The Internet Governance Paradox

https://www.e-ir.info/2020/10/20/the-internet-governance-paradox/

JAQUELINE TREVISAN PIGATTO, OCT 20 2020

Global Internet governance is a rising and relatively new subject. Although an extensive literature has already discussed processes such as the Internet's development by the United States, as well as institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the United Nations' (UN) involvement in processes like the Internet Governance Forum (IGF), there is a lack of consensus on the current state of this governance's setting in the face of multiple regulations on the Internet. The beginning of the 2020s points to an urgency in digital cooperation in the face of critical moments of conjuncture such as the widespread manipulation of electoral processes and the COVID-19 pandemic. The geopolitical component has never been so strong within Internet governance, and its layers of operation and use are increasingly interconnected. These layers of infrastructure, protocols and applications used globally are part of an ecosystem commonly called "Internet governance".

The most accepted definition for Internet governance is:

Internet governance is the application by governments, the private sector and civil society of principles, norms, rules, procedures and programs that shape the evolution and use of the Internet (Working Group on Internet Governance [WGIG] 2005).

We assume that recent events provide the coexistence of three governance models: (1) from the USA that prioritizes free market through its big technology transnationals, concentrating data that become cybernetic power resources; (2) the European, whose recent actions from the European Union created strong extraterritorial regulations, affecting American companies; and (3) the Chinese, in which authoritarian interventionism allowed a restriction on the entry of foreign companies, at the same time that big transnationals of the technology market were created beyond the socioeconomic layer. The paradox that we find in Internet governance is that the network itself is intrinsic to the concept of "global", however, its governance does not correspond to this idea, coexisting different types of governance and regimes on specific subjects that involve nation-states, private sector and even civil society.

Joseph Nye Jr. (2014) mapped the main international institutions and their regimes related to cyberspace – updating parts of his idea of complex interdependence, developed in the 1970s with Robert Keohane – exposing the economic interdependence between countries and the role played by the Internet. One of his main statements is that countries do not have to necessarily cooperate on all issues, and can prioritize the issues related to commerce and economy, usually differentiating more on preferences about Human Rights. It is also what Farrell and Newman (2020) called "chained globalization", about the strong interdependence that maintains links between countries, which may or may not agree on other topics – such as the USA and China. Another point raised by Nye and crucial to the subject of Internet governance is that what the complexes of regimes lack in coherence, is compensated in flexibility and adaptability, which in this theme of fast evolution are advantages that allow the actors to adjust to uncertainties.

Several extant studies on global Internet governance focused on isolated layers of function, or analyzed cases of specific countries, such as China and its "digital sovereignty". The transition scenario in which we are currently living makes these analyses more complex by simultaneously inserting China in layers of infrastructure (through 5G and companies such as Huawei) and of content/socioeconomic (through apps such as TikTok and WeChat). Another important component in this global scenario, besides the traditional United States and its technology giants, is the

European Union and its extraterritorial regulations, such as the General Data Protection Regulation (GDPR), as well as potentially the upcoming Digital Services Act (DSA). Therefore, different governance models coexist to what still is at the protocol level, a single Internet. Standards imposed by nation-states (such as data protection laws) coexist in the current scenario with the ones that come from institutions such as ICANN alongside its political implications and private self-regulatory actions (Belli et al, 2019). ICANN is the international multistakeholder organization responsible for the administration of contracts related to the regulation of Internet Names and Numbers usage, or Domain Name System (DNS) (Datysgeld, 2017).

The discussion is no longer limited to the platforms and private companies that occupy a significant space on the Internet. The multistakeholder model that was arrived at for this governance shows itself insufficient in the face of nation-state pressures and difficulties of the private sector in promoting effective self-regulation (Hofmann, 2016). In this sense, it becomes a question whether the Internet's transnational origins are being called into question in face of the actions of nation-states. This question has already existed for decades, in different contexts and involving different actors. Lemos (2020) also refers to it as Internet moments of dystopia and utopia; in the present moment of 2020, it is a strong dystopia, while the mechanisms of international cooperation try to hold on to the "utopian" ideas of multistakeholderism, but with a high level of realism, which means prioritizing the Westphalian state-led model.

It is valuable to comprehend how Internet governance has been organized since the 2010s. For the West, the event that marks this new scenario is Edward Snowden's revelations in 2013 and the resulting pressure from the international community for Internet decentralization. As for the East, 2012 saw the rise of Xi Jinping to power in China and a new Internet model established marked by reinforced censorship and a maintenance of strong state control. This would soon be expanded to countries with common interests, as in the 'Belt and Road Initiative' (BRI) in the South-East Asia and Africa.

As stated earlier, there are three models to consider for Internet governance: the Chinese, the American and the European. Therefore, we can use the term "model" to refer to the interests of a nation-state in the way that the Internet is operated in its territory (and possibly beyond). We also understand "cybernetic power resources" as a set of resources commonly owned by big technology transnationals, capable of altering behaviors and influencing societies, such as personal data, informational infrastructure, computational capacity, user bases, and use of algorithms (Mariano et al.; 2018).

Today is different from all previous points in Internet governance history and we can justify that statement with two examples: for the first time, by the end of the 2010s, the industry joined the state to ask for regulation, as seen after Cambridge Analytica's case in 2018 (Pigatto, 2020). Also, the European Regulation for Personal Data Protection has put tension even to ICANN, which still tries to implement an access policy to the Whois database (a global database that dates back to the beginning of the Internet, which used to hold all of the registrant data for those who owned domain names in a public manner), and tries to enter the space of the International Telecommunication Union (ITU) – traditionally multilateral.

While US companies invested in the Internet through a layer of content with services such as Facebook and Google, China became a major player in the infrastructure layer, although it also stands out with some apps that threaten American hegemony in this field, especially in Donald Trump's protectionist scenario. Today, Facebook has 2.7 billion active users (Clement, 2020), while the popular Chinese app WeChat has 1.2 billion (Thomala, 2020). ICANN – currently global and multistakeholder but also of American creation in a liberal context – starts this decade trying to find itself in the intermediate layer of protocols while complying with state regulations and maintaining "a single Internet", as its motto says. The institution appears to actively attempt not to get involved with geopolitics.

With this we have a complex Internet governance paradox, where the globalization maintained by the Internet conflicts with nationalisms, policies, and distinct cultures demands at least cooperative resolutions among all the actors. Faced with the challenge of maintaining a globalized economy and a transnational flow of services, the maintenance and uses of the Internet are between favoring national markets or governments, making us question how to find such a balance.

Is there a multistakeholder global governance?

In order to talk about Internet governance, we must start from the main trait that was attributed to it by the United States and some European states: the multistakeholder model. Nowadays it has spread to other fields, but this model basically opens space for all the interested parties, whether they are nation-states, private companies, or civil society. In the most commonly used definitions, there are three groups of stakeholders, with the state's preponderance legitimized by the Westphalian model, in which the state is sovereign. As explains DeNardis (2020):

A critical point for understanding Internet governance is that there is not a single system of oversight and coordination but an entire constellation of functions, each overseen by different governance structures distributed over one or more actors. Collectively, this administration and coordination of the technologies necessary to keep the Internet operational and the heterogeneous policies enacted around these technologies is viewed as distributed, multistakeholder governance, even if in practice multistakeholder arrangements rarely match the rhetoric around multistakeholderism.

Allied to the multistakeholder composition is the bottom-up nature of the system, in which the decisions are made starting from demands raised by participating actors and go through all the other ones. In theory, Internet governance should work starting from the premise that all of the stakeholders that are affected by an action are able to get involved in the debate.

The "cyberlibertarian" disposition from the Internet epistemic community stands out, adopted by many academics amidst political and cultural movements from the 1960s and 1970s. The 1980s saw the rise of one of the most important institutions for the Internet maintenance, under the leadership of its epistemic community: the creation of the Internet Engineering Task Force (IETF) in 1986 was the start of an institutionalization for the network's governance, bringing with it values from the cyberlibertarian culture.

Wu and Goldsmith (2006) make a comparison between the top-down governmental mechanisms – which means when there is a chain of command where citizens obey due to coercion costs – and the opposite mechanism where discussions, arguments, and consensus flow from the bottom to the top. Such an idea is synthesized in the famous line of one of these community members, Dave Clark: "We reject: kings, presidents, and voting. We believe in: rough consensus and running code". This dynamic is crucial for the construction of the principles of the Internet governance that exists today. The central idea is that the Internet protocols are neutral, therefore transnational. Researchers who were present in the creation of the network could carry out in practice the culture and values of their time, in a cosmopolitan trend. However, a manner of "update" happens in these interests as new actors enter the Internet's ecosystem, especially for commercial purposes (and for the expansion of protocols developers as well as alternative and ancillary networks). Using the same IETF example, nowadays several of this institution's participants represent interests from the private sector, meaning the market determines technical decisions that imply public policies. It is what DeNardis (2014) calls "privatization of the Internet governance", after all, if the number of actors increases, so does the interactions between them.

Besides the infrastructure layer, the roles of each actor were determined and are commonly accepted by the Tunis Agenda, a document that resulted from the World Summit on the Information Society (WSIS) that took place between 2003 and 2005 by the ITU, and that created the Internet Governance Forum (IGF), a larger space for discussion on Internet subjects that involve public policies without making binding decisions. According to the document:

Policy authority for Internet-related public policy issues is the sovereign right of states. They have rights and responsibilities for international Internet related public policy issues. The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields. Civil society has also played an important role on Internet matters, especially at the community level, and should continue to play such a role. Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues. International organizations have also had, and should continue to have, an important role in the development of Internet-related technical standards and relevant policies (WSIS, 2005).

Nevertheless, as Doria (2014) recalls, this setting was unilaterally imposed by nation-states without consulting other actors. Currently, these definitions are not reflected in practice. The private sector took over several functions that originally belonged to the state, owning the authority to remove posts from any user of a social network, for instance, including from heads of state. Civil society shows itself as an actor with high levels of participation, but their considerations are not always taken to the decisions, adding up to the fact that several users do not own sufficient knowledge about the functioning of the network and the platforms they use (as well as some government representatives). Lastly, although intergovernmental organizations try to exercise a role of creating spaces to facilitate discussions (such as the IGF itself), they fail to establish incentives for the effective participation of all the actors, contributing to a fragmentation of regimes

One can notice by the development of the layers how an increasing interdependence between them exists – infrastructure, protocols and content – and how they were originally conceived through an assignment of roles that does not always favor dialogue. With the state's sovereign power increasingly present, ramping up the Internet with geopolitical implications, it is natural that a larger demand for international cooperation happens to try to maintain the Internet's own proposal.

There are several efforts at the transnational level to elaborate recommendations and good practices between actors, since the imposition of binding measures seem difficult due to constraints such as state sovereignty itself and the high speed of changes and technological developments demanding flexibility from all actors. An example is "The Age of Digital Interdependence" (UN, 2019), a report for the UN's digital cooperation, released in 2019 by request of UN Secretary-General António Guterres, who also highlights the need for joint efforts from multilateralism with multistakeholderism. The idea of "digital cooperation" refers to maximizing the benefits and minimizing the damage for society that comes from emerging technologies on the Internet, through cooperation "systems", even if it is not specified what kind of "systems" those would be, in a possible approximation with the idea of regimes or multistakeholder treaties. The document also recalls that not only different countries must cooperate, but also their domestic entities such as regulatory agencies, maintaining dialogues as well as an exchange of experiences and knowledge.

The world is suffering from a "trust deficit disorder", in the words of the UN Secretary-General addressing the UN General Assembly in 2018. Trust among nations and in multilateral processes has weakened as states focus more on strategic competition than common interests and behave more aggressively. Building trust, and underpinning it with clear and agreed standards, is central to the success of digital cooperation (UN, 2019).

The 2010s and upcoming transformations

In 2013, Edward Snowden revealed that the PRISM system had direct access to the servers of most key Internet companies. This massive surveillance program enabled access to Internet browsing data, as well as the content of emails, voice and video calls, transfer of files, and much more. Companies such as Google, Microsoft, Facebook, and Yahoo! appear in the files that were shown by Snowden as some of the project's "collaborators". Thereby, this episode revealed the dimension and depth of the power concentrated by these companies and by the US government, which increased international pressure and questions about the centrality of the network in the country.

Several public and private measures were taken as a reaction to this movement, such as the increase on the use of encryption and nation-state regulations providing rights and duties for the Internet's actors, especially regarding personal data protection. These were the cases of the Brazilian Civil Rights Framework for the Internet (or Marco Civil da Internet), in Brazil, and the GDPR, in the European Union. "The year 2016 was a landmark in tech history, the first year since the invention of the Internet that more Web traffic was encrypted than unencrypted." (Snowden, 2019).

With regards to China, before Xi Jinping the network had relatively more liberty, there was a certain freedom of expression and VPN usage was widespread. However, state control was intensifying at the same time that big technology transnationals were growing with the blocking of action from several US companies in the Chinese territory. As Economy (2018) notes: "the challenge for China's leadership is to maintain what it perceives as the

benefits of the internet – advancing commerce and innovation – without letting technology accelerate political change". And the Chinese progress did not happen only in its domestic and corporate context, but also in institutions and international actions.

The Chinese position did not gain traction in international fora at first, such as in the ITU in 2012 where together with Russia, they advocated for a multilateral Internet governance. So, they built a strategy on their own by example of the "Digital Silk Road", a system of advanced IT infrastructure with other countries of the Asian region. In addition to annually hosting the World Internet Conference (WIC), China has now a strong voice in the ITU, where in September 2019 they brought the proposal of a "new Internet", including a new IP (Internet Protocol), through a team composed by members of Huawei. (Gross; Murgia, 2020). It is also worth mentioning that just as with ICANN, the ITU does not usually get involved politically or does not assess the potential uses of technological development. For the organization, the use depends on each person or country, therefore favouring the Westphalian system.

Still the context of the 2010s, there was the *boom* of social networks with the discourse of materializing the "promise" of a democratic Internet that could give voice to any connected individual. Facebook was seen as an instrument of freedom and revolution, just as every Internet tool in the context of the Arab Spring, in 2011 (Kurbalija, 2014). In this way, many of the companies that emerged from social networks carry in their proposals the cosmopolitan ideals of universalization and connection without borders, gaining strong political outlines.

However, this aspect hitherto positive was strongly overturned on the second half of the decade, in election contexts of democratic countries where social media such as Facebook, WhatsApp, Instagram, YouTube, and Twitter was found out to be used for the dissemination of disinformation, resulting in a "*techlash*" against these companies. The regulatory attempts over content vary from self-regulation actions from the platforms themselves to legislative procedures that threaten fundamental values, such as freedom of speech and privacy, exemplified by a bill known as "Fake News Bill" (Bill 2630/2020), discussed during 2020 in Brazil. The bill presents a proposal for traceability of message forwarding on Internet applications such as WhatsApp, violating the principle of presumption of innocence and presenting no guarantees of effectiveness.

We argue that social networks demonstrate a concentration of problems that were already present on the Internet ever since its beginning: conflict with Westphalian jurisdictions, transnational flow of personal data, and developments that affect dimensions "outside the virtual world", such as political elections and socioeconomic dynamics. This present moment can also be seen as a conflict between generations: one can recall the times when the Internet was a synonym of anonymity (due to the Internet's anarchic character in its beginning) or of sharing spaces such as blogs about common interests (or of personal expression, like the photologs, etc.). The arrival of the social networks created a certain social obligation for each user's identification, with several encouragements for posting pictures, localization, activities being done in real-time, among other contents for a larger interaction and less privacy, also contributing for surveillance mechanisms.

Adding up to this complex ecosystem is the proposal for further democratization and reach that the Internet was supposedly going to offer everyone, as well as closer and easier contact between the rulers and the ruled. Such social phenomena collectively built were submitted to rigorous transformations that were barely assimilated by its users, much less by legislation and state bureaucracies, facing the rapid advances of the companies from Silicon Valley. Mark Zuckerberg's famous motto for innovation was to "move fast and break things", but what to do now that things have been broken?

It has become more notable that many platforms are having to adapt themselves to local legislations, like Apple storing data from Chinese users territorially on China's servers; a social network receiving court orders to remove profiles globally, like Twitter and Facebook received from a Brazilian minister; or even a Chinese app in risk of being banned from the US, like TikTok, with the possibility of being bought by a huge US corporation, a measure that goes beyond forced data localization.

Facing this plurality of actors and the different approaches from countries, especially the USA, the European Union, and China, the term "global governance", commonly used in the studies of Internet governance, does not seem

adequate, but nor does “transnational governance”. As stated by Gomes and Merchán (2016, p. 90):

One can argue that it is precisely to highlight this tangle of relationships between public (i.e., state, its organizations and agencies) and private actors (i.e., corporations, social movements, non-governmental organizations or multilateral agencies) – that make the borders between state and market clouded, preferring the term transnational rather than global, because the second one tends to unify these relationships around the ideal of the unique global, decreasing the importance of contextual particularities when this is one of the differences between the global and transnational governance.

Therefore, this is precisely the paradox that we find in Internet governance: the network itself is intrinsic to the concept of “global”, however its governance does not correspond to this idea, coexisting different types of governance and regimes on specific subjects that involve states, private sector and even civil society. A governance that is indeed “global” would demand global efforts in agreements about transnational flows of data (facing, for instance, China’s Great Firewall), content moderation by the platforms and other subjects, that basically need flexible and foundational rules, so it does not quickly become obsolete towards the technological development and consequent new social situations from the use of these technologies.

Final considerations

The present moment of transformation in Internet governance, that came from a setting that was more focused on private self-regulation and now tries to balance the power of large transnationals with state regulations, is increasingly being affected by geopolitical conflicts and national movements. The element that seems to maintain the Internet out of a series of “nationalization” efforts is the economy and the profit that comes with it. Although there are now laws on the regulation of personal data, they seek to maintain the transnational flow of said data, harmonizing safer practices that can give greater reliability to the involved actors. However, there is still the need to analyze if efforts such as the GDPR from the European Union collide with bilateral agreements that allow such flows and continue to promote high financial earnings, whether for the private sector or the state in informational terms, for control or knowledge of preferences, disrespecting basic principles of human rights. Thus, Internet governance seems to be on its way to becoming a huge “cybereconomy”, this one being unified in the “global” concept. Concerns regarding the rights of users and human rights in general are being nationalized and fragmented by different uses of the Internet between countries and regions.

There is an ever-growing demand for studies on the different subjects related to the Internet in order to map a certain degree of fragmentation in distinct fields. Those are the cases of personal data protection, content moderation, surveillance, antitrust regulations, developments of Artificial Intelligence, among others. The present framework is, therefore, a paradox: the Internet is still unique in its protocols, but the content layer shows itself increasingly fragmented and political, with speech that threatens a deeper fragmentation of other network layers. The question that remains is if the fragmentation of governance can be equivalent to a fragmentation of the Internet itself. And if not, we must discover a way to foster cooperation and trust mechanisms between the actors so that the governances are the least distinct as possible.

**This study is financed by The São Paulo Research Foundation, FAPESP.*

References

Belli, L. et al. (2019). Lei do Estado ou lei da Plataforma? Cuidado com a privatização da regulação e da polícia. In: Belli; Cavalli, Governança e regulações da Internet na América Latina: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 556p.

Clement, J. (2020). Facebook: number of monthly active users worldwide 2008-2020. Statista. Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. [Accessed 30 September 2020].

Datysgeld, M. (2017). O papel da Governança da Internet dentro da Governança Global: Um estudo de caso da ICANN. São Paulo: Programa de Pós-graduação em Relações Internacionais San Tiago Dantas – UNESP/UNICAMP/PUC-SP, 156 p.

DeNardis, L. (2020). Introduction: Internet Governance as an Object of Research Inquiry. In: Researching Internet Governance: Methods, Frameworks, Futures. The MIT Press.

DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.

Doria, A. (2014). Use (And Abuse) Of Multistakeholderism In The Internet. In: R. Radu et al ed., The Evolution of Global Internet Governance: Principles and Policies in the Making. Zurich: Co-Publication with Schulthess Juristische Medien, p.115-138.

Economy, E. (2018). The great firewall of China: Xi Jinping's internet shutdown. The Guardian. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown. [Accessed 30 September 2020].

Farrell, H. and Newman, A. (2020). Chained to Globalization: Why It's Too Late to Decouple. Foreign Affairs. Available at: https://www.foreignaffairs.com/articles/united-states/2019-12-10/chained-globalization. [Accessed 13 October 2020].

Goldsmith, Jack and Tim Wu. (2006). Who Controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press.

Gomes, M. and Merchán, C. (2016). Governança Transnacional: Definições, Abordagens e Agenda de Pesquisa. RAC, Rio de Janeiro, v. 21, n. 1, art. 5. p.84-106.

Gross, A. and Murgia, M. (2020). China and Huawei propose reinvention of the internet. Financial Times. Available at: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2. [Accessed 30 September 2020]

Hofmann, J. (2016) Multi-stakeholderism in Internet governance: putting a fiction into practice. Journal of Cyber Policy, Milton Park, v. 1, n. 1, p. 29-49.

Keohane, Robert O. and Joseph S. Nye. (1977). Power and Interdependence. Boston: Little, Brown.

Kurbalija, J. (2014). An Introduction to Internet Governance. DiploFoundation. 6a ed.

Lemos, R. (2020). 'O Dilema das Redes'. Folha de São Paulo. Available at: https://www1.folha.uol.com.br/colunas/ronaldolemos/2020/09/o-dilema-das-redes.shtml. [Accessed 28 September 2020].

Mariano, M. et al. (2018). Atores internacionais e poder cibernético: o papel das transnacionais na era digital. Monções: Revista de Relações Internacionais da UFGD, Dourados, v.7. n.13. Available at: http://ojs.ufgd.edu.br/index.php/moncoes/article/view/8723. [Accessed 30 September 2020].

Nye, J. (2014). The Regime Complex for Managing Global Cyber Activities. Centre for International Governance Innovation and the Royal Institute for International Affairs. Paper series n°1, 20 pages. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf. [Accessed 22 June 2020].

Pigatto, J. (2020). O papel das corporações transnacionais na governança global da Internet: Google e Facebook nas discussões sobre neutralidade da rede e política de dados (2013-2018). São Paulo: Programa de Pós-graduação em Relações Internacionais San Tiago Dantas – UNESP/UNICAMP/PUC-SP, 210 p.

Snowden, E. (2019). Permanent Record. Metropolitan Books; 1st Edition. 352 p.

Thomala, L. (2020). Number of monthly active WeChat users from 2nd quarter 2011 to 2nd quarter 2020. Statista. Available at: https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/. [Accessed 30 September 2020]

UN (2019). The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. Available at: https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf. [Accessed 30 September 2020]

WGIG. (2005). Report of the Working Group on Internet Governance. Château de Bossey: WGIG. Available at: <www.wgig.org/docs/WGIGREPORT.pdf>. [Accessed 30 September 2020].

WSIS (2005). Tunis Agenda for the Information Society. ITU. Available at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html. [Accessed 30 September 2020]

About the author:

Jaqueline Trevisan Pigatto is a Ph.D. Candidate at the School of Humanities and Sciences, Sao Paulo State University (UNESP), Brazil. Her major research area is Internet governance, with interests in data protection and transnational actors.