

GOVERNANÇA TRANSNACIONAL DA INTERNET: COOPERAÇÃO INTERNACIONAL OU PRIVATIZAÇÃO?

GOBERNANZA TRANSNACIONAL DE INTERNET: ¿COOPERACIÓN INTERNACIONAL O PRIVATIZACIÓN?

INTERNET TRANSNATIONAL GOVERNANCE: INTERNATIONAL COOPERATION OR PRIVATIZATION?

Jaqueline Trevisan PIGATTO¹

RESUMO: Este artigo busca contextualizar um período de transição na governança global da Internet. Com o caso Snowden em 2013, fortaleceu-se a autorregulação privada, mas no médio prazo o Estado respondeu com a criação de leis e medidas de constrangimento ao setor privado, especialmente na questão de proteção de dados pessoais e após o caso Cambridge Analytica, em 2018. Ainda mantendo uma preponderância na governança multissetorial, o setor privado agora está sujeito a regulações e procura se aliar aos Estados para uma possível correção de algumas de suas atividades na Internet.

PALAVRAS-CHAVE: Governança da internet. Transnacional. Regulação.

RESUMEN: Este artículo busca contextualizar un período de transición en la gobernanza global de Internet. Con el caso Snowden en 2013, se fortaleció la autorregulación privada, pero a medio plazo el Estado respondió con la creación de leyes y medidas para restringir el sector privado, especialmente en materia de protección de datos personales y después del caso Cambridge Analytica, en 2018. Aún manteniendo una preponderancia en la gobernanza multissetorial, el sector privado ahora está sujeto a regulaciones y busca aliarse con los Estados para una posible corrección de algunas de sus actividades en Internet.

PALABRAS CLAVE: Gobernanza de internet. Transnacional. Regulación.

ABSTRACT: This article seeks to contextualize a period of transition in global Internet governance. With the Snowden case in 2013, private self-regulation was strengthened, but in the medium term the State responded with the creation of laws and measures to restrict the private sector, especially in the matter of personal data protection and after the Cambridge Analytica case, in 2018. Still maintaining a preponderance in multistakeholder governance, the private sector is now subject to regulations and seeks to ally itself with States for possible co-regulation of some of its activities on the Internet.

KEYWORDS: Internet governance. Transnational. Regulation.

¹ São Paulo State University (UNESP), Araraquara – SP – Brazil. PhD Student in Social Sciences. ORCID: <https://orcid.org/0000-0003-0690-1064>. E-mail: jaquetpigatto@gmail.com

Introduction

The Internet has caused, over its almost 30 years of presence in people's lives, clashes between its end users, corporations that create and shape online spaces and governments that allow, in different degrees, the functioning of this means of communication and information. After a period when few still had access to the network, as in the 1990s, and anonymity prevailed among users, driven by common interests such as on websites for games, music and various themes, the advent of social networks driven by the creation of Facebook in 2004, transformed the use of the network. Now, the Internet has become an environment with no space for anonymity: users' faces and information are prerequisites for socializing, communicating, looking for a job or a service where they live.

Moving on to the 2010s, large corporations created personalized services that have become a vital part of everyday life, whether reading news, mapping places, financial services, commerce, instant communication, among many other possibilities. In this way, the Internet has become an increasingly complex environment, based on the exploitation of personal data, creation of content (from the most useful until the phenomenon of disinformation) and market dispute. The State was slow to enter the field of network governance, but since the Snowden case in 2013, this situation has been gradually changing, culminating in a mixture of state regulations with private self-regulation, while civil society is still trying to be heard, but has already with some relevant achievements.

We understand “governance” as a set of regimes composed of different actors, where authority extends beyond the state actor, thus being decentralized and predominating non-coercive measures such as non-binding principles and guidelines (ROSENAU, 1992; RADU *et al.*, 2014). This approach to the field of the Internet ended up branching out in two ways: on the one hand, States that defend the multilateral character, that is, decision-making and effective participation only by countries and preferably linked to the United Nations system (UN), cases from China and Russia; while other countries such as the United States, members of the European Union and Brazil defend the multisectoral character, where States share the arena of debates and decision-making with other actors that make up the Internet, that is, the private sector, academia, technical community and the civil society.

This article shows that depending on specific contexts, the role of state regulation has increased over time. However, Internet governance tends to be shaped by the actions of large transnational corporations, owners of platforms that have billions of users worldwide. While a large part of the Internet community (epistemic community, civil society and the private sector)

values governance with principles and norms agreed by consensus and voluntarily followed by actors, the State brought an approach more focused on regulation: imposition of laws and centrality in the sovereign power.

This situation is due to two recent cases considered in this work as critical for the development of Internet governance: the Snowden case, in 2013, intensified the debates about the duality of privacy versus security, putting in check the role of the State and surveillance activities, thus favoring self-regulation measures by Internet platforms. The case of Cambridge Analytica in 2018, where personal data of Facebook users were used without their authorization to guide election campaigns, reversed the logic of 2013, in the sense that here the private sector broke the trust with its users. Such a case led the European Union, to a greater extent, and the United States, to a lesser extent, to question the functioning of the platform, as well as influenced Brazil to approve, after years of debate and attempts to formulate, its own law for the protection of Data. Also, the case of the election of Donald Trump in 2016 is not ignored, where the control of content on the Internet started to be more questioned by the States.

The question of multisectorialism

Authors such as Scherer et al., (2006) emphasize the need to adapt the State in this new context of reconfiguration resulting from globalization, where there is a division of space, power and authority with non-state actors. Transnational corporations are starting to occupy functions previously performed by the State, with their importance increasing in societies, as well as their responsibilities and political participation, especially in the implementation of standards, rules and practices. In many cases, transnational companies have taken on a role in responding to social needs and expectations. It is worth remembering that, although there is a concentration of power by large corporations, their services also distributed certain power to their users, facilitating communication, information and organization of personal data. Although platforms such as Facebook and WhatsApp were used in a malicious way to influence political elections², they also allow facilities in a democratic context, such as approximation between voter and political representative, communication and access to information. In other words, these technologies can be used both for democratic progress and for society in general, and to harm it.

² On the triggering of automated messages by WhatsApp in the 2018 Brazilian elections, see: MELLO, P. WhatsApp admite envio maciço ilegal de mensagens nas eleições de 2018. **Folha**, 8 out. 2019. Available at: <https://www1.folha.uol.com.br/poder/2019/10/whatsapp-admite-envio-massivo-ilegal-de-mensagens-nas-eleicoes-de-2018.shtml>. Access: 4 fev. 2020.

In view of the plurality of actors and the different approaches of the countries (United States, European Union and China, for example), the term “global governance” does not seem so appropriate, but that of “transnational governance”. As Gomes and Merchán put it (2016, p. 90, author' highlights):

It can be argued that it is precisely to highlight this tangle of relationships between public (i.e., the State, its organizations and agencies) and private (i.e., corporations, social movements, non-governmental organizations or multilateral organizations) - that make the borders between the State and markets nebulous, preferring the term transnational to global, since the latter tends to unify these relations around the idea of the single global, diminishing the importance of contextual particularities, being this one of the distinctions between global and transnational governance³

What happens is that the scenario of Internet governance on public policy issues still does not make binding decisions to the same extent that they provoke multisectoral debates, such as the Internet Governance Forum (IGF)⁴. Then, the debate about regulation and the need for State intervention to enter, to counterbalance the preponderance of the private sector and its self-regulation, begins. The change in the speech of Facebook CEO Mark Zuckerberg, evidences this transformation: in March 2014, still during the unfolding of the Snowden case, Zuckerberg posted on his social network:

The internet works because most people and companies do the same. We work together to create this safe environment and make our shared space even better for the world. **That's why I was so confused and frustrated by the repeated reports of the US government's behavior. When our engineers work tirelessly to improve security, we imagine that we are protecting you from criminals, not our own government.** The US government must be the champion of the internet, not a threat. They need to be much more transparent about what they are doing, otherwise people will believe the worst. [...] **So, it's up to us - all of us - to build the internet we want.** Together, we can build a space that is bigger and a more important part of the world than anything we have today, but that is also safe. I am committed to seeing this happen, and you can count on Facebook to do our part. (ZUCKERBERG, 2014, author' highlights).⁵

³ Pode-se argumentar que é justamente para destacar este emaranhado de relações entre atores públicos (i.e., Estado, suas organizações e agências) e privados (i.e., corporações, movimentos sociais, organizações não governamentais ou organismos multilaterais) – que tornam as fronteiras entre Estado e mercado nebulosas, que **prefere-se o termo transnacional ao global, pois o último tende a unificar estas relações ao redor da ideia do global único, diminuindo a importância das particularidades contextuais**, sendo essa uma das distinções entre a governança global e transnacional

⁴ The Internet Governance Forum (IGF) has been held annually since 2006, bringing together States, the private sector, the technical community, academics and anyone interested in the digital ecosystem. Without making binding decisions, the Forum serves as a great space for dialogue and exchange of knowledge and experiences on a global scale, turning its attention to themes of public policies, economic and social development, in addition to emerging themes such as Artificial Intelligence and Smart Cities. For more information: <https://www.intgovforum.org/multilingual/>. Access: mar. 2019.

⁵ A internet funciona porque a maioria das pessoas e empresas faz o mesmo. Trabalhamos juntos para criar esse ambiente seguro e tornar nosso espaço compartilhado ainda melhor para o mundo. **É por isso que fiquei tão confuso e frustrado com os repetidos relatos do comportamento do governo dos EUA. Quando nossos**

In March 2019, a year after the Cambridge Analytica case was revealed, Zuckerberg wrote on his Facebook page:

I believe that we need a more active role for governments and regulators. By updating the rules for the Internet, we can preserve the best of it - the freedom for people to express themselves and for entrepreneurs to build new things - while also protecting society from wider harm. [...] **Effective privacy and data protection need a harmonized global configuration.** People around the world have asked for an understandable privacy regulation under the European Union's General Data Protection Regulation, and I agree. **I believe it would be good for the Internet if more countries adopted regulations like GDPR in a common setting** (ZUCKERBERG, 2019, author' highlights).⁶

Without going too far into regulation theories, we turn our attention to the idea of responsive regulation, where there is some flexibility about the need for intervention: “The basic idea of responsive regulation is that governments should be responsive to the conduct of those they seek to regulate in deciding whether a more or less interventionist response is needed” (BRAITHWAITE *apud* GOETTENAUER, 2019, p. 135).

Establishing then an idea of cooperation and gradual interventions depending on the need for coercion or not with regulators, Goettenauer (2019) identifies three elements for responsive regulation, namely: 1) a convergence of regulatory models that favor cooperation between regulator and regulated; 2) a pyramid structure where the base is a self-regulatory regime, but the top brings more severe punishments and interventions by the regulator and; 3) the presence of third parties in the regulatory debate.

We combine this responsive regulation with the idea of different degrees of multisectorialism, something that already happens to some extent, especially in the field of data protection. After all, companies have self-regulatory actions applied at all times, already

engenheiros trabalham incansavelmente para melhorar a segurança, imaginamos que estamos protegendo você contra criminosos, e não nosso próprio governo. O governo dos EUA deve ser o campeão da internet, não uma ameaça. Eles precisam ser muito mais transparentes sobre o que estão fazendo, caso contrário, as pessoas acreditarão no pior. [...] **Então, cabe a nós - todos nós - construir a internet que queremos.** Juntos, podemos construir um espaço que é maior e uma parte mais importante do mundo do que qualquer coisa que temos hoje, mas que também é seguro. Estou empenhado em ver isso acontecer, e você pode contar com o Facebook para fazer a nossa parte. (ZUCKERBERG, 2014, grifos nossos, tradução nossa).

⁶ **Eu acredito que precisamos de um papel mais ativo para governos e reguladores.** Atualizando as regras para a Internet, podemos preservar o que há de melhor nela – a liberdade para as pessoas se expressarem e para empreendedores construírem coisas novas – enquanto também protege a sociedade de danos mais amplos. [...] **privacidade efetiva e proteção de dados precisam de uma configuração global harmonizada.** Pessoas no mundo todo pediram por uma regulação de privacidade compreensível de acordo com a Regulação Geral de Proteção de Dados da União Europeia, e eu concordo. **Acredito que seria bom para a Internet se mais países adotassem regulações como a GDPR em uma configuração comum.** (ZUCKERBERG, 2019, grifos nossos, tradução nossa).

embedded in the policies of their platforms⁷. However, the State that enforces a personal data protection law also establishes guidelines and intervenes (through a fine) when necessary. This is the case of the European Union and its General Data Protection Regulation (GDPR), which has become a strong instrument for notifying the violation of platforms with regard to the personal data of its users. Brazil passed a similar law in 2018, but it has not yet entered into force⁸.

This view has the potential to be improved and there is a search for this co-regulation by the debates at the IGF. Among the main problems to be solved, we can notice: 1) the lack of laws in the United States (home country of large corporations such as Google, Facebook and Microsoft), as well as a fragmentation on the understanding of the multiple functions of the platforms where they can be applied consumer protection laws, antitrust laws and privacy laws, for example; 2) the need for alignment / harmonization of regulatory frameworks, where Europe already seeks this and is evident in the participation of regulators in the IGF, also the BRICS (group of countries considered to be emerging in the 2000s, composed of Brazil, Russia, India, China and South Africa) have the potential for such an alignment⁹; and 3) the understanding or lack of knowledge of politicians and legislators about platforms and the use of new technologies in general, such as that even in Brazil, with its outstanding history in the theme of Internet governance, there have already been attempts alteration of the main existing regulatory framework and international model, the *Marco Civil da Internet*.

Portanto, temos que o multissetorialismo funciona ao priorizar agendas, debates, incluir a sociedade civil, acadêmicos, técnicos e outros atores interessados, mas a pressão por decisões fica dependente dos atores mais poderosos - aqui tanto as grandes empresas quanto Estados que tenham um poder de *enforcement*, como é o caso da União Europeia. Tal abordagem faz parte da governança, que pode abranger tanto mecanismos informais quanto formais, ainda que no caso da Internet, exista uma preferência por ações voluntárias, livres de algum tipo de coerção.

⁷ On the platform's privacy and policy terms, see: OBAR, J.; OELDORF-HIRSCH, A. The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. The 44th Research Conference on Communication, Information and Internet Policy, 2018. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465. Access: 20 mar. 2019.

⁸ Expected to come into force in August 2020, the LGPD faces controversies about the creation of its National Data Protection Authority, provided by law as an independent body for monitoring compliance, but in practice having an excessive link with the Executive power. For more details, see: TEFFÉ, C. Por que precisamos de uma Autoridade Nacional de Proteção de Dados? Jota, 7 jan. 2020. Available at: <https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protacao-de-dados-07012020>. Access: 4 fev. 2020.

⁹ According to Belli (2019), the time is ripe for an alignment of regulatory frameworks among BRICS members, as all members of the group have recently adopted or are finalizing normative frameworks in relation to the protection of personal data, aiming at greater security for the digital ecosystem.

The preponderance of the private sector

The problem of formulating and applying regulation is, as pointed out by Hurrell (2007), the dependence on preponderant actors to apply them effectively. A country of little relevance in the international system or a small digital platform would hardly be able to establish a principle or standard that would be applied by many actors in an efficient manner. In contrast, the European Union has political capital and influence over other actors to enforce its laws, just as large corporations such as Facebook have sufficient power to influence the market and regulatory strategies in different countries from their actions. In the case of Internet governance, such actions enter a context previously dominated by the United States, its political and economic powers and its ideology of non-intervention to prioritize the market, which has internationalized and now faces a demand for changes.

It is in this context that we see the post-Snowden period as a transition period in Internet governance, a preponderance of the private sector (restricted to large corporations) and a moment of strengthening multisectorialism, such as the creation of the Brazilian Marco Civil da Internet, for a stronger union of multisectorialism with multilateralism, in what arrives in 2018 (year of the entry into force of the GDPR) as a moment of transformation, for a stronger emergence of state actions, now led by the European Union. If there will be a preponderance of this actor over the private sector, a future research agenda is vital in this monitoring, but for now we can still glimpse the strong permanence of the great American transnationals, with a certain independence and even leadership in several themes of the digital ecosystem.

As pointed out by Hurel and Lobato (2018), the case of Microsoft is a strong example of private action in the international system, as the company diplomatically advocates for the implementation of standards in the field of cybersecurity, together with States and other international actors. The authors argue that this American giant took the lead in formulating norms that aim at the stability and security of cyberspace, even at different levels, such as national and global:

[...] The Transparency Centers, the Geneva Digital Convention proposal, and technical support services (such as cloud services) are part of the company's socio-technical and multifaceted approach to regulating cyber security. **Technically, this engagement takes place through incident responses, botnet removal operations and technical support. Politically, through entrepreneurial norms activities established by its "Global Security Strategy and Diplomacy Team", as well as by international initiatives such as the Global Commission on the Stability of Cyberspace (GCSC).** In this sense, the Transparency Centers understand national and regional

aspects of the company's involvement and deal directly with the issue of infrastructure security and resilience. The Microsoft Diplomacy Team, on the other hand, **engages in the promotion of global "multilateral" cyber standards with a "multi-stakeholder" implementation, thus advocating for a greater governmental commitment to global cybersecurity governance and entrepreneurship standards** (HUREL; LOBATO, 2018, p. 3, author' highlights).¹⁰

Another recent highlight of private action is the implementation of a Supervision Committee by Facebook (Facebook Oversight Board), considered by the company itself as independent, with the objective of evaluating specific cases of content control and use of personal data, reported by any user of the social network. It is expected that the Committee will be composed of forty members, with three-year terms, where Facebook will appoint an initial group that will subsequently select the other members, following diversity criteria (HARRIS, 2019). According to CEO Mark Zuckerberg, Community Standards follow a series of values - authenticity, security, privacy and dignity - guided by international human rights standards. Thus, the Committee will be a mechanism for appealing the platform's decisions.

The implementation of this independent body went through phases of public consultation and the company says it is working based on the feedbacks received. The Committee's decisions will be implemented immediately and it will be able to make policy recommendations to Facebook. In this way, it will be interesting to observe how this mechanism will work in practice and how it will dialogue with global multisectoral governance, because if successful, intermediating the platform's power with the user and the current state regulatory laws, it could become a new institutionalized governance structure for large digital platforms. More than that, its structure and functioning can innovate the way to deal with transnational problems of the Internet, although it raises questions about legitimacy and multisectoral participation. Internet governance thus remains a field of institutional experimentation for contemporary transnational relations.

¹⁰ [...] os Centros de Transparência, a proposta da Convenção Digital de Genebra, e serviços de suporte técnico (como os serviços em nuvem) integram a abordagem sociotécnica e multifacetada da companhia para regular segurança cibernética. **Tecnicamente, esse engajamento acontece através de respostas à incidentes, operações de remoção de botnets e suporte técnico. Politicamente, por meio de atividades de normas empreendedoras estabelecidas por sua "Equipe de Estratégia e Diplomacia de Segurança Global", bem como por iniciativas internacionais como a Comissão Global sobre a Estabilidade do Ciberespaço (GCSC).** Nesse sentido, os Centros de Transparência compreendem aspectos nacionais e regionais do envolvimento da empresa e lidam diretamente com a questão da segurança e resiliência da infraestrutura. A Equipe de Diplomacia da Microsoft, por outro lado, **se engaja na promoção de cibernormas "multilaterais" globais com uma implementação de "várias partes interessadas", advogando, assim, por um maior compromisso governamental com a governança global de segurança cibernética e o empreendedorismo de normas.** (HUREL; LOBATO, 2018, p. 3, grifos nossos, tradução nossa).

The change in discourse also occurs on the part of the government sector and international organizations, such as the opening speech of IGF 2018 where President Macron did not use the term "multisectorial" but spoke of a "new multilateralism", that is, he prioritizes the involvement of states for regulation, without emphasizing the participation of other sectors. UN Secretary General Antonio Guterres also argued in favor of multilateralism when presenting the organization's digital cooperation report in 2019.

We only need to think of Asian cases to see that multilateralism is already strongly present in the conduct of cyberspace, where countries like China and Russia see a tendency to mirror their national borders on the Internet, such as the Chinese Digital Great Wall, which exercises strong censorship over the Internet within its territory. Also, in China, government control operates rigidly over large local corporations, which are looking to expand internationally, while the entry of platforms like Google and Facebook is restricted. Data show a timid presence of some of these Chinese companies at the IGF¹¹, while China already holds its own Internet conference, simply called the World Internet Conference (WIC), where in its fourth edition in 2017, cooperation between the Chinese state and Saudi Arabia, Egypt, Turkey, Thailand, Laos, Serbia and the United Arab Emirates, in the area of digital economy was announced (PATRICK; FENG, 2018). It is this scenario of "digital sovereignty" that the European Union seems to want to avoid, while fighting total freedom of American intervention. The European "new multilateralism", therefore, would be between the American and Asian models, where the participation of civil society is still questionable.

Such a configuration of cooperation and digital interdependence is plausible for Joseph Nye (2014), since cooperation on one theme is not necessarily linked to another. The author exemplifies economic cooperation through the Internet between China and the United States, even though these countries differ on Human Rights and content control. Therefore, we have that part of the Internet may be more focused on regimes and part on more broad governance. Defining these limits depending on the global region, countries and transnational corporations opens a future research agenda, as well as observing the movements in the International Telecommunication Union (ITU) in the face of the new challenges of platform services and the adhesion of 5G technology¹². So far, the focus of this article has been on the West: American liberalism and democratic multilateralism in the European Union. The BRICS also have the

¹¹However, the 2019 edition of the IGF, based in Germany, had a more significant presence of Chinese representatives, especially academics.

¹²The fifth generation Internet, or 5G, expands the use of the network and enables new features such as the dissemination of the Internet of Things, which consequently increases the generation of data and power resources.

potential to make this connection between the eastern and western approaches, especially through the Brazilian state and India, as was already addressed in a joint statement by the group in 2016 (GRIGSBY, 2016).

The view that global Internet governance is fragmented into three distinct approaches is corroborated by Bruce Schneier in a 2019 interview:

It is already fracturing into three large pieces. There is the European Union, which is currently the super regulatory power. There are totalitarian countries like China and Russia, which are using the Internet for social control. And there is the United States, which is allowing technology companies to create any world they find most profitable. Everyone is exporting their visions to receptive countries. For me, the question is how severe this fracture will be (SCHNEIER *apud* THOMSON, 2019).¹³

The fear of a total fragmentation of the Internet was one of the focuses of IGF 2019, based in Berlin, whose theme was “One world, one Internet, one vision”. Following the model started in 2018 in France, where high-level leaders participated for the first time, the 2019 edition also featured speeches by UN Secretary-General António Guterres and German Chancellor Angela Merkel. The head of government emphasized multilateralism, following the line put forward by Emmanuel Macron in the previous year, but reinforcing the need for the involvement of other stakeholders, especially civil society and the private sector. According to Merkel, the Internet cannot be shaped by states alone. She also conceptualized “digital sovereignty”, often identified with isolation and censorship (the term is widely used by Chinese representatives to refer to how China rules the Internet in its territory). In the chancellor's view, “digital sovereignty” concerns each individual and society as a whole to determine, for themselves, how the development of the Internet will be, that is, it relates sovereignty with autonomy (MERKEL, 2019).

Guterres, on the other hand, addressed the challenges to be faced in three existing divisions: there is also the problem of the digital divide, referring to populations that do not yet have access to the Internet; the social division, caused mainly by the operation of algorithms and; the political divide, where national borders and cyber attacks strain the international system. In the Secretary-General's view, the UN is the most propitious place for such problems

¹³ Já está se fraturando em três grandes pedaços. Há a União Europeia, que é atualmente o super poder regulador. Há países totalitários como China e Rússia, que estão usando a Internet para controle social. E há os Estados Unidos, que está permitindo as companhias de tecnologia criarem qualquer mundo que elas acharem mais lucrativo. Todos estão exportando suas visões para países receptivos. Para mim, a questão é quão severa será essa fratura. (SCHNEIER *apud* THOMSON, 2019, tradução nossa).

to be faced, where joint work can take place in sharing expertise and creating common principles among the actors (GUTERRES, 2019).

Therefore, this work understands the strategy put forward by the European Union since 2018 as a new multisectoral approach, to differentiate itself from the American approach in which multisectorialism favors its technological industry.¹⁴ European governments still want to keep the Internet close to its original principles, but regulating it so that they are maintained, thus not being "hijacked" by other actors (such as digital platforms). Angela Merkel reinforced in her speech the issue of freedom as a fundamental principle of the Internet. In this way, the European Union returns to a brief role played by Brazil after the Snowden case, of regulating maintaining a multisectoral character, to guarantee the freedoms and rights of all who use the Internet. Especially between 2014 and 2015, Brazil advocated internationally for multisectoral governance of the Internet, without the preponderance of a single state (referring to the United States). In addition to domestically approving the Law of Marco Civil da Internet in 2014, also passed a UN resolution together with Germany on privacy in the digital age¹⁵.

For now, the private sector of the large transnational corporations maintains a certain preponderance in the midst of multisectoral governance, as the changes in services contracts on the use and processing of personal data, although they follow the guidelines of state laws, do not yet have transparency mechanisms related to the architecture of these platforms, which increases trust between the service and the user; the choice of using cryptography is up to the company, which may restrict third party access to its customers' data, including by the State and; the fines hitherto applied to the large transnational corporations correspond to low values in relation to the billings of these companies, in addition to not requiring significant changes in the business model based on the data.

It should be noted, however, the progress in some concepts and regulations by the States, where the debates at the IGF play an important role in the dialogue and exchange of experiences, especially among regulators. Building flexible regulations has been one of the main successes over the years of the IGF, whose discussions inspired the Brazilian Marco Civil¹⁶.

¹⁴ On American preponderance in global Internet governance, see: CANABARRO, D. Governança Global da Internet: Tecnologia, Poder e Desenvolvimento. Orientador: Marco Aurélio Chaves Cepik. 2014. 431 f. Tese (Doutorado em Ciência Política) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

¹⁵ For more details, see: PIGATTO, J. **O Brasil e a governança da internet: a repercussão do caso Snowden e as ações do governo brasileiro por maior controle internacional da rede.** Orientador: Marcelo Passini Mariano. 2017. 40 f. Monografia (Trabalho de Conclusão de Curso em Relações Internacionais) - Universidade Estadual Paulista Júlio de Mesquita Filho, Franca, 2017.

¹⁶ One of the bases for the Marco Civil da Internet was the work of the IGF Dynamic Coalition called "Internet Rights and Principles". For more details: **Dynamic Coalition on Internet Rights and Principles (IRPC), Internet Governance Forum.** Available at: <https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-internet-rights-and-principles-irpc>. Access em: 25 nov. 2019.

Final Considerations

The libertarian culture of non-state intervention, of a transnational network that does not depend on national borders, added to the configuration of favoring the private commercial sector in the United States, created a pattern that, with the expansion of companies and services, was exported to many other countries, thus creating the Internet that we know today. Debates oppose different state wishes in relation to the principles internalized by the Internet's epistemic community, such as the free flow of information and privacy (CASTELLS, 2001). The development of new services for the Internet and the emergence of large platforms such as social networks or e-mail services, file storage, calendar, etc., all linked to a personal account, demanded new questions from the business model based on personal data. Instead of the user paying financially for these services, the currency of exchange is the very collection of information that it generates to the platform owner, revealing their preferences, personal information such as address, real-time location, type of device used for access, among others.

After Edward Snowden's revelations about North American massive espionage, Brazil played a brief leadership role in global Internet governance, advocating for multisectorialism and instituting a national law, the Marco Civil da Internet, which elaborated on a multisectoral basis established principles and guidelines on rights and duties on the network. The Snowden case also enabled the European Union to strengthen its data protection law, causing GDPR, which came into force in 2018, to create some constraints on platforms like Google and Facebook. The same post-2013 period increased, in the short term, self-regulatory measures, such as the increase in encryption used by Internet services and platforms, including by large corporations. But the misuse of personal data exposed by the Cambridge Analytica case in 2018 caused the state figure to pressure the private sector with more regulation and control on the network.

Despite efforts to establish global governance, we see that it is already fragmented into at least three main approaches used by state actors prevalent in the international system: the United States and its non-interference that prioritizes the free market, consequently prioritizes its transnationals that seek to maintain this status through lobbying and other forms of pressure; the European Union that tries to restrict some of that American libertarian character by establishing rules and laws for the functioning of these digital services; and the Chinese case of authoritarian intervention, not discussed in depth in this work. The adaptation of large transnational corporations to these different configurations then allows a private self-regulation approach. At the same time, state concerns about big platforms are no longer just focused on

economic policies, but now they are also related to fundamental rights issues, that is, the national logic is strained. For the West, we see that while States and other actors seek to define what exactly a “digital sovereignty” is, the question remains whether it is possible to make it compatible with multisectorialism.

ACKNOWLEDGMENTS: this article is part of the master's research entitled “The role of transnational corporations in global Internet governance: Google and Facebook in discussions on network neutrality and data policy (2013-2018)”, funded by the Research Support Foundation of the State of São Paulo (FAPESP), process 2018/02378-4. I thank my advisor, Prof. Dr. Marcelo Passini Mariano, and to my fellow researcher Mark Datysgeld, for the help and discussions that resulted in this work.

REFERENCES

- BELLI, L. 5G e IoT: BRICS precisam de cooperação em cibersegurança. **Convergência Digital**, 9 set. 2019. Available at: <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=sit e&infolid=51649&sid=15>. Access: 12 set. 2019.
- CASTELLS, M. **The Internet Galaxy**: Reflections on the internet, business, and society. New York: Oxford University Press Inc., 2001.
- GOETTENAUER, C. Regulação responsiva e a política de segurança cibernética do sistema financeiro nacional. **Revista de Direito Setorial e Regulatório**, Brasília, v. 5, n. 1, p. 131-146, maio 2019.
- GOMES, M.; MERCHÁN, C. Governança transnacional: definições, abordagens e agenda de pesquisa. **RAC**, Rio de Janeiro, v. 21, n. 1, p.84-106, art. 5, 2016.
- GRIGSBY, A. Do India and Brazil really moderate China and Russia’s approach to cyberspace policy? **Council of Foreign Relations**, 26 abr. 2016. Available at: <https://www.cfr.org/blog/do-india-and-brazil-really-moderate-china-and-russias-approach-cyberspace-policy>. Access: 13 set. 2019.
- GUTERRES, A. **Discurso na cerimônia de abertura do IGF**. In: YOUTUBE. 1 vídeo (transmissão ao vivo). Berlim, 26 nov. 2019
- HARRIS, B. Estrutura e governança do comitê de supervisão. **Facebook Newsroom**, 17 set. 2019. Available at: <https://br.newsroom.fb.com/news/2019/09/estrutura-e-governanca-do-comite-de-supervisao/>. Access: 17 set. 2019.
- HUREL, L.; LOBATO, L. **Unpacking Cybernorms**: Private companies as norms entrepreneurs. Giganet: Global Internet Governance Academic Network, Annual Symposium

2017. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107237. Access: 25 set 2019.

HURRELL, A. Complex governance beyond the state. *In: On global order: power, values and the constitution of international society*. Oxford University Press: New York. 2007. p. 95-117.

MERKEL, A. **Discurso na cerimônia de abertura do IGF**. *In: YOUTUBE*. 1 vídeo (transmissão ao vivo). Berlim, 26 nov. 2019.

NYE, J. The regime complex for managing global cyber activities. Centre for international governance innovation and the royal institute for international affairs. **Paper series**, n. 1, maio 2014. Available at: <http://bit.ly/2yJ0IcI>. Access: 28 maio 2019.

PATRICK, S.; FENG, A. Belt and router: China aims for tighter internet controls with digital silk road. **Council on Foreign Relations**, 2 jul. 2018. Available at: <https://on.cfr.org/2ZBvekx>. Access: 5 ago. 2019.

RADU, R. *et al.* **The evolution of global internet governance: principles and policies in the making**. Switzerland: Springer, 2014. 245p.

ROSENAU, J. Governance, order, and change in world politics. *In: Governance without government: order and change in world politics*. Cambridge University Press, n. 20, 1992. p. 1-29.

SCHERER, A. *et al.* Global rules and private actors: toward a new role of the transnational corporation in global governance. **Business Ethics Quarterly**, v. 16, n. 4, p. 505-532, 2006.

THOMSON, I. Q&A: Crypto-guru Bruce Schneier on teaching tech to lawmakers, plus privacy failures – and a call to techies to act. **The Register**, 15 mar. 2019. Available at: https://www.theregister.co.uk/2019/03/15/qa_bruce_schneier/. Access: 13 set. 2019.

ZUCKERBERG, M. **As the world becomes more complex and governments everywhere struggle, trust in the internet is more important today than ever**. Facebook: Mark Zuckerberg, 13 mar. 2014. Available at: https://www.facebook.com/zuck/posts/10101301165605491?stream_ref=1. Access: 12 set. 2019.

ZUCKERBERG, M. **I've spent most of the past two years focusing on issues like harmful content, elections integrity and privacy**. Facebook: Mark Zuckerberg, 30 mar. 2019. Available at: <https://www.facebook.com/zuck/posts/10107013839885441>. Access: 12 set. 2019.

How to quote this article

PIGATTO, Jaqueline Trevisan. Governança transnacional da internet: cooperação internacional ou privatização? **Rev. Sem Asp**, Araraquara, v. 8, n. 1, p. 225-239, jul./dez., 2019. e-ISSN: 2358-4238. DOI: <https://doi.org/10.29373/sas.v8i2.13357>

Submitted: 21/10/2019

Required revisions: 20/11/2019

Approved: 15/12/2019

Published: 30/12/2019