DOI: 10.1111/polp.12571

ORIGINAL ARTICLE

P&P POLITICS & POLICY

Digital rights in perspective: The evolution of the debate in the Internet Governance Forum

Adriana Veloso Meireles

Political Science Institute, University of Brasilia, Brasilia, Brazil

Correspondence
Adriana Veloso Meireles, Political Science Institute, University of Brasilia, Brasilia, Brazil.
Email: dricaveloso@gmail.com

Funding information
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

Abstract

The article discusses the transformations of technology in the last two decades, especially those related to privacy, based on the digital rights perspective. It debates how the concept of privacy is grounded on the distinction between public and private, a spatial metaphor no longer applicable in the face of the ubiquity of information and communication technologies. Hence, there is a premise stating the personal is increasingly more political nowadays, due to the phenomenon of surveillance capitalism. To anchor the theoretical debate in an empirically informed discussion, the work analyzes discourses about digital rights used in the main sessions of the Internet Governance Forum. The goal is to map the main Forum controversies about digital rights and their relation with contemporary democracies. Using a combined methodology based on both quantitative and qualitative data from the main sessions of the event, the analysis starts from a survey of the recurrence keywords related to the research; privacy, rights, surveillance, and freedom. From these results, a qualitative analysis of the discourses mobilized in these activities is conducted. The outcomes of the empirical analysis are then discussed from examples of technology regulation in the United States and the European Union. Among the main conclusions of the work, the emphasis lies on the need for transparency and accountability of the artificial intelligence algorithms.

KEYWORDS

AI, artificial intelligence, data privacy, data property regulation, democracy, digital rights, digital tools, European Union, IGF, information technology, Internet governance, liberal thought, participation, political theory, public/private distinction, representative democracy, Snowden, surveillance capitalism, United States

Related Articles
Glen, Carol M. 2021. "Norm Entrepreneurship in Global Cybersecurity." *Politics & Policy* 49(5): 1121–45. https://doi.org/10.1111/polp.12430.
Robles, Pedro, and Daniel J. Mallinson. 2023. "Catching Up with AI: Pushing Toward a Cohesive Governance Framework." *Politics & Policy* 51(3): 355–72. https://doi.org/10.1111/polp.12529.
Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty.'" *Politics & Policy* 45(3): 432–64. https://doi.org/10.1111/polp.12202.

Digital democracy emerged as a field of study in the 1990s based on the expansion of information and communication technologies (ICTs) and the possibilities that technical mediums offered to improve the democratic liberal system, such as political representation and participation, among other aspects. At that time, authors emphasized democracies' deliberative deficit (see, e.g., Coleman & Blumler, 2009) to highlight how digital tools could operate as a support to overcome crises in representative democracies.

However, in the field of political theory, the concept of democracy itself is in constant dispute, since different theoretical schools approach the theme from distinct perspectives, starting from the fact that the concept of democracy is now very different from its Greek inspiration. The political systems of countries considered as democratic are based on the electoral system, political representation, the separation of powers, and in the distinction between public and private spheres.

The discrepancy between these principles and our present context has led to the discreditation of political parties and institutions due to the distance between representatives and the represented, to the fluidity of political preferences, and, most of all, to an incompatibility with the ideal of equality since political representation in itself establishes a difference between voters and politicians. Therefore, in the field of contemporary politics, new conceptions and formulations about how contemporary democracies could overcome challenges imposed by the electoral method and political representation emerge. Such a reduction of the ideal of democracy to the electoral and representative systems adopted by the majority of Western countries is based on principles formulated at the end of the 18th century (Manin, 1992). They therefore do not consider current technological advances.

At first, the literature from the digital democracy field emphasized technical mediums as a solution to a few problems deriving from the electoral and representative systems identified by different lines of thought, such as direct democracy practices. Thus, by associating the digital to the concept of democracy, at that moment "a bet" on technology was made in an attempt to minimize the deficit of participation and the problems of political representation the electoral system imposes. In this context, we must consider a central point of ICTs; the way algorithms—the software that establishes the interface of interaction between people and machines—operate. As daily life is increasingly mediated by cybernetic systems, it is crucial to understand the logic in which they work and how they relate to social, cultural, and political processes, which include political campaigns and the emergence of the concept of digital rights, among other phenomena.

The central issue digital technology introduces is the way information is stored. Analogical computers used to be calculation machines that did not generate data about their use unless they were devices built for that purpose. As digital machines are cybernetic devices, they generate all kinds of information each time they are used in complex feedback processes. They are

communication and control technologies in the sense that they regulate systems that register data (Snowden, 2019). However, with the expansion of the Internet and personal computers, these systems started to catalog information about the people who use them as well as metadata. In this context, Lyon (1994) problematized how records of the most diverse interactions in digital format had the potential to generate broad and sophisticated systems of surveillance.

Currently, the constant collection and storage of personal information, which constitutes big data, is the dominant business model of the Internet, based on the collection, storage, and treatment of private information, which are "voluntarily" conceded by users in the terms of use in websites and applications, disguised as a way to improve their user experience. Therefore, in our context of surveillance capitalism, in which there is a constant and automatized monitoring of individual experiences, privacy is suspended, as personal information is constantly registered and processed for purposes lacking transparency. In the liberal conception of democracy, marked by individualism, privacy became the space for the exercise of freedom, establishing the cession of the right to privacy through the use of digital applications as an intrinsic contradiction.

That is the reason why the right to privacy ceases to be enough to deal with the amount of personal information produced by contemporary society (Doneda, 2006). The right to the protection of personal data therefore emerges to protect individuals from the misuse of their information, whether for surveillance purposes, as the topic is often approached, or to influence consumption habits and informational self-determination. In less than 20 years, the phenomenon of automatized monitoring of private experiences carried out by intelligent algorithms with the intention of inducing consumption and behaviors became stable, and conceptualized as surveillance capitalism (Zuboff, 2019).

For Shoshana Zuboff (2019, p. 34), surveillance capitalism is consolidated from three social phenomena: the freedom to explore broad knowledge about the public without interference; users becoming both consumers and resources; and finally, a radical indifference toward democratic values. The two first phenomena are tacitly associated: while people ignore how their personal information is treated, such information constitutes the required resources for the data market. This unprecedented convergence of freedom and knowledge is the substance of the business model based on personal data. Personal data go on to reflect a tripartite nature: they refer to the individual; they sustain the creation of public policies; but they are also the essence of surveillance capitalism. Therefore, the regulation of data property is one of the most complex contemporary issues that society currently has to address in the face of the indiscriminate treatment of personal information.

The radical indifference regarding democratic values can be observed from the abandonment of organic reciprocity toward people, as they are not only consumers but also the source of raw material for the development of personalized products. In addition, Zuboff (2019) emphasizes that technology companies employ fewer workers as compared to other sectors of the economy, removing what she considers a secular balance between market capitalism and contemporary democracies. The author highlights that General Motors "employed more people during the height of the Great Depression than either Google or Facebook employs at their heights of market capitalization" (Zuboff, 2019, p. 468). The comparison between 1929 and 2019 shows the erosion of the model in which the economy prevails over politics, which leads to the consolidation of neoliberalism and income concentration.

Therefore, the last two decades in which the regulation of the protection of personal data has been absent in the United States allowed not only for the consolidation of Google but also watched Facebook collect and leak data without these companies being held accountable for their interference in complex social processes, including the rules and procedural methods in electoral systems of democracies that are considered to be consolidated—such as in Britain and the United States. The operation of the company Cambridge Analytica in the United Kingdom's choice to exit the European Union and Donald Trump's election in the United

States hold similar characteristics: both presented a broad knowledge of the public; little or no commitment to the organic reciprocity with the collectivist perspective of society (or to democracy itself); and were marked by a radical indifference to ethics and truth.

In these examples, the convergence between resources and rules essential for the practice of domination is observed (Bourdieu, 2018). In other words, technology companies held the resources while the government did not carry out any kind of intervention or regulation. Besides the opacity of the way these companies' algorithms operate, there is a constant attempt to impose rules determined by these very companies onto society. In this sense, the personal is even more political nowadays.

Historically, the concept of privacy—structured from the distinction between public and private spheres—alludes to a spatial metaphor that cannot be applied to the reality of ICTs, in which presence is also virtual, hybrid, and interactive independently from the physical space. Initially developed under the umbrella of the right to be left alone (Warren & Brandeis, 1989), the concept was similar to that of negative freedom (Berlin, 1969); that is, not suffering interference from external agents. In the liberal tradition, individual freedom is based on the private sphere and understood as a space of autonomy and political exercise (freedom of association and speech). It contrasts with the classical perspective, in which freedom was exercised in the public space, the Greek *polis* (Saxonhouse, 1983). The notion of privacy emerged precisely when the representative model of democracy was consolidated, with the secret vote in the early stages of liberal democracy (Manin, 1992). Aligned with the conformation of capitalism and liberal thought, a process of individualization in which personal choices were strengthened via focusing on the "free man" took place. This was when privacy took on its value, considered by some the initial right—the right to the self—constitutive of the other rights. From this perspective, it is impossible to develop one's personality without privacy.

Hence, the consolidation of the idea of individual privacy is relatively new regarding ways of thinking "the social," even though the conception of public and private spheres dates back to Ancient Greece. The point to be underlined here is that the distinction between what is public and what is private is culturally formed and sensitive to historical context. What is understood as public or private changes according to historical and cultural aspects. It also changes according to the kind of chosen discourse. For example, the distinction may sometimes lie between what is political and what is not; and at other times it may lie between what belongs to the government and what belongs to the market; or even between what is domestic and personal or not.

The separation between what is public and private in contemporary societies is a founding principle of liberalism. In the liberal perspective, the separation is anchored in the divide between matters of common interest (that is, what demands state interference), and matters of private interest (in which governments do not establish the rules determined by the law and the market). In liberal thought, the dichotomy between the public and private is related to what are governmental or individual matters. Based on this thought lies the idea of the individual as a political unit and, despite the existence of the recognition of the family as an entity of rights, the authority in the private sphere belongs to the person.

This tradition, founded in the social contract, creates a divide between what is public and what is private, and is based on the proposition that the regulation of private relations would be an intrusion of the state into individual rights. During the Middle Ages, sociability was based on the family. With liberalism, the beginning of an individualization process can be observed from the valuing of the individual rights of men. Thus, the origin of liberalism and capitalism is anchored in a negligence of the private sphere—since, for these lines of thought, political theory should occupy itself with collectivity and what is public, as if private relations did not interfere with public space. Therefore, one of the main contributions to this debate is the feminist perspective which emphasizes that what takes place in the private sphere influences the

public sphere (Okin, 1989). What happens in the private sphere cannot be excluded from the systems of justice, equity, and citizenship. This separation between spheres, between what is universal and what is particular, is based on a conflicted narrative, on a dialectical and binary logic, and therefore, it does not encompass the relational character between what is public and private.

Historically neglected in political theory, the private sphere became the main asset in the technology market (Pateman, 1989) since the technology sector consolidated itself through a business model in which personal information is "voluntarily" given by subscribing to "free services." Surveillance capitalism is a concept that emphasizes how private experiences have become a source of income and commercial advantage for big technology corporations. In the face of these changes, legal norms and institutions can no longer neglect what happens in the private sphere. As a matter of fact, in the last decades, privacy policies have thoroughly embraced data protection.

To illustrate these changes, Nissenbaum's (1998) work is worth mentioning as it discusses the issue of privacy in public. From the example of cameras installed in cities' public spaces by Google Street View, the author explains how the company had to change its algorithms[1] to blur people's faces and other sensitive information. The company's initial allegation was that those images were captured in public spaces and therefore could not be considered private. This case illustrates how the spatial dimension of spheres is insufficient to define what is private or not. On the other hand, the example illustrates how public opinion has interfered in a reactive and not a preventive action because the regulation of the technology sector in the United States is minimal. The lack of regulation made a neoliberal arrangement possible without precedents that enabled some companies in the technology sector to merge with investor groups (see, e.g., Dantas, 2019; Dardot & Laval, 2017; Zuboff, 2019). As a result, the main tech companies' owners are among the richest people in the world.[2] Indeed, FAMGA (Facebook, Apple, Microsoft, Google, and Amazon) are known as companies that lobby with the American government against privacy and data protection regulation.[3] The main allegation they use is that legislation would prevent innovation.

Contradicting this argument is the example of the state of California, the birthplace of Silicon Valley, where the headquarters of most of the FAMGA companies are located. It has its own Privacy Act,[4] a law very similar to the European General Data Protection Regulation (GDPR). This neoliberal arrangement between technology companies and the U.S. government was made possible partially because of the September 11, 2001, attacks that placed the combat against terrorism as a priority and made government investment in surveillance tools possible. Another milestone that must be considered regarding surveillance involved Edward Snowden's revelations in 2013.[5] The end of privacy seemed to be inevitable.

METHODOLOGY AND EMPIRICAL ANALYSIS

To discuss and map these transformations, starting from the concept of privacy and its changes throughout the last century, the first half of this article is devoted to an analysis of the Internet Governance Forum (IGF) debates. Considered the main global event concerning technology

[1]Google begins blurring faces on Street View. Available at https://www.cnet.com/news/google-begins-blurring-faces-in-street-view/.

[2]The World's Billionaires. See https://www.forbes.com/billionaires/list/#version:static.

[3]Google, Amazon, and Facebook all spent record amounts last year lobbying the U.S. government. See https://www.recode.net/2019/1/23/18194328/google-amazon-facebook-lobby-record.

[4]Is Industry Ready for the California Consumer Privacy Act? See https://www.govtech.com/policy/is-industry-ready-for-the-california-consumer-privacy-act.html.

[5]The NSA files. See https://www.theguardian.com/us-news/the-nsa-files.

and society, they have been organized annually by the United Nations since 2006. The applied methodology I use combines different techniques, both quantitative and qualitative, to demonstrate how the debate between civil society, technology companies, and governments has evolved in the last few decades. As an outcome of the investigation, a framework of controversies is drawn up, followed by the description and context of the debates occurring within the main sessions of the IGF.

The empirical analysis presented in the first section shows the initial years of the IGF debates were very formal, often centralized in the dichotomy between privacy and security. In political theory, these arguments refer to the social contract theory. In its contemporary version, a parallel between the terms of service of digital platforms and the social contract theory can be established. In the social contract, people renounce some freedoms in exchange for the security provided by the state—the exclusive holder of the power force. In our current context, rights are alienated to the corporations through the terms of service.

A key outcome of the analysis in this study can be seen as a current diagnosis of the regulation of technology—from firms' terms of service to privacy policies—and how states deal with their power and influence. I present this in the second part alongside some examples adopted by the European Union and the United States, where it is observed that regulation involves issues of privacy and data protection, but also other controversial topics such as content removal and freedom of speech and its limits. Here I highlight the revision of legislation concerning the liability of platforms regarding content published by third parties. The case regarding the right to be forgotten is resumed to illustrate the notice and take-down policy adopted by the European Union. On the other hand, the revision of Section 230 of the American Communications Decency Act is discussed, since it sets the precedents for the non-liability of Internet companies regarding content published by third parties.[6] I argue that, since the platforms became the web's gatekeepers, they play an important role in the Internet ecosystem.

In the following sections, I develop several of the points introduced above in some depth. They revolve around (1) the asymmetry of the terms of services (ToS) contracts between people and technology companies, (2) the property of data generated in cybernetic systems, (3) the private sector's accountability regarding content regulation and its impacts on public debate and electoral democratic systems, and (4) the exercise of human rights in the digital environment. These topics are summarized in the empirical analysis of the evolution of the IGF main session debates. The discussions illustrate the main controversies involving three classes of actors: civil society and academics, the private sector, and governments.

Starting from the emphasis on the collective aspect of privacy and data protection, this article aims to contribute to the discussion on how ITCs are increasingly affecting the exercise of citizenship, rights, and freedoms. Privacy and freedom of speech are rights that are affected by the Internet and its corporations. Hence, among the conclusions of this research, I emphasize the need to regulate the algorithms that operate the web. Since they are the intellectual property of FAMGA, there is no transparency about how they work. The need for the regulation of algorithms of artificial intelligence based on ethics and democratic principles is therefore a key debate for contemporaneous social and political theories.

From these introductory and central issues for political thought and the debates around technology and society, this article presents an empirically informed analysis of the debates on ICTs through a combined methodology. As outlined earlier, the sources of the inquiry are the discourses made in the main sessions of the IGF.

The event was an outcome of the United Nations' approval to hold the World Summit on the Information Society that took place in Geneva and Tunis in 2003 and 2005, respectively.

[6]For example, Senate bill 921 is one of the amendments to change Section 230. See https://legiscan.com/US/bill/SB921/2023.

This two-phased summit was a notable outcome of pressure from the international community for a debate on Internet governance, mainly because ICANN (Internet Corporation for Assigned Names and Numbers) is associated with the U.S. Department of Commerce. The result was the IGF, an annual event organized by the United Nations in cooperation with the International Telecommunications Union (ITU), the world's oldest international organization, founded in 1865 to negotiate the communications infrastructure around the world.

One of the goals of the IGF was to expand the participation of various sectors of society in its management. The multi-stakeholder model was adopted involving governments, civil society, and the private sector. Consequently, the IGF became an internationally qualified space that reflects the main controversies and the evolution of debates on technology and society. This empirical source was chosen, first, because of the multi-stakeholder nature of the IGF and its role in shaping policy debates regarding digital rights. Second, it was chosen given that it is organized within the United Nations, bringing together local and international authorities capable of impacting the social world, institutions, and legal norms. Transparency—all IGF sessions are transcribed in a standardized and structured way[7]—is a third characteristic that justifies the present analysis of the speeches within the scope of the IGF. The period under analysis spans the main sessions of the face-to-face editions of the IGF events that took place between 2006 and 2019.

The main goal of this work is to map the central controversies regarding technology and society in the past few years through the discussions carried out in the IGF activities. The kind of data analyzed were the transcriptions of the speeches both from the speakers and from the public during the main sessions of the IGF. The concepts selected for the quantitative analysis of these transcribed speeches were: privacy, security, surveillance, and freedom.[8] These concepts were chosen because, as shown in the introduction, they are essential to discuss digital democracy and its rights as well as the regulations of the technology sector.

To complement the data, a qualitative analysis of the discourses mobilized regarding digital rights was carried out (see also King et al., 2021; Latour, 2012). King and others (2021) have supported the methodological references for the construction of variables and their relation with the themes of the analysis. I start from the issue of privacy and move toward an understanding of more complex inquiries, such as democracy itself and its justice systems. To complement the research, Latour's (2012) theory, known as the actor-network theory (ANT) is applied to contribute toward a deeper understanding of the relationship between technology and society from interrelated perspectives, or in networks.

Before continuing, a methodological clarification regarding the data sources is appropriate. One has to take into account that the number of the activities of the IGF increases each year, and hence the occurrence of the terms evaluated are proportionally enhanced. As an example of that, while the first Forum held in Athens in 2006 had 11 activities officially transcribed, in the last year of the analysis, 2019, there were 348. In addition, not all parallel activities were filmed and transcribed, and hence it is not possible to evaluate their content. However, by emphasizing the main sessions of the Forum, it is possible to accomplish a quantitative analysis without bias because it conforms to a proportion compatible with the transformations of the event and of society itself.

The quantitative selection of the main sessions of the IGF between 2006 and 2019 derived from their total of 162 activities. For each one, this research verified the incidence of usage of the keywords ("privacy," "rights," "surveillance," and "freedom"). From the first analysis

[7]Internet Governance Forum. See https://www.intgovforum.org/multilingual/.

[8]Other keywords were also analyzed—such as data protection and rights—but for reasons of parsimony, only the most relevant ones for the proposed debate are presented in this article.

of the number of times each term was mentioned by keynoters and the audience, another selection of the sessions was made: those with more keyword occurrences. These transcriptions were read and interpreted from the contextual analysis of the discourse in combination with the main theoretical aspects discussed earlier. Departing from theoretical issues on privacy and democracy, the analysis of the debates is deepened according to the empirical examples, such as the discussion about content removal (which has become increasingly more recurrent throughout the years) that I engage later in this article. Thus, discourse analyses are applied in articulation with the actor-network theory for the mapping of controversies. The sessions' title, year, and location are presented in Table 1.

From the main sessions that had the highest rates of recurrence of the keywords, presented in Table 1, I applied discourse analysis to map the arguments the keynoters and the public have utilized around digital rights and democracy. From these combined methods, I identified the evolution of controversies throughout the years.

For didactic purposes, Table 2 presents the analytical result of these mapped controversies, before I proceed to detail the way discussions occurred in graphics exhibiting the quantitative data regarding the analysis of the frequency in which the selected terms appeared.

The detailing of the discourse analysis was divided into five main periods: (1) the Forum's first years (2006 to 2008), (2) the social networks period (2009 to 2012), (3) the impact of the disclosures regarding mass surveillance by the U.S. National Security Agency (NSA; 2013, 2014), (4) the centrality of human rights (2015 and 2016), and (5) the return of the Forum to Europe (2017 to 2019). Throughout the discursive analysis, a quantitative evaluation is also derived from an inquiry into the recurrence of keywords used in the discourses. These data are later illustrated with graphs regarding the terms "privacy," "rights," "surveillance," and "freedom."

TABLE 1 Main session titles in the qualitative analysis and the event location in each year.

Year	Session	Country
2006	Security Session	Greece
2007	Security Session	Brazil
2008	Broadening Security, Privacy, and Openness	India
2009	Security, Openness, and Privacy	Egypt
2010	Security, Openness, and Privacy	Lithuania
2011	Security, Openness, and Privacy	Kenya
2012	Security, Openness, and Privacy	Azerbaijan
2013	Pressing surveillance issues on the Internet	Indonesia
2014	Evolution of the Internet Governance Ecosystem and the Future of the IGF	Turkey
2015	Human Rights on the Internet	Brazil
2016	Human Rights broadening the conversation	Mexico
2017	Local Interventions, Global Impacts: How Can International, Multi-stakeholder Cooperation Address Internet Shutdowns, Encryption, and Data Flows	Switzerland
2018	Cybersecurity, trust, and privacy	France
2019	Emergent technologies and their interfaces with inclusion, security, and human rights	Germany

Source: Author/data extracted from the IGF website.

TABLE 2 Evolution of the controversies.

Year	Main controversies
2006	Dichotomy between security and privacy
2007	How to regulate different aspects of the technology sector?
2008	How can platforms account for the content published on the web?
2009	How to address the issue of online hate speech and what are the limitations on freedom of expression?
2010	How to fight the concentration of power of the content platforms, private control of public opinion, and the fact that they are becoming the Internet's gatekeepers?
2011	How do automatized filters of content operate and how do algorithms categorize online profiles?
2012	Is online surveillance causing self-censoring and limiting the right to freedom of expression?
2013	In the face of mass surveillance, how to ensure cryptography in interpersonal communications?
2014	Is it the end of privacy? Have we resigned ourselves to accepting surveillance? What is the future of the Internet Governance Forum?
2015	What is corporate accountability in the sales of surveillance technologies? How to ensure privacy in the face of the expansion of the Internet of Things?
2016	How to fight fake news and its repercussions on electoral processes throughout the world? What are the impacts of decision-making algorithms? How to contest the concentration of power of the web platforms and financial system?
2017	How to ensure data anonymization and increase cryptography in interpersonal communications?
2018	How to ensure data protection in the legislation on cybersecurity?
2019	How to ensure privacy by design in technologies based on artificial intelligence?

Source: Author/empirical analysis of the main sessions of the IGF.

FIRST YEARS

The two first years (2006 and 2007) of the main activities of the Forum had a predominant characteristic of being introductory and contextual. The participants emphasized the private sector's role in the expansion of the Internet infrastructure and how governments acted in mediating between public and private interests. They evaluated the theme of the states' interference from the viewpoint of their determination of technical patterns, such as security protocols. The argument that technology advances quickly and, for that reason, the market should regulate itself, was recurrent. It is worth mentioning that the main disputes were centered around the false opposition between security and privacy. The main consensus, a discourse that participants would repeat year after year, is that the solution for the challenges involving privacy and security should revolve around collaborative multi-stakeholders, including governments, civil society, and companies. Among the controversies raised by the participants, it is important to emphasize the audience's criticism of the surveillance developed by their nations.

In 2007, the debate about privacy was still secondary in panelist speeches which, in their majority, highlighted security and cybercrime issues. However, the audience's interventions emphasized privacy issues by mentioning the data market. The audience also mentioned the relationship between privacy and the exercise of freedom of expression in the agenda, a theme that would become the protagonist in the following years. Another important issue concerned the need for transparency regarding the way to deal with security; that is, the form of dealing with democratic controls so that there is no abuse of power by governments.

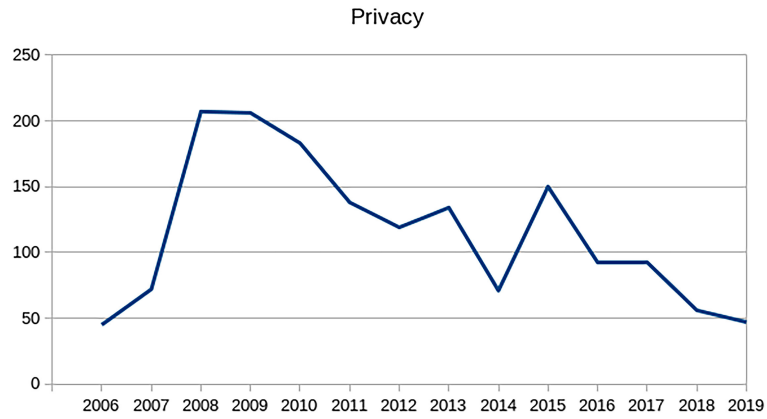

FIGURE 1 Use of the term "privacy" in the Forum's main sessions (1612 occurrences). *Source*: Author/data extracted from the IGF website.

In 2008, there was a change in the sessions' title including the terms "openness" and "privacy," which were present in the next five seasons (until 2012). Another particularity is the fact that 2008 was the year when the term "privacy" was more utilized in the Forum's main sessions. Figure 1 demonstrates the evolution of its recurrence.

The high incidence of the term "privacy" in 2008 is justified by the fact that for the first time there was a main session with that theme in its title. The qualitative evaluation of this year's activity presents other peculiarities. It is important to mention that, after three hours of debate, the session was concluded without the participation of the present or the remote audience, which may have contributed toward a debate with fewer controversies. In that year, the discussion concerning the accountability of the platforms materialized itself in the controversy on technology sector regulation. Such disputes became central throughout the following years. For that reason, it is significant to highlight from the beginning that the topic became directly associated with Article 230 of the American Communications Decency Act (a U.S. law from 1996) which was established to fight online pornography. This rule determined the jurisprudence that service providers should not be held liable for third-party content. However, in the 1990s the Internet still had a more academic and less commercial character. There were no search mechanisms, no Web 2.0, no indexation of multimedia content, and no consequent interaction deriving from such technologies.

Optimism during the period of social networks

In 2009, with the expansion of mobile technologies and the consolidation of the social network phenomenon, IGF speakers discussed issues inherent to the "sharing culture": such as the voluntary offering of personal data, the risks involved in self-exposure, the need for consent regarding data collection and re-utilization, and the very evolution of the big data market (Lyon, 1994). Keynoters focused on a great controversy regarding what was known at the time as "the right to be forgotten."[9] In that year, speakers questioned the controversy

[9]In 2009, a Spanish newspaper published an article including the name of a person involved in a debt from 1998. Mario González requested the removal of his name, but the newspaper refused to do so and his name continued to be shown in search results. He made the same request to Google. After years of dispute, the Court of Justice of the European Union decided that Internet search mechanisms are responsible for processing personal information shown in third-party websites. The decision opened precedents for the removal of content in specific cases, such as irrelevant facts, for example, that occurred a long time ago, or were considered inadequate. The case was known by the expression "the right to be forgotten." However, this is now considered *not* to be the most adequate name to describe such a right, as it is more related to the de-indexation of search mechanisms than to the erasure or removal of a specific Internet content.

over the terms of service and the contract established between people and companies from the perspective of the contextual integrity of information (Nissenbaum, 2009). That is, users offer their data for a determined purpose, but companies, through guarantees established in the terms of service, utilize such information for other purposes, frequently without the user's informed consent. Hence, the alienation of rights becomes even more problematic, going against the thesis of the unity and indissolubility of rights. Finally, a topic that initially appeared in a discreet way is that of the limits of freedom of expression in the face of the proliferation of hate speech, a theme that would become even more relevant in the following years.

From 2010 on, the format of the main sessions ceased to be the panel and acquired the characteristics of a plenary. In 2010, activity was divided into three large themes: (1) the social network phenomenon; (2) the nature and characteristics of Internet networks, technologies, and standards; and (3) international cooperation. Based on the analysis of that year's main interventions, this research observed the consolidation of the debate on content moderation. The key point of the discussion was that platforms were increasingly becoming the judges and executors of their own rules, determining what is or is not allowed according to their interests, and precisely based on their terms of service. As will be seen in the analysis of the coming years, the prioritization criteria, the negligence regarding some kinds of hate speech, and, at the same time, the censorship of some kinds of content was established by very opaque rules.

In the 2010 interventions, an attempt to discuss the regulation of the Internet from a model similar to traditional media's model can be identified. The speakers advocated for the need to determine the minimum rules of action considering democratic principles of justice, transparency, diversity, and plurality (see Benkler et al., 2018). However, the web's characteristics are distinct from those of traditional media. Other relevant variables should therefore be taken into account (including recommendation algorithms; auto-complete tools in search mechanisms and other criteria that influence the fruition of content), since the format of online interaction is much more active than that of the traditional communication mediums. In that context, such conflict unfolds issues involving freedom of expression, free sharing of information, and the protection of intellectual property. Content copyrights relate directly to the free fruition of online media. For that reason, piracy (and pornography) serve as an argument for the consolidation of the notice and take-down regime. On the other hand, it is critical to also highlight that the removal of fake news and hate speech, among other contents that directly affect democracies, will not be as effective as the ones involving piracy.

The 2011 political effervescence caused by events such as the Arab Spring, Occupy Wall Street movement, and Indignados in Spain, among others, reflected itself in the Forum's activities. Speeches emphasizing the political use of social networks were recurrent creating an atmosphere of optimism regarding the use of the web in political organization and social engagement, even though the participants also recognized the risk of surveillance carried out by the state, or by the platforms themselves. Paradoxically, 2011 was the year when the word “rights” was less mentioned in the event's main sessions. It has oscillated annually as depicted in Figure 2.

The second phase of surveillance capitalism gained force precisely when the web apparently consolidated itself as an instrument to amplify political participation. In the face of the intensification of social networks as the main form of online interaction, the controversy over the roles of the platforms acquired new elements. If big tech companies had previously not wanted to be held accountable for the content published by third parties in a prior moment, now they were already adopting opaque measures regarding their practices of content regulation. Hence, they determined the rules about what may or may not be published—notably with low transparency criteria. This violated freedom of expression and, at the same time, failed to contain the dissemination of illegal content such as hate speech, for example.

Most of all in this second phase, content platforms developed algorithms of artificial intelligence to manage content filters, subordinating personal interactions to decisions made by

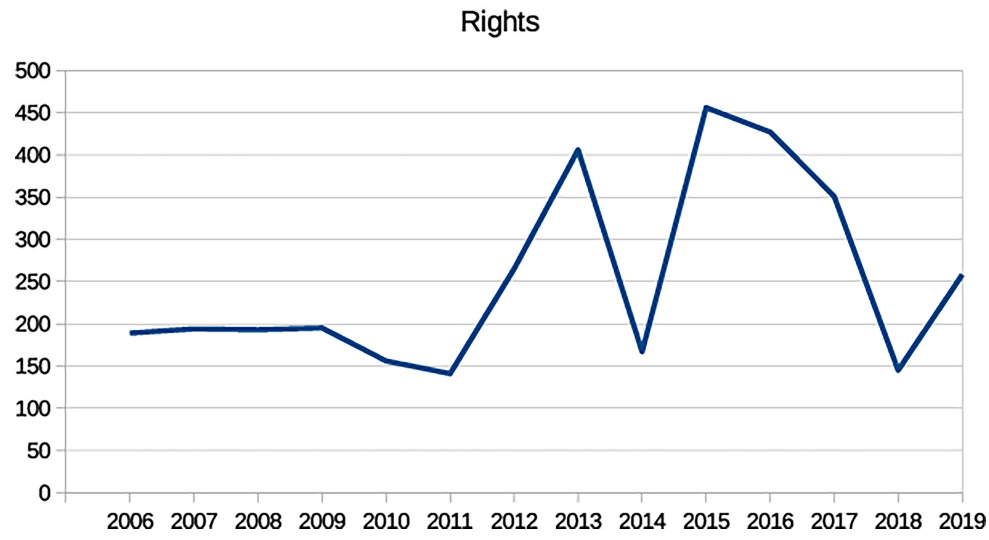

FIGURE 2 Use of the term "rights" in the Forum's main sessions (3543 occurrences). *Source*: Author/data extracted from the IGF website.

machines. The opaque criteria these algorithms adopted do not allow for their auditing, which indicates that they reproduced patterns of discrimination while creating social profiles and moderating content (O'Neil, 2016; Tutt, 2017). Emerging themes also solidified from this period onward, especially the Internet of Things and artificial intelligence. This fact emphasizes the issue of the decision-making process of the algorithms, responsible for creating profile categorizations that reinforce bias based on sensitive data such as sexual orientation, political preference, gender, and class (O'Neil, 2016).

In 2012, the theme of surveillance appeared with more emphasis during the speeches of the Forum's main sessions. It was treated from the perspective of self-censoring practices; that is, people began to recognize that, by being monitored, they limit their freedom of expression. The starting point of the debate concerned the theme of anonymity. According to some, anonymity is necessary for the exercise of freedom of expression, especially in authoritarian countries. However, others consider that anonymity promotes the propagation of hate speech. In such a context, the controversy over the accountability of the platforms was summarized from the perspective of a more severe criticism regarding terms of service and sanctions applied by them to their users, therefore creating a parallel justice system.

The 2013 scandal and the subsequent silence

The year of 2013 was marked by the publication of Edward Snowden's disclosures on the mass surveillance schema practiced by the U.S. NSA in partnership with the largest technology companies in the world. The Forum was carried out a few months after the first news reports, which directly influenced the discussions. Moreover, the Forum established a specific main activity to debate the theme, becoming one of the most controversial sessions of the event, with approximately 30 interventions. On the occasion, the term "surveillance" was highly used, as can be observed in Figure 3.

As Figure 3 shows, rather dramatically, the 2013 conference was marked by the surveillance theme. Among the issues raised, a new debate emerged about digital colonialism practiced through the monitoring technologies. It referred to the fact that some countries serve as tests

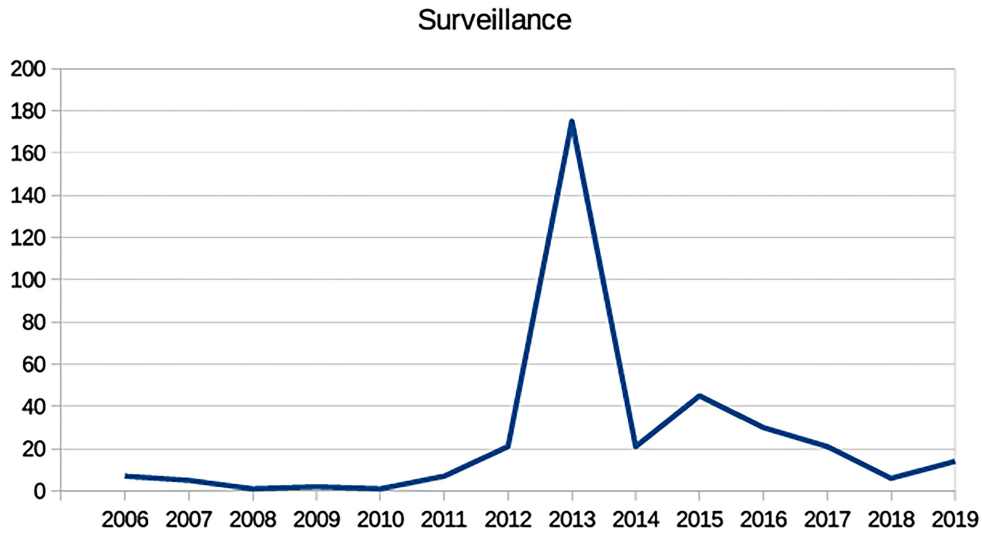

FIGURE 3 Use of the word "surveillance" in the Forum's main sessions (356 occurrences). *Source*: Author/ data extracted from the IGF website.

for the development of new experimental techniques involving biometrics, DNA manipulation, facial recognition, and the utilization of drones, among other technologies. In such a context, it is worth recognizing that human rights—although universal—are not equally implemented among different states: there is an asymmetry of its practice comparing the Global North and South.

At this juncture, it is useful to distinguish between the surveillance of electronic communication and the collection of intelligence information, since they have distinct purposes as data. Besides that, it is worth emphasizing the scale and proportion with which these activities are carried out in the passage from the analog to the digital model. Another key point that had timidly manifested in previous years was cryptography, an important tool to protect privacy in communications. From such a perspective, the debate over the role of whistle-blowers emerged. A growing recognition of the view that whistle-blowers reveal information of public interest and should therefore be protected became evident. However, such protection was not what actually happened, as we may confirm with Julian Assange's condition after the Wikileaks scandal.

After so many controversies, the 2014 Forum was atypical. The NSA scandal was followed by a deafening silence and a strategic change of focus: privacy was no longer the protagonist in IGF debates. It was the only year when the themes of security and privacy were not present in the main sessions' titles (see Table 1). In its place, the broader vocabulary of human rights was adopted.

The center of the debate was a self-evaluation of the role of the multistakeholder model of the event and its practical implications. The timidity in placing controversial debates on digital rights on the agenda implies an accommodation. It seems as if the reality of the facts had been incorporated and there were no alternatives to surveillance capitalism since it would be necessary to transform the business model of the big technology corporations to change the situation. Consequently, the qualitative analysis performed for this study of the main sessions did not identify new topics.

The return of human rights

From 2015, the theme of privacy lost centrality in the titles of the IGF activities, giving way to human rights in a broader sense. The qualitative analysis performed in this research indicates the presence of a more conciliatory and less controversial discourse in comparison to previous years.

In parallel, between the optimism of the golden years of social media and the reality of surveillance, it is possible to observe the rise of other relevant themes, especially content removal, given the expansion of social networks and phenomena such as hate speech and disinformation. The accountability of platforms as gatekeepers of what is published online became central in the recurrent debate about the limits of the freedom of speech and the expansion of the "influence industry," denounced by the Cambridge Analytica scandal.[10] Also, the consolidation of the debate on the Internet of things and the collection of data in the physical world took place. Such discussions are extremely relevant, as they represent the collective dimension of privacy and the relevance of the debate beyond the point of view of individual rights. Such debates also involve considerations regarding the property of collected data as it occurs in smart city projects around the world. To whom does such data belong? To the citizens who generated it? Or to the state or corporations who manage and store them?

In 2016, the format of the plenary was broader, with the presence of about 20 people on stage. They discussed the right to privacy as a prerogative for the exercise of freedom of expression. Participants emphasized that technology cannot be superimposed upon, or superior to, rights, with the risk of harming the future of societies, making them weaker, especially in terms of their authorities' and institutions' reliability. These arguments reflected the entering into force of the GDPR in the European Union, a set of legislation that assures more rights to its citizens who can control their information. It was also responsible for establishing new rules for the technology sector. Such regulation inspired other laws around the world such as the Brazilian *Lei Geral de Proteção de Dados* (LGPD) [General Personal Data Protection Law] and the California Consumer Privacy Act (CCPA).

Still in 2016, the fake news theme was discussed from the perspective of the limits of journalism in attempts to combat it. The speakers argued that the concentration of communication mediums violated the principles of diversity and pluralism in communications. These issues were treated from the electoral perspective, precisely in the year before the Cambridge Analytica scandal. Hence, the controversy over freedom of expression, content moderation, and hate speech became consolidated as one of the major debates in the context of IGF's main sessions.

Paradoxically, when freedom of expression gained centrality in the debate, especially given the private control of the online content and the recommendation algorithms of the web, a downfall in the recurrence of the term in the scope of the IGF's main sessions occurred. Among the 1,650 times that the term "freedom" was used in speeches in the main sessions of the Forum, more than half—815 times—it was accompanied by the word "expression" (see Figure 4).

As the content platforms became consolidated as web gatekeepers, the discussion about content removal and prioritization criteria became more and more relevant. Its influence at the time on public opinion, electoral processes, and online political propaganda indicates the theme of algorithmic transparency as one of the central discussions regarding platforms' liability. In this context, the power concentration of the large web content platforms becomes evident, a fact that contradicts antitrust laws and their combat against monopoly.

[10]Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. Available at <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Accessed on 21/07/23.

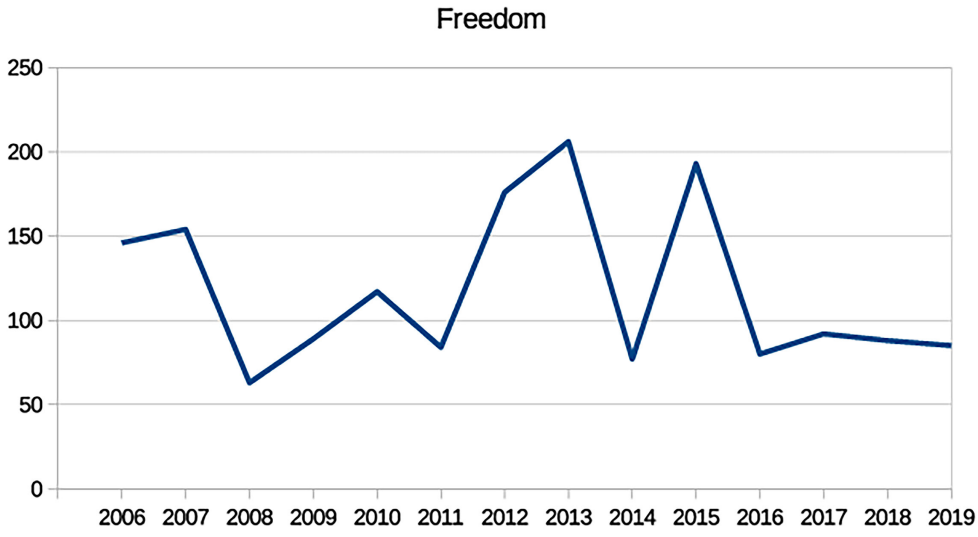

FIGURE 4 Use of the word "freedom" in the Forum's main sessions. *Source*: Author/data extracted from the IGF website.

Political propaganda, as well as misogynous, racist, and xenophobic discourses were sometimes permitted, due to the platform's commercial interests, ignoring democratic principles of diversity and pluralism when determining the rules over content moderation. The platforms made all kinds of content equivalent and were not concerned if the content was journalistic—that is, verified, or mere disinformation. The conversion of "clicks" was considered to be what mattered, independently if they were clicks on advertisements, fake news, or checked content. Still, it is worth considering that the web is part of an ecosystem of mediums marked by asymmetries and concentrations of power and, therefore, in certain aspects, the Internet was, and is, merely reproducing the communication sector's historic patterns.

Final years: A return to Europe

Over time, the Forum was held in practically all continents of the planet, with only a few events in Europe. The 2017 plenary, hosted at the United Nations headquarters in Geneva, established a new format: as the debate occurred, the panelists would leave the stage to open space for other people. In terms of qualitative analysis, it is important to emphasize initially that, for the first time, the cryptography theme gained prominence in a main session in 2017. The anonymization of the data as an additional resource to privacy was also highlighted. Such techniques strengthen data protection. Even with such an emphasis, though, no new controversies were found in the present qualitative analysis of the debates in that year.

In 2018, the theme of privacy returned to the main activities' titles (see Table 1). Yet, the term "privacy" was utilized only 16 times during the whole panel, which was reflected in the present qualitative analysis. I was unable to identify this year's new debate controversies which reinforces the argument that the Forum has become a less conflicted and more conciliatory space.

Finally, in 2019, another change in the activity format took place: there was a round table with approximately 30 chairs, where local Forum representatives reported on the theme of emergent technologies in their regions. The highlight of the last qualitative evaluation lies in

the evolution of the discussion on the ethics involved in the decision-making processes made by artificial intelligence associated with the expansion of the Internet of things.[11]

So, the last three on-site and face-to-face editions of the Forum were not significantly controversial, opening up space for the consolidation of consensus, pacifying, and repetitive discourses (such as the importance of the multi-stakeholder model). Diversity, disputes, and controversies were certainly present in the many other parallel sessions of the event. However, when divergences lose centrality, the quality of the debates is harmed in the same proportion, since democracy is itself built from antagonistic positions. This general point holds for the Forums from 2017 to 2019. Chantal Mouffe (1999) previously offered a solid contribution that applies here in recognizing the conflicted character of politics in its pluralistic agonistic model of democracy in which disputes among political actors contribute to a healthier society.

DISCUSSION, EXAMPLES, AND INITIAL CONCLUSIONS

Throughout almost two decades, the discussions held in the IGF events reflected the evolution of technology itself. Moreover, the event witnessed the transition from the first to the second phase of surveillance capitalism, the consolidation of artificial intelligence, the Internet of things, and other phenomena (Selinger et al., 2018). Paradoxically, the centrality of the debate on the right to privacy was lost. In the past few years, the fact that the cybernetic systems are constantly monitoring private experiences ceased to be a surprise, as if there had been a collective resignation to the view that the end of privacy was actually inevitable. Not even our very irrelevance frees us from the fact that our data feeds surveillance capitalism. In this section of the article, I argue that the technology regulations adopted by different regions reflect social and ethical values that are intrinsic to their democratic system (Grama, 2020). Points of view about liberalism, human rights, the exercise of freedom of expression, citizenship, and democracy manifest themselves in the normative approaches. In the context of IGF, the tension points involved precisely the three categories of actors noted earlier; the state, the private sector, and civil society and their rights.

A central conclusion to be underlined at the outset is that the topic in which there are more divergences is the role of the private sector. The expansion of the business sector starting in the 2000s reflects the transition of the model of capitalist corporations into neoliberalism. For Dardot and Laval (2017), neoliberalism is not an ideology but a "practical order," or a new rationality, that represents the exhaustion of liberal democracy—even though the concept of democracy is constantly in dispute—since the economy guides the politics and not the contrary. This change also has a fundamental characteristic in the transformation of the state's role where the state starts to act more in defense of private interests than in the protection of social rights. These new forms of government change the perception of what is public and what is private, what is political and what is economic (Dardot & Laval, 2017; Fraser, 2021; Harvey, 2007). It is no longer the state that imposes limits on market activity, not even through monopoly control, as is the case with FAMGA.

On the other hand, in the European Union, the main legislation about data protection came into force in 2016. The GDPR aims to contain the advances of technology companies and their business models with mechanisms of informed consent and limitation purposes. The legislation reflects a vision of democracy in which the state is the protector of individual rights and freedoms, representing the welfare state model of the postwar period. The regulation aims to contain the advance of tech companies and their business model based

[11]AI Decision-Making Poses Unique Challenge for State Legislators, Regulators. See https://www.ncsl.org/state-legislatures-news/details/ai-decision-making-poses-unique-challenge-for-state-legislators-regulators.

on the personal data market. In addition, the European Union—which does not cease to be neoliberal—occupies a strategic position in world geopolitics. Therefore, it might be strong enough to contain the advances of the technology companies, most of them located in the United States. In such a context, the regulations on data protection, such as privacy policy, have proved to be insufficient to contain the expansion of surveillance capitalism. Similar to Europe, U.S. antitrust laws have also not prevented big tech firms from broadening their monopolies. The financial market has fused itself with these companies, as they are controlled by the same agents.

Regulating the technology sector is a monumental challenge since, most of the time, the legislative process does not match the speed of its evolution. Notwithstanding this, it is the role of the state to intervene in order to guarantee rights and freedoms. For liberals, the main argument might be securing the foundations of the free market, i.e., a commercial environment that is fair, open, and competitive that benefits the consumer. For those preoccupied with human rights, the arguments are even simpler; it is the role of the state to guarantee that the economy does not trump politics and democratic values, and that human rights are preserved.

An example illustrating such different approaches concerns the court decisions regarding an antitrust case that occurred in 2013. In that year, Google was investigated by consumer defense institutions from both the United States and the European Union for favoring its products in search results, and "hiding" its rivals. In the first case, the U.S. Federal Trade Commission (FTC) considered that Google's manipulation of search results offered no violation of antitrust laws.[12] The European Commission, however, condemned the company in 2017 to pay a fine of 2.42 billion euros—which, at that time, was the greatest conviction of a tech giant.[13] This example in which the court's rules were divergent illustrates the significance of different comprehensions about matters that involve technology and innovation. Jurisprudence is, of course, in constant dispute. In the United States, investigations for violations of antitrust laws are ongoing and may lead to different outcomes. However, is the dilution of the five big techs into 20 or 30 companies really the solution, or is the monopoly break only one of the aspects of the controversy? The outcome of monopoly dilution would mean more companies, but it would almost certainly occur under the control of the same financial actors, as has already occurred in varying degrees in the monopoly regulation of the traditional media.

For all these reasons, the greatest controversy around debates on digital rights identified in the present empirical analysis of the IGF's main sessions concerns the regulation of the technology sector. The traditional media legislation does not adapt easily to the web, whether in terms of its model of concessions, infrastructure expansion, measurement of audience, dissemination of propaganda, protection of privacy, or consumer rights. In such a context, the research has identified a second greatest controversy involving the debates on digital rights in the Forum editions: platforms' liability on content moderation. The discussions involved bear little, if any, correspondence with traditional media, precisely because platforms do not possess editorial control over what is published. On the web, each person can disseminate whatever they choose to. The central pivot of this debate concerns the exercise of freedom of expression and its limits in addition to the prevention of crimes that take advantage of the unregulated online environment, such as hate speech and political violence, among others.

[12]Statement of the Federal Trade Commission Regarding Google's Search Practices. See https://www.ftc.gov/system/files/documents/public_statements/295971/130103googlesearchstmtofcomm.pdf.

[13]"Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service." https://ec.europa.eu/commission/presscorner/detail/pt/IP_17_1784.

Another conclusion of the present study is that the ways to approach data protection are very different in the United States and in the European Union. In the former, perspectives based on consumer rights and antitrust laws are dominant. It starts with the terms applied. The topic is treated as data privacy, not as personal data protection. Another important premise to approach the issue of privacy and data protection in the United States is the September 11, 2001, attacks that directly influenced the suspension of legislation regarding these themes on behalf of the argument of combating terrorism. Precisely for that reason, most of the regulation of the country dates from the 1990s; that is, before web interactivity.

The main legislation that, in theory, protects content platforms is the Communications Decency Act and its Section 230, which states that service providers are not liable for third-party content. In practice, by exempting intermediaries from responsibility, it has enabled the emergence of practices such as the creation of fake accounts on social networks, the dissemination of hateful content, and the use of robots and other contemporary phenomena that did not exist in 1996. This topic is related to data protection precisely because it has established the rules adopted in most of the legislation, protecting big intermediate companies and not people's rights (such as privacy and even freedom of expression). The lag in legislation has become so discrepant that judgments have been recently scheduled at the U.S. Supreme Court with the aim of revising Section 230 of the Communications Decency Act.[14]

The industry's restrictions have not been enough to contain the dissemination of hate speech and disinformation on the web. In these cases, the private sector was initially responsible for distinguishing between what could be online or not. Thus, content platforms have become the gatekeepers of information, especially in social media. Their low transparency rules indicate the creation of content review filters for automated moderation. Then, by trying to fight phenomena such as hate speech, they ended up instituting censorship mechanisms, limiting freedom of expression, and affecting public opinion as a whole. However, advertised content is not moderated, even if it propagates hate speech, political violence, or incitement to crimes.

The technology evolution has changed the understanding of some of these topics in the scope of the European Union. Between 2009 and 2014 the debates about the "right to be forgotten" occurred. The GDPR holds some possibilities for content removal under certain cases. However, the controversy is far from ending, since it involves much more than removing links to information that are no longer relevant or outdated. The role of the private sector in these topics is broader and includes phenomena such as fake news, hate speech, and their influence in the public debate, and, even more seriously, in the results of electoral processes. This case has set a precedent for the notice and take-down policy in the European Union in which companies are held liable if they do not remove content that was notified by the user as harmful. As there is no need for a judicial order, moderation practices have become more dynamic.

Regarding the issue of hate speech, in 2016, the European Union signed, together with the content platforms, a code of conduct to combat the advancement of discrimination due to race, color, religion, sexual orientation, descent, and national or ethnic origin.[15] However, only the German law—known as NetDG—determined that platforms must provide reports on the decision processes involved in curating removed items. The central point is who decides what should or not be removed from the online environment. Judicial determination has been late on some occasions when certain publications have already reached millions of people in a

[14]"How Two Supreme Court Cases Could Completely Change the Internet." See https://time.com/6256887/supreme-court-section-230-internet/.

[15]"European Commission and IT Companies announce Code of Conduct on illegal online hate speech." See https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1937.

short time before being removed. Besides, even when withdrawn, these had already been replicated in other platforms or private chat applications.

Far from ending such controversy, the regulation of platforms frequently focuses on the final aspect of the issue, in this case, content moderation. A central conclusion that emerges here is that the legal framework should impose itself on the regulation of technology companies' processes. How exactly do their algorithms operate? Is it possible to affirm that the decisions of artificial intelligence are based on ethical and democratic principles? How do recommendation mechanisms work? What are the criteria for content prioritization? How do machines learn to auto-complete the results of web searches? Do they reproduce bias? What is considered inappropriate content? How do automated content reviews and filters operate? All of these involve technical decisions through which technology companies may be held accountable in a sense that is broader than the posting of illegal content by third parties. And all these questions will need to be recognized and thoroughly debated as tech firm regulation is more fully engaged in the 2020s and beyond.

The evaluation of such controversy leads to a related and significant conclusion of this research: it is increasingly urgent to regulate the very algorithms operating the web, the artificial intelligence and machine learning systems, the autonomous car and mobile software, and all cybernetic systems that are intermediaries in people's daily life (Tutt, 2017). The decision-making processes of artificial intelligence must be public. Transparency, present in the neoliberal discourse of development, becomes fundamental in the regulation of the technology sector. Opening the source code is an initial step. However, in U.S. jurisprudence, these codes are considered intellectual property and should be kept secret so competitors cannot copy them, impacting their business model. Yet, several open-source initiatives show the financial viability of such a business model. Currently, the best example is the Android operating system which dominates the mobile market and has been expanding itself to other devices such as watches, televisions, and digital appliances. It is open source but has a closed license. There is no copyleft requirement. Thus, the main issue is not only the opening of algorithms but its model of proprietary licensing. The free software user license is different from the open source one precisely for assuring that derivative systems must remain open, impacting the whole ecosystem.

Finally, the article addressed the duality and complementarity between privacy and security with the discussions around the terms of service. In classical social contract theory, people renounce some freedoms in exchange for the security offered by the state, the only authority able to legitimately interfere in the private sphere (Hobbes, 2019). Currently, the parallel with the terms of service of digital apps and platforms reflects how these agreements are made on conditions that are impossible for users to deny, leading them to abdicate certain freedoms, such as that of not being monitored. Thus, the exercise of rights ceases to be indivisible, interrelated, and interdependent, corroding the bases of human rights. The alienation of rights held through the terms of use then becomes a central problem for contemporary political theory.

In short, there are four main aspects of technological regulation I have identified as core issues of the debate: the regulation of privacy and data protection, the limits of antitrust laws and the discussion on content removal, the liability of platforms regarding third-party publications, and artificial inteligence transparency. That said, we proceed to the closing arguments and final conclusions.

CONCLUSION AND FINAL REMARKS

The Internet changed radically in the last 20 years. If initially, in the early 2000s, it was seen as a utopia of an open, non-hierarchical, and decentralized space, more recently, the scenario has thoroughly changed. After two decades, the Internet became a “walled garden condominium”

in which five companies—FAMGA—own most of the network's traffic and the data that flows in it. In a neoliberal arrangement without precedents, these companies profit from each citizen's personal data connected through "free" services that pervade the most everyday aspects of urban life; transportation, e-mail, messaging applications, pictures, and so on. People "voluntarily" give up their personal data, which has become the object of targeted marketing used for both commercial and political purposes.

This article has mapped the main transformations that happened to ICTs from a perspective based on empirical data source from the IGF, an international series of events that are considered a reference in technology and society. Based on this information, a plural methodology was adopted—both quantitative and qualitative—to identify the central disputes involving the debates (summarized in Table 2). The main sessions of the in-person editions from 2006 to 2019 were analyzed offering insights to map the technological transformations that shaped the Internet. The study's main goal was to evaluate the evolution of the debates about technology among civil society, the private sector, and the governments. The discussion began with the false dichotomy between privacy and security and proceeded to question how the absence of regulation of the technology sector and its content platforms influence public opinion. The relationship between data collection and freedom of expression becomes evident with the consolidation of social networks using targeted marketing for very opaque purposes. With the expansion of artificial intelligence and the Internet of things, the need to regulate the operation of the algorithms themselves from ethical, democratic, justice, and human rights principles became salient.

The research problem nevertheless remains in constant dispute as the legislative process generally has difficulty keeping up with the rapid evolution of the technology sector. Yet, in practical terms, the changes have been very discreet for the population in general. The websites' configurations have incorporated disclaimers on the use of data to improve user experience. However, there is an ironic aspect to this. In the vast majority of cases, these notifications only offer the option "accept" so that the website can be accessed. When advanced options of management are present, the options are restricted. Hence, the negotiation margin is still kept to a minimum. One may either accept the imposed terms or will not be able to access the services or information provided. The opt-out options are extremely limited.

Above all, I hope to have shown in this article that data processing challenges the exercise of citizenship, rights, and individual freedoms and that future research and adequate policy advancements have a great deal of important questions to more thoroughly debate and decide upon. Indeed, the data market has become indubitably a collective concern for contemporary democracies. As such, there is a critical need to apply justice criteria in the private sphere since, in the 21st century, what is personal is increasingly political.

ORCID

Adriana Veloso Meireles https://orcid.org/0000-0002-7095-7022

REFERENCES

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press.

Berlin, Isaiah. 1969. "Two Concepts of Liberty." In *Four essays on liberty* (pp. 118–72). Oxford: Oxford University Press.

Bourdieu, Pierre. 2018. "Distinction A Social Critique of the Judgement of Taste." In *Inequality* (pp. 287–318). Oxfordshire: Routledge.

Coleman, Stephen, and Jay G. Blumler. 2009. *The Internet and Democratic Citizenship: Theory, Practice and Policy*. Cambridge: Cambridge University Press.

Dantas, Marcos. 2019. "The Financial Logic of Internet Platforms: The Turnover Time of Money at the Limit of Zero." *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 17(1): 132–58.

Dardot, Pierre, and Christian Laval. 2017. *The New Way of the World: On Neoliberal Society*. New York: Verso Books.
Doneda, Danilo. 2006. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar.
Fraser, Nancy. 2021. "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy." In *Public Space Reader*, edited by Craig Calhoun, (pp. 34–41). Oxfordshire: Routledge.
Grama, Joanna Lyn. 2020. *Legal and Privacy Issues in Information Security*. Burlington, MA: Jones & Bartlett Learning.
Harvey, David. 2007. *A Brief History of Neoliberalism*. Oxford: Oxford University Press.
Hobbes, Thomas. 2019. *Leviathan*. Berkeley, CA: Mint Editions.
King, Gary, Robert O. Keohane, and Sidney Verba. 2021. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press.
Latour, Bruno. 2012. *Reagregando o social: uma introdução à teoria do ator-rede*. Salvador: Edufba.
Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.
Manin, Bernard. 1992. *Metamorfosis de la representación*. Qué queda de la representación política, 1.
Mouffe, Chantal. 1999. "Deliberative Democracy or Agonistic Pluralism?" *Social Research* 66: 745–58.
Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17: 559–96.
Nissenbaum, Helen. 2009. *Privacy in Context*. Redwood City, CA: Stanford University Press.
Okin, Susan Moller. 1989. *Gender, the Public and the Private, 116*. Toronto: Faculty of Law, University of Toronto.
O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books.
Pateman, Carole. 1989. *The Disorder of Women: Democracy, Feminism, and Political Theory*. Redwood City, CA: Stanford University Press.
Saxonhouse, Arlene W. 1983. "Classical Greek Conceptions of Public and Private." In *Public and Private in Social Life*, edited by Stanley I. Benn and Gerald F. Gaus, 363–84. London: Croom Helm.
Selinger, Evan, Jules Polonetsky, and Omer Tene, eds. 2018. *The Cambridge Handbook of Consumer Privacy*. Cambridge: Cambridge University Press.
Snowden, Edward. 2019. *Permanent Record: A Memoir of a Reluctant Whistleblower*. London: Pan Macmillan.
Tutt, Andrew. 2017. "An FDA for Algorithms." *Administrative Law Review* 69: 83.
Warren, Samuel, and Louis Brandeis. 1989. "The Right to Privacy." In *Killing the Messenger: 100 Years of Media Criticism* 1–21. New York: Columbia University Press.
Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

AUTHOR BIOGRAPHY

Dr. Adriana Veloso Meireles holds a PhD degree in political science from the University of Brasília (2020). She earned a master's degree in interaction design from the University of Brasília (2015), a Specialist in Interaction Design from PUC Minas (2013), and a bachelor's degree in social communication-journalism from the Centro Universitário de Belo Horizonte (2008). She has worked as a digital culture coordinator for the Brazilian Ministry of Culture (MinC). She was a UNDP consultant for the Ministry of Justice, Interaction Design at the strategic priorities office in the state of Minas Gerais, and a writer at the publisher Digerati, Rockcontent, among others. Her academic and other publications appear in newspapers and magazines, as well as articles for the web. She works as a consultant in the areas of digital culture, political participation and new technologies, open innovation, free software, and interaction design (usability/ux).

How to cite this article: Meireles, Adriana Veloso. 2024. "Digital Rights in Perspective: The Evolution of the Debate in the Internet Governance Forum." *Politics & Policy* 52(1): 12–32. https://doi.org/10.1111/polp.12571.