Law, Code, and the Play of Everyday Practice. New Haven: Yale University Press, 2012.

COHEN, Julie E. Between Truth and Power: The Legal Constructions of Informational Capitalism. New York: Oxford University Press, 2019.

COLEMAN, Stephen; BRUMER, Jay G. The Internet and Democratic Citizenship: Theory, Practice and Policy. Cambridge: Cambridge University Press, 2009.

COSTA, Lucas Matheus Torres; ALVES, Moabe Barbosa; GUIMARÃES, Rafael Figueredo. LGPD compliance: aplicando checklist para avaliação de sistemas à luz da Lei geral de proteção de dados. 2022. Trabalho de Conclusão de Curso - Monografia (Curso de Bacharelado em Engenharia da Computação) - Instituto Federal da Paraíba, 2022.

DAHLGREN, Peter. The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation. Political Communication, v. 22, n. 2, p. 147-162, 2005. DOI: https://doi.org/10.1080/10584600590933160

DENHARDT, R. B. Teorias da administração pública. São Paulo: Cengage Learning, 2011.

DE GREGORIO, Giovanni. Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society. Cambridge: Cambridge University Press, 2022.

EPSTEIN, Dmitry; KATZENBACH, Christian; MUSIANI, Francesca. Doing internet governance: practices, controversies, infrastructures, and institutions. Internet Policy Review, v. 5, n. 3, 2016. Disponível em: https://policyreview.info/articles/analysis/doing-internet-governance-practices-controversies-infrastructures-and-0.

FARIA, Cristiano Soares de. O parlamento aberto na era da internet: pode o povo colaborar com o Legislativo na elaboração das leis?. Brasília: Câmara dos Deputados, 2012. (Série Temas de Interesse do Legislativo, n. 18).

FARRANHA, Ana Cláudia. A Administração Pública e participação: é possível mais democracia por meio das redes sociais? In: V Congresso CONSAD de Gestão Pública. Brasília, 2012.

FARRANHA, Ana Cláudia; SANTOS, Viviane Silva dos. Governo eletrônico, democracia online e direito à informação: análise do perfil em redes sociais da Secretaria de Políticas de Promoção da Igualdade Racial (Seppir/Brasil). In: SILVA, Sivaldo Pereira da; BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso. Democracia digital, comunicação política e redes: teoria e prática. Rio de Janeiro: Folio Digital: Letra e Imagem, 2016. p. 249-268.

FOLEGATTI, Daniel. STF: além do X, relembre os bloqueios do WhatsApp e Telegram no Brasil. Migalhas, 2024. Disponível em:

https://www.migalhas.com.br/depeso/414499/stf-alem-do-x-relembre-os-bloqueios-do-whatsapp-e-telegram-no-brasil. Acesso em: 5 jan. 2025.

FRIEDMAN, David. Does technology require new law? Harvard Journal of Law & Public Policy, v. 25, p. 71-82, 2001.

FUCHS, Christian. Social media and the public sphere. TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, v. 12, n. 1, p. 57-101, 2014.

GOLDSMITH, Stephen; EGGERS, William D. Governing by Network. Washington, DC: Brookings Institution, 2004.

GOMES, Wilson. A democracia digital e o problema da participação civil na decisão política. Revista Fronteiras: Estudos Midiáticos, v. 7, n. 3, p. 214-222, set./dez. 2005.

GOMES, Wilson. Democracia digital: que democracia? In: II Congresso da Compolítica, Belo Horizonte, 2007. Anais. Belo Horizonte: UFMG, 2007.

GOMES, Wilson. Internet e participação política em sociedades democráticas. Revista Famecos, Porto Alegre, n. 27, p. 58-73, ago. 2005b.

HABERMAS, Jürgen. Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy. Cambridge, MA: MIT Press. 1996.

HABERMAS, Jürgen. Teoría de la acción comunicativa. Trad. Manuel Jiménez Redondo. Madrid: Taurus, 1987. t. 2.

HAN, Byung-Chul. Infocracia: digitalização e a crise da democracia. Editora Vozes, 2022.

HENRIKSEN, Ellen Emilie. Big data, microtargeting, and governmentality in cyber-times. The case of the Facebook-Cambridge Analytica data scandal. 2019. Dissertação de Mestrado em Ciência Política. University of Oslo.

HOFMANN, Jeanette; KATZENBACH, Christian; GOLLATZ, Kirsten. Between coordination and regulation: finding the governance in Internet Governance. New Media & Society, v. 19, n. 9, p. 1406-1423, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836068.

HOWARD, Philip; HUSSAIN, Muzammil. Democracy's Fourth Wave? Digital Media and the Arab Spring, Oxford Studies in Digital Politics, New York, 2013. Disponível em: https://deepblue.lib.umich.edu/handle/2027.42/117564

HU, Margaret. Cambridge Analytica's black box. Big Data & Society, v. 7, n. 2, p. 2053951720938091, 2020.

JACKSON, Sarah, BAILEY, Moya, & WELLES, Brooke. #HashtagActivism: Networks of Race and Gender Justice. The MIT Press. 2020. Disponível em: https://doi.org/10.7551/mitpress/10858.001.0001

JUNQUILHO, Tainá Aguiar; SILVEIRA, Marilda de Paula; FERREIRA, Lucia Maria Teixeira; MENDES, Laura Schertel; OLIVEIRA, André Gualtieri de. (org.). Construindo consensos: deep fakes nas eleições de 2024 relatório das decisões dos TREs sobre deep fakes. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa: Laboratório de Governança e Regulação de Inteligência Artificial, 2024.

KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e direitos humanos. Revista de Direitos e Garantias Fundamentais, v. 24, n. 3, p. 43-71, 2023.

LEMOS, Amanda. Atores da regulação da Internet no Brasil: diálogo entre as decisões de bloqueio do Whatsapp e a elaboração do Marco Civil. 2019. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília.

LESSIG, Lawrence. Code: Version 2.0. New York: Basic Books, 2006.

LOADER, Brian, & MERCEA, Dan. Networking Democracy? Social media innovations and participatory politics. Information, Communication & Society, 14(6), 757–769. 2011. https://doi.org/10.1080/1369118X.2011.592648

LUSOLI, Wainer. Voice and Equality: The State of Electronic Democracy in Britain. New York: Hampton Press, 2013.

MARINHO, Flávio Ayres, CANÇADO, Airton Cardoso, & IWAMOTO, Helga Midori. A constituição popular da islândia: uma nova perspectiva de participação popular por meio das redes sociais / Iceland's crowdsourced constitution: a new perspective on people's participation through social networks. Brazilian Journal of Business, 3(5), 3550–3567. 2021. Disponível em: https://doi.org/10.34140/bjbv3n5-003

MCGAUGHEY, Ewan. Could brexit be void?. King's Law Journal, v. 29, n. 3, p. 331-343, 2018.

MEDEIROS, Simone Assis; MAGALHÃES, Roberto; PEREIRA, José Roberto. Lei de acesso à informação: em busca da transparência e do combate à corrupção. Informação & Informação, v. 19, n. 1, p. 55-75, dez. 2013. Disponível em: http://dx.doi.org/10.5433/1981-8920.2014v19n1p55.

MIGALHAS. Moraes em posse: liberdade de expressão não é liberdade de agressão. Migalhas, 16 ago. 2023. Disponível em: https://www.migalhas.com.br/quentes/371795/moraes-em-posse--liberdade-de-expressao-nao-e-liberdade-de-agressao. Acesso em: 9 set. 2024.

MILAN, Stefania; TRERÉ, Emiliano. The Rise of the Data Poor: The COVID-19 Pandemic Seen from the Margins. Social Media + Society, v. 6, n. 3, 2020. DOI: 10.1177/2056305120948233.

NOBRE, Gabriel P.; ALMEIDA, Jussara M.; FERREIRA, Carlos HG. Caracterização de bots no Twitter durante as Eleições Presidenciais no Brasil em 2018. In: Brazilian Workshop on Social Network Analysis and Mining (BraSNAM). SBC, 2019. p. 107-118.

O'DONNELL, Guillermo. Accountability horizontal e novas poliarquias. Lua Nova, n. 55-56, p. 85-103, 2002.

OLIVEIRA, Fábio Cesar dos Santos. Democracia e internet: a revolução digital e os desafios à representação política. Revista de Informação Legislativa, Brasília, v. 50, n. 199, p. 143-158, jul./set. 2013.

OLSON, Mancur. The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press. 1965

PATRÍCIO, Nathalia Sautchuk. A importância do multissetorialismo na governança da internet. Boletim CEST, v. 2, n. 2, p. 8-16, ago. 2017.

PERSILY, Nathaniel. Can Democracy Survive the Internet? Journal of Democracy, v. 28, n. 2, p. 63-76, 2017.

PERUZZOTTI, Enrique. La política del accountability social en América Latina. 2012. Disponível em: http://ebpdn.org/download/download.php?table=resources&id=509. Acesso em: 10 jun. 2024.

PERUZZOTTI, Enrique; SMULOVITZ, Catalina. Accountability social: la otra cara del control. In: PERUZZOTTI, Enrique; SMULOVITZ, Catalina. Controlando la Política: Ciudadanos y Medios en las Nuevas Democracias Latinoamericanas. Buenos Aires: Editorial Temas, 2002.

PODER 360. Em delação, Mauro Cid teria detalhado "gabinete do ódio". Poder360, 6 nov. 2023. Disponível em: https://www.poder360.com.br/justica/em-delacao-mauro-cid-teria-detalhado-gabinete-do-odio/. Acesso em: 15 maio 2025.

PROVAN, Keith G.; KENIS, Patrick. Modes of network governance: Structure, management and effectiveness. Journal of Public Administration Research and Theory, v. 18, n. 2, p. 229-252, abr. 2008.

RACCAGNI, Dario. The Cambridge Analytica Case: The Evolution of Political and Implications on Communication Strategies and Regulations. 2023. Dissertação de Mestrado. Universidade NOVA de Lisboa (Portugal).

SHIRKY, Clay. Here Comes Everybody: The Power of Organizing Without Organizations. 2008. Penguin Books. Disponível em: https://techofcomm.wordpress.com/wp-content/uploads/2015/11/here_comes_everybody_power_of_organizing_without_organizations.pdf

SILVA, Edmilson Eduardo da; LASMAR, Fábio Costa; PEREIRA, José Roberto. Redes sociais e governança democrática: o caso de uma instituição federal de ensino superior de Minas Gerais. Revista Redes, v. 18, n. 2, p. 104-123, maio/ago. 2013.

SILVA, Irley David Fabrício da; PAIVA, Cláudio Cardoso de. Ciberativismo e democracia nas redes sociais: um espaço de reivindicações e direitos. In: Congresso de Ciências da Comunicação na Região Nordeste – Mossoró -RN, 12 a 14/06/2013. João Pessoa: Intercom, 2013.

SUZOR, Nicolas. Lawless: The Secret Rules That Govern Our Digital Lives. Cambridge: Cambridge University Press, 2019.

TEIXEIRA, Graziela Dias; SENA, Lucas; SILVA, Suylan de Almeida Midlej e. Governança pública e democracia: o papel da Controladoria Geral da União na promoção da Accountability Social. Tempo Social, São Paulo, Brasil, v. 36, n. 2, p. 171–202, 2024. DOI: 10.11606/0103-2070.ts.2024.216403. Disponível em: https://www.revistas.usp.br/ts/article/view/216403.

TUFEKCI, Zeynep. Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press, 2017.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, p. 1-88, 4 maio 2016

VERONESE, Alexandre; CAPELA, Gustavo. Petições em linha e ação política: aplicações de comunicação ou de participação política. Cadernos Adenauer, Rio de Janeiro, v. 18, n. 1, 2017.

WEIDINGER, Laura et al. Ethical and social risks of harm from Language Models. The Alan Turing Institute, 2021. Disponível em: https://arxiv.org/abs/2112.04359. Acesso em: 02 maio 2025.

Abour the authors

Lucas Sena holds a PhD in Political Science from the University of São Paulo (USP), a Master of Laws from the University of Brasília (UnB), and Bachelor's degrees in both Law and Political Science from UnB. Email: lucas.sena@alumni.usp.br. ORCID: https://orcid.org/0000-0002-1444-1347.

Guilherme Otaviano Soares is a PhD candidate in Public Administration and Policy at the University at Albany, United States. He holds a Master's degree in Public Policy and Government from FGV, and a Bachelor's degree in Political Science from the University of Brasília (UnB). Email: gotavianosoares@albany.edu. ORCID: https://orcid.org/0009-0001-5313-9466.

Authorship credits

Both authors are responsible for the conceptualization, investigation, methodology, and writing of the article.

Conflict of interest statement

There are no possible conflicts of interest in carrying out and communicating the research.

Data Availability Statement

Data sharing is not applicable to this article as no data / new data were created or analyzed in this study.

Editors Responsible for the Evaluation Process and Editing

Carolina Alves Vestena and Bruna Bataglia.