

Beyond Copy-Paste: The Brussels Effect and the Evolution of Digital Law in Brazil

Alexandre Pacheco da Silva^{ID}, Rebeca Maldaun Cabral^{ID}

São Paulo School of Law, Getulio Vargas Foundation, São Paulo, Brazil

Email: alexandrepachecodasilva@gmail.com, beckycabral03@gmail.com

How to cite this paper: da Silva, A. P., & Cabral, R. M. (2025). Beyond Copy-Paste: The Brussels Effect and the Evolution of Digital Law in Brazil. *Beijing Law Review*, 16, 610-642.

<https://doi.org/10.4236/blr.2025.161029>

Received: February 11, 2025

Accepted: March 28, 2025

Published: March 31, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

The recent growth of the information technology sector around the world and, consequently, its challenges, have resulted in an increased interest in regulation. Given this scenario, the European Union (EU) has been seeking to take the lead in regulating new technologies so as to expand its influence in the legal field, in such a way that other countries have been adopting the European model. Thus, the EU is frequently the first to establish new obligations for tech companies, and many countries tend to follow the EU's regulatory footsteps, as part of a phenomenon known as the "Brussels Effect". In this context, Brazil's current approach to regulating the digital environment provides a good illustration of the Brussels Effect, most notably in the examples of the General Data Protection Regulation (GDPR) and current legislative debates similar to the Artificial Intelligence (AI) Act. The paper also discusses the characteristics of legal transfers in the context of the Brussels Effect, highlighting that it is not an unilateral legal transplant, but actually a transfer that takes place through local adaptations, as showcased by the Brazilian scenario. However, transfers tend to follow an unilateral direction from the Global North to the Global South, which is demonstrated by the previously mentioned legal imports Brazil has made. Therefore, this paper concludes that the Brazilian example can assist in understanding the implications of the Brussels Effect, in particular how this phenomenon can manifest itself through local adaptations of laws and regulations that fit the receptive country's needs.

Keywords

Brussels Effect, Legal Transfers, Comparative Law, Digital Ecosystem, Digital Platforms

1. Introduction

Over the past few decades, recent innovations in information technology and the

widespread access to social networks have led the technology sector to grow immensely worldwide, marked by the rise of big tech platforms and amplified in particular by the use of artificial intelligence (AI). With such growth, concerns regarding privacy protection, antitrust issues, content moderation, the risks and dangers of AI, and other controversial aspects about the tech industry start to rise.¹ Recently, in the majority of cases, the European Union (EU), as one of the dominant digital powers of the world, has been the first to regulate these challenges. The EU has been imposing new responsibilities and duties for tech companies to comply with in European territory, with the aim of preserving the fundamental rights of its citizens in view of the growth of these challenges in the digital environment.

In this context, Brazilian regulators are constantly looking at Europe's discussions and progress when it comes to regulating the digital environment, in fact, several Brazilian legislators have mentioned being inspired by European regulations in interviews and in official documents with regulatory proposals.² This is part of a phenomenon known as "Brussels Effect", which refers to the EU's influence over regulatory decisions in other countries around the world (Bradford, 2020: p. 2). The Brussels Effect explains how the EU has become the predominant exporter of norms around the world, yet, this phenomenon tends to reflect the prevailing perception that legal transplants, that is, the exportation and importation of legal institutions from one country to another, can only follow the Global North to Global South direction.

In this sense, in the last few years, Brazil has become known for being heavily influenced by EU's debates on regulations concerning digital challenges, with the most notable example legislative being the General Data Protection Law (*Lei Geral de Proteção de Dados*—LGPD, in Portuguese), which regulates the treatment of personal data in the country's territory, similarly to the General Data Protection Law (GDPR) in the EU, while there are also other debates taking place in the country concerning regulation of AI. Although there are several examples of the Brussels Effect in Brazil concerning the regulation of the digital economy, this paper will focus on two main instances, which regards data protection and AI systems, since the EU has already approved regulations on the subject, while discussions in Brazil are at a more advanced stage.

In this regard, the EU's most recent step towards regulating the digital economy

¹For instance, the European Commission has recently fined Meta €797.72 million for "breaching EU antitrust rules by tying its online classified ads service Facebook Marketplace to its personal social network Facebook and by imposing unfair trading conditions on other online classified ads service providers". Similarly, Google was also fined for breaching EU antitrust rules for abusing its market dominance as a search engine by giving an illegal advantage to Google products. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5801 and https://ec.europa.eu/commission/presscorner/detail/hr/memo_17_1785.

²For instance, in the summary of Bill No. 21/2020, on the principles, rights and duties for the use of AI, the rapporteur Representative Luiza Canziani mentioned that the proposal's main inspiration was the EU AI Act, which was underway in the European Parliament and the European Council at the time. She praises the successful partnership between Brazil and the EU when the GDPR served as inspiration for the drafting of the LGPD.

was approving the AI Act, which addresses the risks of AI and sets requirements and obligations to developers and deployers of AI. On a similar note, currently one of the biggest discussions taking place at the Brazilian National Congress regards the implementation of a legislation to set rules on the development, promotion, ethical and responsible use of AI in the country.

Thus, our intention with this paper is to explore the meaning of the Brussels Effect through the lens of the Brazilian example, qualifying the meaning of legal transfer from the perspective of local adaptations made by the receptive country. This will be done through an analysis of national and international bibliography, as well as an analysis and comparison of the content of the European regulations on data protection and AI, and the content of the Brazilian data protection law, as well as the Bill of Law currently being discussed regarding AI. With that in mind, this paper intends to show how the ongoing deliberations in Brazil challenge the concept of legal transplants. Although Brazil is deeply influenced by the EU's regulations in the digital environment, and one could say that legal institutions are in fact traveling from the EU to Brazil, the Brazilian discussions are not exact replicas of the European discourse. In Brazil, these legislations have been modified and adapted to the society's demands and particular characteristics, and therefore, can be described as legal transfers instead of legal transplants.

As such, Part I provides a contextual background about the transplanting and transferring of legal concepts and institutions, together with the direction they usually follow and the role Latin America's law plays in this discussion. Part II focuses on the EU's strategy for regulating the digital economy and how Brazil is influenced by these discussions. Part III offers an overview of the recent examples of how the Brussels Effect has affected the Brazilian regulatory discussions regarding the digital environment, with similarities and differences in the projects.

2. The Direction of Legal Transfers

2.1. Legal Transplants and Legal Transfers

The study of comparative law allows us not only to have better knowledge of different legal systems, but also to understand the behavior of law, that is, how law is capable of developing and traveling from one jurisdiction to another. In this sense, the global spread of legal institutions, ideals, ideologies, doctrines, and so on, usually by the hands of the elite (Graziadei, 2006: p. 1), has become known as "legal transplants". Legal transplants can be understood as the exportation and importation of legal institutions that have previously worked in a country to another country. In other words, it happens when a rule or a system of law, from any branch of the law, is borrowed by one jurisdiction from another. Currently, legal transplants are seen as one of the major topics of comparative law, attested by its immense influence on the globe's present legal landscape.

Alan Watson, the legal historian who introduced the term "legal transplants", explains that one of the most startling and obvious characteristics of legal rules is the "apparent ease with which they can be transplanted from one system or society

to another” (Watson, 1978: p. 313). Watson claims that transplanting has been the major feature of legal change in the Western world for the last thousand years, and the borrowing of rules and structures from elsewhere is the main way law changes (Watson, 1978: pp. 314, 321). The desire behind legal transplants comes from the mainly functionalist perspective that “when legal institutions are confronted with problems, they look for better solutions elsewhere” (Frankenberg, 2022: p. 336).

Nonetheless, it is relevant to point out that there are controversies surrounding the topic of legal transplants. The view that legal transplants are the root of societies’ legal systems is not ubiquitous, so much so that some comparative law scholars believe legal transplants are in fact impossible. This approach understands that legal transplants cannot happen, since when an original rule crosses boundaries, it will have its meaning changed and unavoidably be reduced to “bare-propositional-statements”, that is, meaningless forms of words. Those who advocate against legal transplants express that law is a culturally-situated phenomena, and as such, the idea of legal transplants fails to acknowledge that rules result from divergent and conflicting interests specific to each society (Legrand, 1997).

Furthermore, even among legal scholars who believe that law does travel between countries exists an uncertainty about the correct terminology of the field, which “reflects the open character of the discussion about the law’s mobility (Graziadei, 2006: p. 3). Günter Frankenberg proposes the term “legal transfer” as they do not resemble organ transplants, since:

“legal transfer’ alerts comparatists to a problematic phenomenon (Graziadei 2006) that may be ‘extremely common’ but is anything but ‘socially easy’ (Watson 1978, pp. 7, 96). Moreover, it supports a more contextual approach that focuses on comparison as practice and a theory of law constituting it as a cultural artefact (Frankenberg 2016). By choosing this term, one dismisses the ‘naturalism’ of legal transplants as well as the solipsism of the notion of a ‘nomadic character of rules’ (Legrand 1997). Directing the attention on what happens when transfer happens at least implicitly favours the analysis of differences (Legrand 1997; Monateri 2000; Samuel 2007) rather than the search for similarities (Zweigert and Kötz 1998), and moves away from thinking in terms of congruence and convergence or looking for ‘common cores’ or ‘universal’ categories, theories, and histories of law. Finally, transfer captures the commodity structure of the exported/imported legal information as a product that comes with standardization.” (Frankenberg, 2022: p. 22).

In Frankenberg’s view, legal transfers operate as part of world-making and when the export and import of legal information happens, the information that arrives at a new setting isn’t in its pristine form or design, but is always already processed intensely on the way. As professors Frankenberg and Fernanda Nicola explain, the idea of a legal transplant conceals the fact that when an item migrates, “the translation and application of legal information in a new environment invariably presupposes intense modification” (Frankenberg, 2024: p. 22). Therefore,

they argue that transfers are neither socially easy (as pointed out by Watson), nor impossible (as described by Legrand), but they actually demonstrate the complexity of law's cross-cultural travels, requiring close attention to contexts and cultures, as well as risks and side effects (Frankenberg, 2024: p. 22).

2.2. Why Legal Concepts and Institutions Are Predominantly Transplanted from the Global North to the Global South

Although, as stated by the authors mentioned above, legal transplants have become a relevant part of our world making, it is necessary to address the fact that legal institutions are majorly exported from countries of the Global North and imported by countries of the Global South (Bonilla, 2018). The Global South refers to the regions outside of Europe and North America, and is made up of socially, economically, and politically underdeveloped and developing countries. When it comes to their legal systems, the assumptions aren't much different.

According to professor Michele Graziadei, a variety of factors can cause legal change, including the desire to follow prestigious models. In the past, one of the main forms of legal change was through the imposition of foreign legal models after military conquest or expansions, but he also illustrates that "the desire to have what others have, especially if it is deemed superior, may be enough to trigger transplants or receptions" (Graziadei, 2006: p. 16). Along these lines, the receptive countries are willingly adhering to different cultural models. Graziadei concludes that, while the originators of the invention might be unaware, the prestigious model can influence the development of the law in the receptive country "by shaping legal ideas, institutions, categories, and rules" (Graziadei, 2006: p. 16).

Colombian professor Daniel Bonilla Maldonado explains that Global North countries are usually seen as having a rich context for the production of legal knowledge, with rich tradition and solid legal and political institutions. Global North countries have high academic capital, high-quality academic products, rich academic institutions (such as the Ivy League schools), and experience in the use of legal knowledge (Bonilla, 2018: p. 59). On the other hand, Global South countries tend to be seen as having poor context for the production of legal knowledge and a nonexistent legal tradition, and thus, their legal institutions are fragile and unstable (Bonilla, 2018: p. 58). As opposed to Global North countries and partly because of its colonial past, the Global South denotes countries that are "politically unstable, relatively poor, militarily weak, or at least not as strong as Global North countries, and culturally subordinate" (Bonilla, 2018: p. 33).

Hence, the prestige of North American and European legal institutions, deemed to be superior to the law of Global South countries, is associated with social stratification and can be understood as a variety of power (Graziadei, 2006: p. 16). In this sense, we currently face a situation of unequal distribution of power when it comes to creating and exchanging legal knowledge, in which an unidirectional model of exchange prevails: the Global North understands they have the capacity of creating, exporting, and using legal knowledge, while the Global South can only

“disseminate, reproduce, or apply locally the knowledge created elsewhere” (Bonilla, 2018: pp. 32, 33, 58, 59).

Comparative law encourages the study of “other peoples’ normative practices and ideas, their visions of a well-ordered community and the instruments and institutions they have designed to establish and sustain such order” (Frankenberg, 1985: p. 412). However, by understanding the other, we are also able to understand ourselves. Others’ perspectives can change the way we see ourselves. The Global North sees their legal systems as flawless. They assume that any legal knowledge produced in their territory and by one of their lawyers is instantly worthy of respect, recognition, and positive qualifications, regardless of its actual quality (Bonilla, 2013). Moreover, Global North countries also believe that their development process has also been favored by the qualities of their legal system and thus, the exportation of their norms and rules could contribute to the development of countries in the Global South. When this perspective is presented to countries of the Global South, one could assume they are persuaded to believe their own legal systems aren’t enough, and that they should constantly be looking up to the Global North’s law for inspiration, in an effort to reach a higher status.

Particularly in the Latin American scenario, there is a common perception that the region’s law is a “constant and irrepressible image of failure” (Esquirol, 2008: p. 85). Jorge L. Esquirol argues that this representation of Latin American law as a failure is a fiction that denies the value and legitimacy of state laws and institutions. There is an assumption that, compared to elsewhere, in Latin America “the gap between book law and action law is wider; the legal culture and local culture is more distant; the official actors are more corrupt; the rules are more inefficient” (Esquirol, 2008: p. 85), and although some of the critiques might be appropriate in certain situations, the cumulative repetition of these assumptions creates a common acceptance, even by Latin American countries themselves, of the dysfunction of their law. This failure discourse is so widely echoed that Latin Americans tend to hold their national law with little regard.

In this context, the success of legislation from a Global South country is rarely recognized by representatives of the Global North. One of the most prominent examples concerns the Brazilian Internet Civil Framework (Law No. 12,965/2014 or Marco Civil da Internet—MCI, in Portuguese). When the MCI was enacted in 2014, it was internationally recognized, including by North-American Internet organizations, for being a groundbreaking regulation on the rights of Internet users, helping promote freedom of expression on the internet in Brazil (IRIS.BH, 2017). Although nowadays there are discussions about changing the MCI’s main provisions, the project was highly praised by prominent figures in the Internet’s history, such as Sir Tim Berners-Lee, inventor of the World Wide Web, who stated that “Marco Civil has been built by its users—the groundbreaking, inclusive and participatory process has resulted in a policy that balances the rights and responsibilities of the individuals, governments and corporations who use the Internet” (Web Foundation, 2014a).

Yet, MCI's example is an exception. The law reforms in Latin America supported by the United States (U.S.) and other law and development institutions contribute to the reinforcement and normalization of the failure narrative. In the majority of times, the "solution" for the failed law is to reform the existing arrangements by U.S. or internationally supported alternatives, marked by the reflexive assumption of superiority of U.S. and European law. Legal transplants represent part of Latin America's history, as the majority of the region's positive law has been borrowed from European sources (Esquirol, 2008: p. 85).

The unequal distribution of power to create and exchange legal knowledge between the Global North and South countries directly influences how others see ourselves and how we see our own selves. For all these reasons, it is understood that the legal knowledge of the Global South countries can only be applied to their own borders. Due to their very specific realities, the law of the Global South can't be generalized and therefore isn't reproducible in countries of the Global North. Contrarily, the law of the Global North is viewed as universally relevant, meaning that other countries might find it useful and inspiring.

Therefore, countries of the Global North believe that they don't need to look at other countries, mainly those located in the Global South, to find legal solutions to address their political problems. Consequently, the tendency is that legal transplants happen from developed to developing countries, and the Global South ends with legal theory, doctrine, and practices that are more or less faithful copies of Global North law (Bonilla, 2018: p. 75). As a consequence, the law of Latin America is often seen both as a failure and a producer of "bad transplants", given that it is disconnected from the social norms and legal professionals in the region's countries. And, as pointed out by Watson, often those responsible for borrowing an idea have no direct experience of how well the rule works in practice (Watson, 1978: p. 315).

Given this context, it is also pertinent to address that over the decades there has been change in the direction of legal transplants in the west, however, the exporters of legal knowledge are always either Europe or the U.S. Ugo Mattei has presented the notion that France and Germany were the leaders during the expansion of the civil law tradition in the world. According to Mattei, a legal system is considered to be leading when it is "considered, discussed, copied or adapted in a larger number of other systems than any other legal system at that historical moment". He argues that, starting in the 1930s, the winds shifted in the Western world, and the U.S. started to gain more attention than Europe in various areas of law (Mattei, 1994: pp. 201, 204).

Similarly, Duncan Kennedy's theory of the "Three Globalizations of Law and Legal Thought" argues that until the 1930s, "legal development was heavily determined by what was happening in Germany and later in France" (Kennedy, 2006: pp. 23-24) and after this period the U.S. started to have influence over these countries. As such, Kennedy explains that between 1850 to 1900, German legal thought was hegemonic and from 1900 to the 1930s, French legal thought was predominant.

After 1950, the influence of the U.S. became manifest (Kennedy, 2006: pp. 23-24). Hence, there has been change in the direction of legal transplants in the Western world in the past, but the leadership has always been from either Europe or the U.S., and never from a Global South country.

3. Regulating the Digital Economy: The Transfer Direction from the EU to Brazil

The Brussels Effect: How Europe Is Regulating the Digital Economy

Nowadays, the EU is successfully exporting the influence of its legal institutions and standards to the rest of the world across multiple areas of law, and this time without the need for imposition and colonization. Author Anu Bradford explains that the EU is capable of declaring regulations that shape today's global environment, and, consequently, raise world standards in several sectors of society (Bradford, 2020: p. 2).

Bradford argues that through a “unilateral regulatory globalization” (Bradford, 2020: p. 2), the rules and regulations that emerge from Brussels, where the headquarters of the EU are located, have penetrated a variety of aspects of economic life inside and outside of Europe, a phenomenon she named as “Brussels Effect”. Bradford explains that the EU has become the predominant exporter of norms given to the fact that it has the largest internal market and very strong regulatory institutions. This encourages corporations to adjust their business practices in order to be in compliance with the strict European regulations, thus adhering to a single global standard (Bradford, 2020: p. 14) and facilitating international trade.

To no surprise, the Brussels Effect tends to follow the same North-South direction as legal transplants. This is because, in several instances, the U.S. is reluctant to apply national strict regulations in areas in which the EU was the precursor. Bradford reinforces that presently the EU has been adopting increasingly tighter standards of protection for consumers and the environment, which the U.S. has failed to follow. This mainly comes from the fact that, unlike the EU, the U.S. is more sensitive to the costs of regulatory action, and in order to justify regulatory intervention, there must first be a risk quantification and a cost-benefit analysis (Bradford, 2020: p. 14). One of the main examples that illustrates the different regulatory approach between the U.S. and the EU concerns AI. In the EU, the AI Act, which establishes a risk-based regulatory model, results from a long process of discussion and negotiation. While in the U.S., the Executive Order 14110 on “Safe, Secure, and Trustworthy Artificial Intelligence” was issued as a set of recommendations, incentives and investments in AI. Thus, most of the time developing countries are the ones racing to follow the EU's regulatory footsteps. Along these lines, in the last few years, Brazil has been one of the main countries following the EU's regulatory steps, especially when it concerns digital challenges.

In this sense, the unbalance in the new digital ecosystem and, as explained by Bradford, “the risks and potentially harmful effects associated with the use of these

digital tools and with tech companies' vast economic power and social impact" (Bradford, 2023: p. 5) has demonstrated the need for state intervention through regulation. Most of the time, the EU, as one of the dominant digital powers of the world, is the first regulator to put it into practice with the intention to reclaim control over the industry, before being followed by other countries (Bradford, 2023: pp. 6, 326).

The EU's regulatory model for the digital economy is considered as a "rights-driven" model, according to which "regulatory intervention is needed to uphold the fundamental rights of individuals,³ preserve the democratic structures of society, and ensure a fair distribution of the benefits from the digital economy" (Bradford, 2023: p. 9). Thus, by creating regulatory mechanisms to be followed by tech companies, the EU intends to protect the rights they see as the foundations of a liberal democratic society, establishing a balance between the right to free speech and other fundamental rights of digital citizens (Bradford, 2023: pp. 9-10).

When it comes specifically to the digital economy, the U.S., in contrast to the EU, is especially reluctant to adopt aggressive regulations that affect the American tech companies in fear of weakening the country's technological supremacy. While the EU doesn't have a vibrant tech industry of its own, it has been recognized as the most powerful regulator of the digital economy, with the goal of protecting European citizens from exploitation by U.S. tech companies (Bradford, 2023: p. 12). Yet, the EU is not only interested in its capacity to curtail U.S. companies' market power, but also in its ability to shape the global digital order and expand its international influence by exporting the rights-driven regulatory model and the rights deemed to be fundamental in Europe to other countries (Bradford, 2023: p. 17).

In this sense, Bradford explains that the Brussels Effect frames digital regulation around the world in two ways: (i) by shaping tech companies' business practices (known as "de facto" Brussels Effect), as these companies frequently choose to follow the strictest regulatory standard to ensure regulatory compliance worldwide; and (ii) by encouraging foreign governments to adopt EU-style regulations ("de jure" Brussels Effect) (Bradford, 2023: p. 325).

Over the last few years, the European Commission has expressed several times that digital transformation is one of the EU's priorities for 2019-2024, with the goal of making Europe fit for the digital age (European Commission, 2024a). In this sense, the EU has adopted a digital strategy in order to "strengthen its digital sovereignty and set standards, rather than follow standards set by others" (European Parliament, 2021) with a clear focus on data, technology, and infrastructure (European Commission, 2024b).

³It is worth mentioning that, according to Pietro Dunn and Giovanni De Gregorio, the AI Act is not strictly based on conferring rights to European citizens. According to the authors, the AI Act is framed to build governance in companies that develop and use AI tools, structuring it through a risk identification and classification methodology. However, even though it is governance-based legislation, it aims to ensure that the adoption of the AI Act's model can ensure the protection of fundamental rights within the EU. Available at: https://ceur-ws.org/Vol-3221/IAIL_paper7.pdf.

As part of its digital strategy, in 2020 the European Commission released its agenda for shaping Europe's digital future, which will focus on three key objectives: (i) technology that works for people; (ii) a fair and competitive economy; and (iii) an open, democratic and sustainable society (European Commission, 2024c). Moreover, as a global leader, the EU stated it would (i) aim to become a global role model for the digital economy; (ii) support developing economies in going digital; and (iii) develop digital standards and promote them internationally (European Commission, 2020).

Furthermore, in March 2021, the European Commission presented "Europe's Digital Decade" policy program, which guides Europe's digital transformation by setting concrete targets and goals for 2030. The policy aims to achieve the EU's ambition of pursuing "digital policies that empower people and businesses to seize a human centered, sustainable and more prosperous digital future". To do so, they propose a governance structure made up of four cardinal points: (i) digitally skilled citizens and highly skilled digital professionals; (ii) secure, performant and sustainable digital infrastructures; (iii) digital transformation of businesses; and (iv) digitalisation of public services (European Commission, 2021). Thus, as pointed out by Bradford, the EU's intention of shaping policies that will strengthen its capacities in regulating new technologies, and exporting its standards around the world, is clear.

Bradford argues that given the global nature of the digital economy, the current leading regulatory models—the U.S.'s market-driven model, China's state-driven model, and the EU's rights-driven model—extend "across jurisdictions, impacting foreign societies and shaping lives of foreign individuals" (Bradford, 2023: p. 11). As aforementioned, when it comes to regulation of themes concerning information technology, in the past few years many Brazilian legislators have relied on the European experience, proposing heavily influenced Bills.

In spite of that, the specific characteristics of the digital ecosystem reveal other factors for the importation of the EU's regulatory model. This includes the increasing rejection, by countries around the world and even U.S. citizens, of the U.S. free-market and free-speech approach, combined with the rise of concerns regarding the benefits of an unregulated digital marketplace. This leads democracies to pursue the EU's model instead of China's, since the latter is oftentimes linked to censorship and constant surveillance. On the other hand, the set of values associated with the EU's model—fundamental rights, democracy and fairness—tend to be a bigger attraction for other democracies to align their digital economies with the European (Bradford, 2023: pp. 21-22).

Furthermore, Brazil, like Europe, does not have a prominent tech industry, and both Brazilian and European tech companies fail to compete with the U.S. and China's tech giants. Additionally, a significant portion of the Brazilian legal elite chooses to take post graduate courses in Europe and many Brazilian universities are still strongly influenced by European standards, which could also explain why Brazil tends to lead towards the European regulatory model when compared to

the U.S. and China.

Under these circumstances, Brazil has become known for quickly transferring the EU's regulatory discussions regarding the digital economy, as usually merely months after the introduction of the new regulation in Europe, the Brazilian National Congress and Brazilian regulators start debating the need to adopt similar nationwide regulations too. Over the last few years, they have proposed several draft laws with very similar (but not identical, as will be demonstrated) content to the EU regulations on a wide variety of topics concerning the digital environment, including protection of data privacy, regulation of social media and content moderation, regulation of digital markets from a competition perspective, and regulation of AI systems.

This paper will address some of these key examples in recent years of the Brussels Effect in Brazil's digital environment, thus discussing how the Brazilian regulators were inspired by the European debates concerning the regulation of the digital economy. Yet, when it comes to regulating the internet, Brazil hasn't always been inspired by the EU. In fact, Brazil can be considered as one of the protagonists in the early days of internet regulation.

4. A Comparative Analysis: Recent Regulations Governing the Digital Environment

4.1. Brazil as an Original Creator

In the early days of internet regulation in Brazil, the country was mainly influenced by the discussions that were taking place in the United States concerning the digital ecosystem. In the early 2000s, the internet's popularization around the world led to the perception that its increased use by companies, governments, civil society organizations and a growing number of people posed new questions and challenges regarding the online protection of civil and political rights. In this context, Brazilian society started to notice the importance of establishing minimum and essential conditions for the internet to remain based on the principle of free and open use and also to allow for continuous innovation, economic and political development and the emergence of a culturally vibrant society (CGI.br, 2014).

For this reason, in 2009 an open and collaborative effort to build Brazil's first internet legislation was launched through online discussion forums, so different stakeholders could share their opinions on the use of the internet in the country. Based on comments received from members of the public, companies, government agencies, universities and organizations, a preliminary draft of the law was prepared and introduced to the National Congress in 2011, with the goal of defining principles, guarantees, rights and duties for the use of the internet in Brazil (Rezende & De Lima, 2015). In April 2014, the MCI was sanctioned, so the use of the internet in Brazil was now subject to legal principles and guarantees.

The MCI was created to guarantee the right to exercise citizenship within digital media, as well as to ensure the rights to diversity and freedom of expression on the internet. The law's fundamental aspects are the guarantee of freedom of

expression, the inviolability of privacy, and neutrality in the use of the internet. In this regard, besides providing for the foundations, principles and goals of the internet use in Brazil, the MCI also addresses the relationship between Internet Service Providers (ISP) and Content Application Providers (CAP), covering issues such as net neutrality, protection of connectivity and access records, protection of personal data and private communications, and liability for damages arising from content generated by third parties.

The legislation put Brazil at the forefront of debates on internet regulation around the world, leading the country to occupy a prominent position for its multi sectoral governance organization and for creating a regulatory framework that defines the key principles of a free and open internet, as well as the rules for protecting users (CGI.br, 2014). At the time of its sanctioning, MCI was recognized as an innovative legislation and an international benchmark, especially because the law was a pioneer in dealing with net neutrality, protection of privacy and personal data, and liability systems for content created in digital media (Senado Notícias, 2024b).

Regarding net neutrality, it is a no discrimination principle that guarantees that all internet traffic will be treated equally. In other words, when managing data traffic, ISPs must provide equal treatment, which includes speed and access, to all data on the internet, regardless of content, user, platform, application or device (Kenton, 2023). While Brazil was not the first country to codify the net neutrality principle, MCI established that:

Art. 09 The party responsible for the transmission, switching or routing has the duty to process, on an isonomic basis, any data packages, regardless of content, origin and destination, service, terminal or application (emphasis added).

The discussions surrounding net neutrality started in the U.S. in the early 2000s, with the advent of broadband internet connections. The net neutrality principle comes from a demand mainly from U.S. tech companies, which want their content to traffic through all networks, so consumers can easily access the content that they want in all of the digital platforms, instead of allowing ISPs to freely discriminate, block or throttle content for their own economic advantage.

In order to promote net neutrality, the Federal Communications Commission (FCC), the U.S.'s telecommunications regulatory agency, adopted a policy statement in 2005 claiming that "consumers are entitled to lawful internet content, applications, and services of their choice" (Linebaugh, 2022: p. 2). However, in 2010, the U.S. Court of Appeals for the District of Columbia Circuit rejected the FCC's effort to enforce this policy statement, which led the FCC to issue a new order to adopt binding rules on the open internet, which prohibited broadband internet access service providers from blocking or discriminating against lawful internet traffic, services, or devices. Yet, in 2014 the U.S. Court of Appeals for the District of Columbia Circuit once again rejected the FCC's determination, and overturned the anti-discrimination and blocking rules (Linebaugh, 2022: p. 2).

Thus, by the time of MCI's approval, the implementation of net neutrality in the U.S. was still highly controversial. It wasn't until 2015, that is, after MCI was enacted, that the FCC adopted the Open Internet Order, which was upheld by the U.S. Court of Appeals for the District of Columbia Circuit. The Open Internet Order imposed three rules to foster net neutrality by prohibiting providers from:

- (i) "blocking" lawful content, applications, services, or non-harmful devices;
- (ii) "throttling" (i.e., impairing or degrading) lawful internet traffic on the basis of content, applications, services, or non-harmful devices; and (iii) engaging in "paid prioritization", defined as favoring some internet traffic over others in exchange for consideration.

In Europe, the European Parliament, Commission and Council only agreed on the rules needed to guarantee an open internet in November of 2015, when the Regulation (EU) 2015/2120 was passed, laying down measures concerning open internet access⁴. Under the European rules, ISPs are prohibited from blocking or slowing down internet traffic, except in situations when it is necessary (Berec, 2023). Thus, while it is undeniable that the Brussels Effect is present in the Brazilian regulation of the digital environment, the EU was not always the first to create regulatory standards.

Not only that, but through the MCI, Brazil was a pioneer in creating a brand new system of judicial civil liability for internet intermediaries. According to Article 18 of MCI, ISPs will not be held liable for damages that arise from content generated by third parties, while Article 19 provides that intermediary platforms, that is, digital platforms or application providers, "will only be liable if they fail to comply with a court order requesting the removal of certain content" (Affonso et al., 2017: p. 93). In this sense, Article 19 of MCI determines that:

Art. 19. In order to ensure freedom of expression and prevent censorship, Internet application providers may only be held civilly liable for damage resulting from content generated by third parties if, after specific judicial order, the provider fails to take action to make the content identified as offensive unavailable on its service by the stipulated deadline, subject to the technical limitations of its service and any legal provisions to the contrary.

In this perspective, the MCI guarantees an immunity for CAPs, since they will not be held liable for user generated content even if they are notified by users and made aware of illegal content being shared in their platform. The MCI recognizes that the Judiciary branch has the authority to determine whether a content posted by a third party in a digital platform is illicit or not, consequently encouraging the claim to be brought before Brazilian courts (Affonso et al., 2017: p. 94). Thus,

⁴European Parliament and Council. Regulation (EU) 2015/2120. Laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012. Official Journal of the European Union, Luxembourg, 2015. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02015R2120-20181220>, Access on Nov. 26, 2023.

judges have the competence to interpret the legislation and decide whether a content should be removed or not, and the intermediary platform does not have to make this assessment. This does not mean, however, that CAPs can't establish their own requirements and rules for content removal after damage has been caused by content posted in their platforms or that has infringed their terms of use (Affonso et al., 2017: p. 93).

One of the main criticisms about this provision regards the long time it takes for a lawsuit to be brought before the Judiciary and for a decision to be made, especially when compared to the quick speed that content travels nowadays, as a post can be shared and reposted in the internet in merely seconds (Affonso et al., 2017: p. 95). Notwithstanding, the MCI defines two exceptions to its liability regime. According to the law, in the event of copyright infringement or revenge porn material, the intermediary might be held liable, even if there is no court order, as long as the platform is notified about the infringing content, but still does not remove it.

Concerning revenge porn, Article 21 of the MCI establishes what is known as a “notice and takedown” system, according to which internet content providers will be held subsidiarily liable for the violation of privacy resulting from the disclosure, without the authorization of its participants, of images, videos or other materials containing scenes of nudity or sexual acts of a private nature when, after being notified by the participant or their legal representative, the platform fails to diligently make the content unavailable, within the scope and technical limits of its service.

Thus, Brazil innovated the regulation of the internet by determining that digital platforms can only be held liable if they do not follow a court order to remove illegal content from third parties that has been made available on the internet. Still, MCI's civil liability regime has been compared to the U.S.'s framework concerning intermediaries' liability with respect to user-generated content, as many argue that the Brazilian approach is very similar to what has been set out in the U.S.'s Federal Communication Decency Act (CDA), from 1996.

This is due to Section 230 of the CDA, which “provides limited federal immunity to providers and users of interactive computer services” (Brannon et al., 2024: p. 2). This means that providers and users will not be held liable for information provided by other people, but they are not immune from information that they have authored or for activities unrelated to third-party content. At the time, the U.S. Congress' aim was to “allow online services to moderate content on their platforms in good faith, removing harmful or illegal content while still providing a forum for free speech and a diversity of opinions” (Johnson et al., 2022). To this extent, Section 230 (c) of the CDA states that:

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Yet, the CDA also establishes statutory exceptions for Section 230's safe harbor, that is, situations that fall outside of its scope. According to the Act, nothing in Section 230 shall have effect on (i) federal criminal law, (ii) intellectual property law, (iii) any state law consistent with Section 230, (iv) privacy laws applicable to electronic communications, and (v) sex trafficking law (Brannon et al., 2024).

Unlike Article 21 of the MCI, which refers to the exception of revenge porn, Section 230 of the CDA does not provide for a “notice and takedown” system, since it shields digital platform from liability by determining that they can freely moderate content, while only the users who create and post the defamatory content might be held liable. This guarantees a lower market entry barrier for digital platforms, as there is a low liability risk associated with hosting user generated content. In this sense, many believe that Section 230 has enabled the business models of the digital platforms we know today, contributing to the rise of technology giants that nowadays prevail in the digital public sphere (Rozenstein, 2024).

The “notice and takedown” system, on the other hand, places a higher responsibility on digital platforms, as they must remove content after receiving a notification of infraction, in a timely manner (Londoño, 2021). Over the years, the “notice and takedown” system has been criticized mainly by free speech organizations, who claim it will lead to an overly precautionary approach to content moderation, suppressing innovation and speech online (Londoño, 2021). The claim is that a notice-based liability can result in platforms removing legitimate content, as they would be exposed to potential liability everytime they received a notice of infringing content, thus they would be encouraged to simply remove the content upon notification, whether it was defamatory or not. Hence, noticed-based liability results in a chilling effect on the freedom of speech, caused by the fear of a possible future effect (Rozenstein, 2024).

In this context, the Brazilian liability system for intermediary platforms has been internationally praised by experts for favoring freedom of expression and access to information on the internet. Besides the risks associated with models that pressure internet intermediaries to promote the removal of content generated by third parties before a judicial assessment, some argue that the private nature of the intermediaries prevents them from acting impartially and legitimately in the

assessment of content removal, and can lead to economic interests prevailing to the detriment of freedom of expression and access to information for users. Thus, many believe that there are well-founded reasons for the Judiciary branch to examine and decide on the legality or illegality of certain content (Oliva, 2019).

Therefore, Brazil was influenced by the U.S. liability model for digital platforms regarding user generated content, as both systems provide immunity for intermediaries, favoring freedom of expression. Yet, while in the U.S. platforms have “full” immunity, Brazil innovated this discussion by allowing the liability of intermediaries only after the legitimacy of requests for content removal has been assessed by the Judiciary branch.

Accordingly, in the early days of internet regulation, Brazil was recognized as a leading player in the fight for changes in internet governance, especially after hosting the NETMundial and being at the forefront for regulating the rights of citizens online (Agência Brasil, 2014). At the time of MCI’s approval, Sir Tim Berners-Lee, gave a statement in support of Brazil’s initiative, saying that “by passing this Bill, Brazil will cement its proud reputation as a world leader on democracy and social progress and will help to usher in a new era” (Web Foundation, 2014a).

Therefore, it is clear that, in the past, Brazil was acknowledged for passing a legislation that managed to address a complex debate that other countries were not regulating yet, resulting in experts in the field to call “on other countries to follow Brazil’s lead and enshrine in law the rights of all to a free and open internet” (Web Foundation, 2014b). At the time, Brazil was primarily influenced by the U.S. approach for regulating the digital economy, as attested by the MCI’s rulings on net neutrality and liability for intermediary platforms. Thus, in the beginning of the internet’s rise, Brazil pursued the U.S. regulatory model, which is mainly characterized by the importance of protecting the business models of internet companies and users’ free speech online. Yet, recently Brazil’s search for influence in regulating digital services has shifted from the U.S. to Europe, as showcased by the example of the LGPD, which was heavily influenced by the EU regulation.

4.2. The GDPR in the EU and the LGPD in Brazil

The prime example of the Brussels Effect across the world refers to the protection of data privacy. In 2016, the European Parliament passed the General Data Protection Regulation (GDPR) which became known as the “toughest privacy and security law in the world”⁵ (Wolford, 2023). Confirming the EU’s rights-driven regulatory model for the digital economy, one of the main reasons behind the GDPR is the protection of the fundamental right to information self-determination, which refers to individuals’ right to determine what information about themselves will be disclosed to others and the purposes for using such information

⁵European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, Luxembourg, 2016. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Access on Nov. 1, 2024.

(Kocharyan, 2024). The GDPR quickly became the model for privacy compliance programs across the globe, with lots of countries adopting privacy rules similar to the European model. The U.S., however, has been an exception, as to this day the country does not have a general applicable federal law covering all industries and data (Bradford, 2020).

In 2018, the preparations for GDPR's entry into force mobilized companies, governments, civil society and members of the academia, since numerous practices had to be reviewed to adapt to the new European model, generating important extraterritorial impacts. The GDPR's innovations, such as extended rights for personal data subjects and new responsibilities for companies, effectively put the debate on personal data protection at the center of attention in Brazil (Affonso et al., 2020: p. 44), which was one of the first countries to pursue a regulation that faithfully emulates the European law, as part of the "de jure" Brussels Effect. The LGPD changed the regulatory discussions in Brazil, and the country was suddenly looking at the EU for inspiration on regulating the digital environment.

In the same year, the Brazilian National Congress passed Law No 13,709/2018, also known as the General Data Protection Law (*Lei Geral de Proteção de Dados*—LGPD, in Portuguese), which regulates the treatment of personal data in the country's territory. Although Brazil's regulatory framework, such as MCI, already provided for certain personal data protections, LGPD is the first national law specific on the subject (Affonso et al., 2020: p. 45), thus strengthening data subjects' rights in the country.

Although the EU can be credited for advancing the discussions about regulating the protection of personal data, other countries, including Latin American ones, already had nationwide data protection laws in effect even before the GDPR was proposed in the European Parliament. For instance, Argentina's National Congress introduced the country's general personal data protection system in 2000, through Law No. 25,326/2000⁶. The Law's purpose is to comprehensively protect personal data kept in records, to guarantee the right to honor and privacy of individuals. Subsequently, Decree No. 1,558/2001 and Decree No. 1,160/2010 laid down additional rules for the implementation of the law. In 2003, Argentina was the first Latin American country to be recognized by the EU for having an "adequate" level of data protection. Likewise, Colombia, Chile and Peru also had federal data protection legislations in place before 2013 (Baptista Luz, 2022).

It is worth mentioning that, at the time, several Latin American countries were influenced by the European Union's Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement

⁶ARGENTINA. Ley 25.326 (Protección de los Datos Personales). Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Buenos Aires, Oct. 30, 2000. Available at: [https://www.unterseccionalroca.org.ar/imagenes/documentos/leg/Ley%2025326%20\(PROTECCION%20DE%20LOS%20DATOS%20PERSONALES\).pdf](https://www.unterseccionalroca.org.ar/imagenes/documentos/leg/Ley%2025326%20(PROTECCION%20DE%20LOS%20DATOS%20PERSONALES).pdf). Access on Oct. 07, 2024.

of such data⁷. Among others, the Directive sought to harmonise the protection of fundamental rights and freedoms of people in respect of data processing activities and to ensure the free flow of personal data between Member States. In addition, Spain's first data protection law, Organic Law 5/1992 (LORTAD), which regulated automated processing of personal data and defined the basic principles and recognised the legal protection of the constitutional right (GDPRHUB, 2024), also served as inspiration to Latin American countries. The cultural proximity between Spain and its former colonies and linguistic ease may also have facilitated the process of creating personal data protection laws in Latin America.

However, Brazil was not inspired by its neighboring countries and did not become one of the first countries in the continent to ratify a national data protection law. Yet, for the reasons explained in the previous chapters, discussions in Brazil regarding the topic only started to gain more traction after the GDPR was approved. The first Brazilian Bill on personal data protection was submitted in 2012, by Representative Milton Monti (Bill No. 4060/2012), which provided for the processing of personal data. At the time, the Representative's main reasoning for the proposal was the need for a law on the subject in the face of increasing digitalization of society. Although the proposal had some similarities with the Directive 95/46/EC, the Bill made no direct references to the European Directive.

The LGPD was heavily inspired by the GDPR, attested by the fact that at the time of its entry into force, companies that were already in compliance with the GDPR had "already done the bulk of the work necessary to comply with the LGPD" (Koch, 2023). For example, the GDPR and the LGPD share very similar goals and legal bases for defining personal data, broad definitions for personal data, and definitions for data subject rights (Koch, 2023), as well as are fairly consistent regarding personal, material and territorial scope (Data Guidance by One Trust and Baptista Luz Advogados, 2024: p. 4). The differences and similarities between the LGPD and the GDPR have been a topic of academic and professional discussions countless times since the LGPD's enactment. Thus, since the purpose of this paper is not to replicate these discussions, the comparison will focus on one specific aspect of the discussion, which refers to the appointment of the Data Protection Officer (DPO) in the regulations, since it illustrates how the Brussels Effect in Brazil has the characteristics of a transfer given the local adaptation of the legal instrument, and it should not be seen as a legal transplant.

Both laws determine the appointment of a DPO, and although the GDPR doesn't provide its definition, Brazil imported the idea of a DPO in the LGPD and introduced this concept in the country. Article 5, VIII, of the LGPD defines it as "person appointed by the controller and processor to act as a communication channel between the controller, the data subjects and the Brazilian Data Protection Authority (ANPD)".

⁷European Parliament and Council. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, Luxembourg, 1995. Available at: <https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng>. Access on Feb. 9, 2025.

Under Article 37 of the GDPR, controllers and processors must designate a DPO in specific circumstances, which will depend on the “core processing activities which are defined as those essential to achieving the company’s goals” (Inter-soft Consulting, 2024). Under the LGPD, only controllers must appoint a DPO, and no specific situations are set out. Thus, at first glance, all controllers need to assign one (Data Guidance by One Trust and Baptista Luz Advogados, 2024: p. 5), although, as per Article, §3, of the LGPD, ANPD can establish scenarios in which the need to indicate a DPO is waived, depending on the nature and size of the entity or the volume of data processing operations.⁸

Even though the concepts of DPO are very similar in both laws, when it comes to the DPO’s attributed tasks, the LGPD didn’t exactly follow the GDPR’s footsteps. By analyzing the Table below (Table 1), which compares the duties that were assigned to the DPO, it is possible to conclude that the Brazilian regulator opted to assign less overall responsibilities to the DPO when compared to the European model. Not only that, but a careful reading shows that their duties are quite different.

It is also important to note that the GDPR’s list isn’t exhaustive, as it provides for the minimum tasks to be followed by the DPO. Article 38(6) of the GDPR states that the DPO may fulfill other tasks and duties, and even hold other roles within the organization (Dpo Centre, 2023), as long as they do not result in a conflict of interests. As for the Brazilian scenario, the LGPD expresses that the DPO can perform other duties determined by the controller, and Article 41, §3, states that the national authority may establish complementary rules on the definition and attributions of the DPO.

Hence, Brazilian regulators were clearly inspired by the GDPR to include the

Table 1. DPO’s attributed tasks in the GDPR and in the LGPD.

GDPR - Article 39	LGPD - Article 41, §2
To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;	Accept complaints and communications from data subjects, provide clarifications and adopt actions;
To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;	Receive communications from the national authority and take action;
To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;	Provide guidance to the organization’s employees and partners on the practices to be followed related to the protection of personal data;
To cooperate with the supervisory authority;	Perform other duties determined by the controller or established in complementary rules.
To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	

⁸It should be noted that ANPD’s Resolution No. 2/2022 eases the obligation for controllers to appoint a DPO. The Resolution sets criteria for waiving the requirement of appointing a DPO, while maintaining the need for every controller to have a communication channel with the ANPD.

DPO in the LGPD, given that this character did not previously exist in the national regulatory framework. However, they did not transplant the notion of a DPO, once, despite the similar concepts, the legal roles and characteristics of the DPO did not arrive in Brazil in its pristine form, but instead were modified and adapted to the local circumstances, as showcased by the the different “nature and scope of their role and responsibilities” (Data Guidance by One Trust and Baptista Luz Advogados, 2024: p. 33). Although the structures of the DPO are very much alike in both laws, in detail there are important differences that demonstrate Brazil’s concern to adapt the idea to its context.

In July 2024, ANPD approved Resolution No. 18/2024, which provides for the role of the DPO in Brazil, regulating Article 41, §3, of the LGPD. The new regulation addresses the appointment, characteristics and work of the DPO, expanding the activities and attributions that had been established beforehand in the LGPD. For instance, while controllers must appoint a DPO, it is now optional for processors to do so, but it will be considered as good practice for sanctioning purposes.

Concerning the DPO’s tasks, the regulation reinforced LGPD’s provisions and introduced complementary attributions of the DPO regarding (i) answering ANPD’s requests and (ii) providing guidance to the controller/processor in a series of activities. Table 2 compares the DPO’s assigned tasks by the GDPR and ANPD’s Resolution No. 18/2024, illustrating the expansion of the Brazilian DPO’s duties in the new regulation.

Table 2. DPO’s attributed tasks in the GDPR and in ANPD’s Resolution No. 18/2024.

GDPR	ANPD’s Resolution No. 18/2024
Article 39	Article 15
<p>The DPO shall have at least the following tasks:</p> <ul style="list-style-type: none">• To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;• To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;• To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;• To cooperate with the supervisory authority;• To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	<p>The DPO’s activities consist of:</p> <ul style="list-style-type: none">• Accept complaints and communications from data subjects, provide clarifications and adopt actions;• Receive communications from the national authority and take action;• Provide guidance to the organization’s employees and partners on the practices to be followed related to the protection of personal data;• Perform other duties determined by the controller or established in complementary rules. <p>Sole Paragraph. Upon receiving communications from the ANPD, the DPO must adopt the necessary measures to fulfill the request and provide the relevant information, which includes, among others, the following measures:</p> <ul style="list-style-type: none">• Internally forward the demand to the competent departments;• Provide the necessary guidance and assistance to the controller/processor; and• Expressly appoint the controller/processor’s representative before the ANPD for the purposes of acting in administrative proceedings, when this function is not performed by the DPO.

Continued

Article 16

It is also the DPO's responsibility to provide assistance and guidance to the controller / processor in the preparation, definition and implementation, as appropriate, of the following:

- Register and report security incidents;
- Register personal data processing operations;
- Personal Data Protection Impact Assessment;
- Internal mechanisms for supervising and mitigating risks related to the processing of personal data;
- Technical and administrative security measures to protect personal data from unauthorized access and accidental or unlawful destruction, loss, alteration, communication or any form of inappropriate or unlawful processing;
- Internal processes and policies that ensure compliance with LGPD and ANPD's regulations and guidelines;
- Contractual instruments governing issues related to the processing of personal data;
- International data transfers;
- Rules of good practice and governance and a privacy governance program;
- Products and services that adopt design standards compatible with the principles set out in the LGPD, including privacy by default and the limitation of the collection of personal data to the minimum necessary to fulfill its purposes; and
- Other activities and strategic decision-making regarding the processing of personal data.

ANPD's regulation aligns the work of the Brazilian DPO better with that of the European DPO. Now, similarly to the European DPO, the Brazilian DPO must also advise the controller on the data protection impact assessment and on the implementation of data protection regulations. Nonetheless, ANPD established even more attributions to the DPO than the GDPR, confirming, once again, that it is not copying the European legislation, but rather developed the original idea, providing greater legal and operational security for companies in Brazil.

Furthermore, ANPD's Resolution No. 18/2024 also addresses conflicts of interest involving the DPO, which hadn't been brought up by the LGPD. The Resolution defines "conflict of interest" as the "situation that may improperly compromise, influence or affect the objectivity and technical judgment in the performance of the DPO's duties" (free translation). Besides, the Resolution explains the situations that might characterize a conflict of interest, which includes the accumulation of the DPO's role with other activities that involve making strategic decisions about the processing of personal data by the controller.

In 2023, the Court of Justice of the European Union (CJEU) issued a preliminary ruling following a request submitted by the German Federal Labour Court about the application of Article 38(6) of the GDPR, since a possible conflict of

interest was said to have arisen⁹. The CJEU interpreted that a conflict of interest “may exist where a DPO is entrusted with other tasks or duties, which would result in him or her determining the objectives and methods of processing personal data on the part of the controller or its processor” (CJEU, 2023). In other words, “the DPO cannot be entrusted with performing tasks or duties which could impair the execution of the functions performed by the DPO” (CJEU, 2023).

Thus, it is evident that there are many similarities between the CJEU’s ruling and ANPD’s Resolution regarding the situations in which a conflict of interest involving the DPO’s role might arise. The Brazilian regulator was inspired by the European case law, but went a step further by creating an entire section in its Resolution regarding conflicts of interest involving the DPO, in which it sets, among others, the possibility of sanctioning in the event of conflict of interest and the measures to be adopted by the controller or processor if a conflict of interest arises.

Therefore, by determining that the processor might also appoint a DPO, expanding the duties of the DPO, and defining the circumstances in which a conflict of interests exist, the Brazilian regulation has brought the DPO’s role much closer to the European DPO, as established by the GDPR and the CJEU’s decision. This proves how the European influence in the Brazilian data protection landscape is very significant and subtle at the same time. As mentioned above, when it comes to the DPO, Brazil isn’t transplanting the European regulation, but instead it is just transferring the concept and applying it locally. Yet, by bringing the DPO’s characteristics closer to the European model, ANPD shows how the influence is so profound that the Brazilian regulator is strongly impacted by the European discussion.

4.3. The AI Act in the EU and AI Regulation in Brazil

The European Parliament’s most recent step towards its digital strategy was adopting the Artificial Intelligence Act, in March 2024¹⁰. A regulatory framework for AI was first proposed by the European Commission in April 2021, with the intention of making sure that the AI systems used in Europe are safe, transparent, traceable, non-discriminatory and environmentally friendly, in order to prevent harmful outcomes (European Parliament, 2023). By establishing “safety requirements that companies must meet before placing an AI product on the EU market”, (Pouget & Zuhdi, 2024) the EU aims to protect a series of fundamental rights, including the right to human dignity, non-discrimination, data protection, education,

⁹Court of Justice of the European Union. C-453/21 X-FAB Dresden GmbH & Co. KG v FC. Decision from Feb. 09, 2023. Available at:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=258249&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=366992>. Access on Oct. 09, 2024.

¹⁰European Parliament and Council. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, Luxembourg, 2024. Available at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>. Access on Nov. 1, 2024.

and consumer protection (Van Bael & Bellis, 2024).

Although the AI Act is known as “the first comprehensive regulation on AI by a major regulator anywhere” (EU AI ACT, 2024), the EU wasn’t the first digital market to set forth a regulation on AI. In October 2023, the U.S. government issued Executive Order 14110 on “Safe, Secure, and Trustworthy Artificial Intelligence”, which results from a government-wide effort to guide the responsible development and deployment of AI and, according to the government, to ensure that “America leads the way in seizing the promise and managing the risks of AI” (The White House, 2023). Even though the Executive Order has been recognized as an important step towards AI regulation worldwide, experts claim that its practical results are limited and it has few remarkable legal impacts, especially given that it was designed to provide a set of recommendations and measures to foster innovation in AI. It does not contain a regulatory framework that addresses potential conflicts created by the use of technology. In this sense, the Executive Order is a clear advancement in the U.S.’s intention to expand its leadership abroad, and mirrors the country’s political ambition to be at the forefront of the race to regulate AI (Bassini, 2024).

The Executive Order, as a presidential directive, is only binding to the addressed federal agencies and is not directly applied to the private sector. Thus, it aims to guide the federal government’s approach to AI governance by establishing eight policies and principles to be followed in order to promote the development of AI safely and responsibly, without details of specific regulations. However, much of the order still requires additional implementation through future legislative actions or regulations by the competent authorities (Casovan & Zweifel-Keegan, 2023).

Yet, the Executive Order’s limited enforceability reflects its intention to set broad guidelines and best practices to promote the government’s “comprehensive strategy for responsible innovation” (The White House, 2023). It aims to encourage voluntary compliance and industry-led standards, without imposing specific requirements (Petrosyan & Ataliotou, 2024), to foster AI innovation and competition, creating an environment for the U.S. to exploit AI’s full potential without hindering human rights and freedoms (Bassini, 2024). One could say that through Executive Order 14110, in conformity with its market-driven regulatory model, the U.S. is promoting technological progress with caution, as it is not regulating its tech companies too aggressively in fear of preventing innovation and weakening the U.S.’s battle for technology supremacy.

The EU, on the other hand, takes a different approach to regulate AI. The AI Act is a comprehensive legal structure which aims to create a single regulatory framework for all member states, providing for obligations, prohibitions and enforcement mechanisms for AI systems to comply with. According to the Act’s Article 1, the regulation lays down: (a) harmonized rules for the placing on the market, the putting into service and the use of AI systems in the EU; (b) prohibitions of certain AI practices; (c) specific requirements for high-risk AI systems and

obligations for operators of such systems; (d) harmonized transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content; and (e) rules on market monitoring and surveillance.

In this regard, the AI Act reflects a risk-based approach, setting obligations for providers of AI systems depending on their risk level, which are classified in four different categories: unacceptable risks (which are considered as a threat to people's safety, livelihood and rights, and as such, will be banned), high risks (which negatively affect users' safety, and are subject to specific requirements before they can be put on the market), limited risks (whose companies will have to comply with transparency requirements, which includes disclosing that the content was generated by AI), and minimal risks (which are largely left unregulated) (European Commission, 2024c).

As per the EU's official website for the AI Act, "like the GDPR, the EU AI Act could become a global standard, determining to what extent AI has a positive rather than negative effect on your life wherever you may be" (EU AI ACT, 2024). As such, to prove that the EU's AI regulation is already making waves internationally, the website mentions Brazil's Bill No 21/2020, which creates a legal framework for AI in the country (EU AI ACT, 2024).

Bill No 21/2020 was first introduced in the House of Representatives in February 2020, that is, before the AI Act draft was presented by the European Commission, with the purpose of establishing foundations, principles and guidelines for the development and application of AI in Brazil. The first version of the Bill was very broad, providing for (i) the foundations for the use of AI in Brazil; (ii) the objectives to be achieved with the use of AI; (iii) the principles for the responsible use of AI; (iv) the rights of the interested parties in the use of the AI system; (v) the duties of the AI agents; and (vi) guidelines for the federative entities' actions related to the use of AI. Yet, a new version of the Bill was submitted for appreciation in September 2021 by Representative Luiza Canziani, merely months after the AI regulation was proposed by the European Commission.

In the Bill's summary, Representative Luiza Canziani justifies the need for a new version of the regulation by stating that the original text needed to be improved for the sake of greater clarity and legal certainty in the application of the future law. To do so, the main inspiration for the suggested changes came from the EU AI Act's proposal, which was underway in the European Parliament and the European Council at the time. She then proposes the renewal of the successful partnership observed in the field of personal data protection, where the GDPR served as inspiration for the drafting of the LGPD.

Therefore, with the European AI draft regulation in mind, she proposes the need to guarantee that any regulation of AI systems takes into account the actual risks and the context of their operation, among other fundamental aspects. Unlike the European approach, however, there were no proposed *ex ante* limitations on

types of AI (that is, absolute prohibitions), nor even *ex ante* specifications of what would be high-risk AI, leaving such definitions to future sectoral legislation, regulation or self-regulation, to be elaborated and implemented as the technology matures in Brazil and the more precise identification of the risks involved in each activity or application becomes available. In this sense, this Bill does not replicate the regulatory model provided by the AI Act, as it does not adopt the risk-based approach, nor does it establish the governance structures that are mandatory in the context of the AI Act. Thus, the European influence is weaker, reaching principles and certain rights. This version of the Bill was approved by the House of Representatives in September 2021 ([Agência Câmara Notícias, 2021](#)), and is now awaiting approval from the Federal Senate.

Yet, although Bill No 21/2020 was mentioned by the EU as proof of its global influence in AI regulation, this Bill isn't the main legislative proposal aiming to regulate AI in Brazil. In fact, the media has recently reported that there are currently 46 Bills in the National Congress with similar purposes ([Amorozo, 2024](#)). Besides Bill No 21/2020, special attention has been given to Bill No 5,051/2019, which sets the principles for use of AI in Brazil, and Bill No 872/2021, which provides for the use of AI. Given the similarity between the three bills, they are now being processed jointly in the Federal Senate and in February 2022, the Senate's chairman, with a view to drafting a legal text with the most advanced technicality, set up a Commission of Jurists to help prepare a draft substitute for these Bills.

This Commission was made up of notorious jurists, who held several public hearings and discussions, and in May 2023 presented Bill No 2,338/2023, a draft law to regulate AI in Brazil, based on the Commission's conclusions, that rules on the development, promotion, ethical and responsible use of AI based on the centrality of the human person. The Bill's structure is made up of principle-based rules and prescriptive rules that regulate the involved agents' conducts by setting obligations and prohibitions. The current version of Bill No 2,338/2023, which was approved by the Federal Senate in December 2024, mentions in its first article that:

"This law establishes general national rules for the responsible governance of artificial intelligence (AI) systems in Brazil, with the aim of protecting fundamental rights, stimulating responsible innovation and competitiveness and guaranteeing the implementation of safe and reliable systems, for the benefit of the human person, the democratic regime and social, scientific, technological and economic development." (free translation)

Inspired by the EU AI Act, Bill No 2,338/2023 adopts a risk-based approach that, unlike Representative Luiza Canziani's proposition in Bill No 20/2021, proposes *ex ante* limitations on certain types of AI and classifies the AI system based on different risk levels. As such, Bill No 2,338/2023 classifies AI risks into (i) excessive risks, whose development, implementation and use are forbidden, (ii) high risks, which are subject to stricter rules, and (iii) any level of risk, which are subject to specific governance measures. In other words, Bill No 2,338/2023 has added to

the Brazilian discussion of AI regulation one of the EU AI Act's most striking features, which is the assignment of applications of AI into risk categories.

The current version of the Bill determines the need for a preliminary assessment in order to determine the AI system's level of risk before they are introduced on the market or used by the population. This assessment will be based on the criteria set out by the Bill and good practices, in accordance with the state of the art and technological development. From this perspective, the Bill defines the criteria of forbidden AI systems, which are considered as causing excessive risks, and lists the purposes and contexts of AI systems classified as high-risk. The list of purposes and contexts of high-risk use of AI systems provided for in Bill No 2,338/2023 is very similar to the AI Act's list, also including management and operation of critical infrastructures, educational and professional training, employment, management of workers and access to self-employment and administration of justice.

Yet, there are differences within the risk-based approach proposed by the AI Act and Bill No. 2,338/2023. The AI Act also adopts a model of prior listing of AI systems that are considered as high-risk. Along these lines, Annex III of the AI Act defines that AI technology used in specific areas and services that have direct impacts on citizens' lives will be classified as high-risk, which includes critical infrastructures, educational or vocational training, employment, management of workers and access to self-employment, law enforcement, and administration of justice and democratic processes.

Thus, the AI Act defines the areas of use of AI systems that are defined as high-risk, while Bill No 2,338/2023 does not use the same strategy, providing only the criteria to be used by the regulator and economic agents to classify the risk of AI systems. The European approach gives less freedom to classify systems between high and low risk within the same sector (e.g. biometrics), while the Brazilian model ensures that the likelihood and severity of adverse impacts on affected persons or groups must be taken into account before defining an AI system as high-risk.

Moreover, unlike the AI Act, Bill No 2,338/2023 also presents a rights-based approach, by dedicating an entire chapter to the rights of people and groups affected by AI systems. The Bill devotes specific rights to those affected by AI systems regardless of their risk level and other rights to people and groups who were affected by AI systems that produce relevant legal effects or are classified as high-risk.

In this sense, Bill No 2,338/2023 states that people and groups affected by AI systems regardless of their risk level have the rights to: (i) prior information regarding their interactions with AI systems, including the automated nature of the interaction, in an accessible, free and easy-to-understand manner, by using icons and symbols easily identified; (ii) privacy and the protection of personal data; (iii) human determination and participation; and (iv) non-discrimination that is unlawful and/or abusive and correction of direct, indirect, unlawful or abusive discriminatory biases.

Therefore, it is clear that the Brazilian approach to regulate AI is in many ways in line with the European regulation, especially in comparison to the U.S.'s Executive Order 14110. In spite of that, through Bill No 2,338/2023, Brazil has not fully incorporated the AI Act model, attested by the differences regarding the risk-based approach and the adoption of a rights-based model by the Brazilian legislator. To such a degree, in the same way as the other aforementioned examples, Brazil is transferring the European AI regulation, and not transplanting it. Brazilian authorities have locally adapted the draft AI regulation based on rights and attentive to risks, taking into account the international scenarios, which facilitates dialogue between regulations from different countries and Brazil, reducing the effort for organizations to adapt to the Brazilian context (*Coalizão Direitos Na Rede, 2024*).

Bill No 2,338/2023 was approved by the Federal Senate in December of 2024 and is currently awaiting approval from the House of Representatives, so by this moment, it is not possible to estimate when or whether it will come into effect. Nonetheless, the Brazilian National Congress seems eager to decide on the matter soon. The National Congress' chairman, Senator Rodrigo Pacheco, has stated that AI regulation is one of the priorities for the legislative branch (*Amorozo, 2024*). Moreover, several stakeholders in the country, including parliamentarians, experts and representatives of civil society, have publicly defended the Bill's approval (*Senado Notícias, 2024a*).

5. Conclusion

The examples of the Brazilian data protection law and the ongoing discussions surrounding AI regulation exemplify how Brazil is borrowing European regulations, especially the ones that encompass new technological advances and the constantly evolving internet environment. Yet, throughout this paper it was discussed that none of the Brazilian versions of the regulations (at their current state, considering that Bill No. 2,338/2023 is still being analyzed and its final text might change) are a true copy and paste to the European ones. That is because, once the legislation reaches Brazil, different aspects have been changed in some way to reflect the particular circumstances of Brazilian society. In this sense, it is plausible to say they are legal transfers, and not transplants, as explained by professors Frankenberg and Nicola.

These legal transfers are gradual, as they can be more generic at first and become more similar over time, as in the case of the convergence between the functions of the Brazilian and European DPOs. At the same time, the transfers can be very similar at first, but diverge in the details, such as the absence of a predefined list of AI activities considered to be high-risk, distancing Brazil from the European model. Based on the presented Brazilian examples, local adaptation in the transfer of rules can occur at different times (during the drafting of the Bill of Law itself) and come from different agents (such as the ANPD expanding the functions of the DPO present in the LGPD).

Europe and the U.S. have always been recognized as the leaders in exporting legal knowledge to other countries, especially those located in the Global South. Even so, in the early days of internet governance, Brazil was considered one of the protagonists of the regulation of the digital ecosystem, as it was one of the first countries to approve a regulation on the use of the internet in the country. Nonetheless, at the time Brazil was primarily influenced by regulatory discussions taking place in the U.S., as attested by the MCI's rulings on net neutrality and liability for intermediary platforms.

Somewhere along the lines, Brazil's position shifted, as the country became more prominent to pursue the EU's regulatory footsteps concerning the digital ecosystem. Author Anu Bradford explains that this was due to the phenomenon known as Brussels Effect, according to which the EU has become the world's main exporter of norms given to the fact that it has the largest internal market and very strong regulatory institutions. When it comes to internet regulation, the EU's rights-driven regulatory approach, which aims to protect the fundamental rights of its citizens, has also influenced other nations to follow the EU's approach. Moreover, the EU knows the influence it holds around the world, especially in countries from the Global South, and is interested in becoming a global role model for regulating the digital economy. Seen as a source of authority, European regulatory discussions are being closely monitored by these countries.

In the last few years, the case of privacy and personal data protection has become known for being one of the most notable examples of the Brussels Effect around the world. Although Brazil's LGPD was clearly inspired by the European model to protect personal data, set in the GDPR, a close analysis showcases subtle differences between the legislations, as explored in the example of the DPO. In this sense, although the structures of the regulations are very similar, in detail there are important distinctions that illustrate how Brazil wants to align itself with the European model (including for international trade purposes, as many companies who operate in Brazil were already in compliance with the LGPD before it was even sanctioned), at the same time that it is able to set cohesive standards considering the country's reality.

As for the regulation of AI, whose discussion is still underway in Brazil, with new regulation on the topic inspired by the European approach possibly being passed in the near future, the distinctions between the European model and the Brazilian one are not so subtle, further indicating that Brazil is distancing itself from the idea of legal transplants. By translating and applying legal information that originally came from Europe, Brazil modifies and adapts them to fit the country's culture and context.

The concept of legal transfer takes into consideration the political economy and social context of the regulation and jurisdiction in question, acknowledging it can work from Global South to Global North countries if we go beyond the failed law narrative. Although, by this moment, Brazil does not have the political strength to become an inspiration for Global North countries to solve their own legal problems, Brazil has shown that it can make coherent local adaptations that enhance

the debate.

Therefore, while the European legislative influence is heavily present in the Brazilian digital ecosystem, this paper showed that the European regulation isn't imported in a "copy and paste" manner (and neither should it be), as it is necessary to understand and take into consideration the realities of the national market.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

- Affonso, C., Magrani, E., & Carneiro, G. (2020). Lei Geral de Proteção de Dados Pessoais: Uma transformação na tutela dos dados pessoais. In C. Mulholland (Ed.), *A LGPD e o novo marco normativo no Brasil* (p. 44). Arquipélago.
- Affonso, C., Viola, M., & Lemos, R. (2017). *Brazil's Internet Bill of Rights: A Closer Look*. Institute for Technology and Society of Rio de Janeiro (ITS Rio).
https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa_pages_mio_lo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf
- Agência Brasil (2014). *Manifestantes pedem que governo brasileiro conceda asilo a Edward Snowden*.
<https://agenciabrasil.ebc.com.br/internacional/noticia/2014-07/manifestantes-pedem-que-governo-brasileiro-conceda-asilo-edward>
- Agência Câmara Notícias (2021). *Câmara aprova projeto que regulamenta uso da inteligência artificial*. Câmara dos Deputados.
https://www.camara.leg.br/noticias/811702-camara-aprova-projeto-que-regulamenta-uso-da-inteligencia-artificial?utm_source=POLITICO.EU&utm_campaign=25c6120bdd-EMAIL_CAMPAIGN_2021_11_17_09_59&utm_medium=email&utm_term=0_10959deb5-25c6120bdd-190866048
- Amorozo, M. (2024). *Congresso tem pelo menos 46 projetos de lei para regulamentar do uso de inteligência artificial*. CNN Brasil.
<https://www.cnnbrasil.com.br/politica/congresso-tem-pelo-menos-46-projetos-de-lei-para-regulamentar-do-uso-de-inteligencia-artificial/>
- Baptista, L. (2022). *Guia América Latina: Legislações de Proteção de Dados*.
https://baptistaluz.com.br/wp-content/uploads/2022/12/bluz_221130_AYIP_America-Latina-Legislacao-de-protecao-de-dados_V2.pdf
- Bassini, M. (2024). *The Global Race to Regulate AI: Biden's Executive Order Spillover Effects on the EU AI Act*. Institute for European Policy Making at Bocconi University.
<https://iep.unibocconi.eu/publications/global-race-regulate-ai-bidens-executive-order-spillover-effects-eu-ai-act>
- BEREC (2023). *All You Need to Know about the Open Internet Rules in the EU*.
<https://www.berec.europa.eu/en/all-you-need-to-know-about-the-open-internet-rules-in-the-eu-0>
- Bonilla, D. (2013). Towards a Constitutionalism of the Global South. In D. Bonilla (Ed.), *Constitutionalism of the Global South* (pp. 10-12). Cambridge University Press.
- Bonilla, D. (2018). The Political Economy of Legal Knowledge. In D. Bonilla, & C. Crawford (Eds.), *Constitutionalism in the Americas* (pp. 32, 33, 58, 59, 75). Elgar Publishing.
- Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*.

- Oxford University Press. <https://doi.org/10.1093/oso/9780190088583.001.0001>
- Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press. <https://doi.org/10.1093/oso/9780197649268.001.0001>
- Brannon, V. C., & Holmes, E. N. (2024). *Section 230: An Overview*. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/R/R46751>
- Casovan, A., & Zweifel-Keegan, C. (2023). *Implications of the AI Executive Order for Business*. IAPP. <https://iapp.org/resources/article/implications-of-the-ai-executive-order-for-business/>
- CGI.br (2014). *Um pouco sobre o Marco Civil da Internet*. <https://www.cgi.br/noticia/notas/um-pouco-sobre-o-marco-civil-da-internet/>
- CJEU (2023). *C-453/21 X-FAB Dresden GmbH & Co. KG v FC*. Decision from Feb. 09, 2023. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=258249&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=366992>
- Coalizão Direitos na Rede (2024). *Projeto de Lei n. 2338/2023*. <https://direitosnarede.org.br/2024/06/18/projeto-de-lei-n-2338-2023>
- Data Guidance by One Trust and Baptista Luz Advogados (2024). *Comparing Privacy Laws: GDPR v. LGPD*. <https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf>
- DPO Centre (2023). *The Role of a DPO: Dismissal and Conflicts of Interests*. DPO Centre. <https://www.dpocentre.com/the-role-of-a-dpo-dismissal-and-conflicts-of-interests/>
- Esquirol, J. L. (2008) The Failed Law of Latin America. *American Journal of Comparative Law*, 56, 75-124. <https://doi.org/10.5131/ajcl.2007.0003>
- EU AI Act (2024) *The EU Artificial Intelligence Act: Up-to-Date Developments and Analyses of the EU AI Act*. <https://artificialintelligenceact.eu/>
- European Commission (2020) *Shaping Europe's Digital Future*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en
- European Commission (2021). *Europe's Digital Decade: Commission Sets the Course towards a Digitally Empowered Europe by 2030*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983
- European Commission (2024a). *A Europe Fit for the Digital Age*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
- European Commission (2024b). *Shaping Europe's Digital Future—AI Act*. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- European Commission (2024c). *Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273
- European Parliament (2021). *Shaping the Digital Transformation: EU Strategy Explained*. European Parliament. <https://www.europarl.europa.eu/topics/en/article/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained>
- European Parliament (2023). *EU AI Act: First Regulation on Artificial Intelligence*. European Parliament. <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

- Frankenberg, G. (1985). Critical Comparisons: Re-Thinking Comparative Law. *Harvard International Law Journal*, 26, 412.
- Frankenberg, G. (2022). Legal Transfers. In M. C. Foblets et al. (Eds.), *The Oxford Handbook of Law and Anthropology* (pp. 333-351). Oxford University Press.
<https://doi.org/10.1093/oxfordhb/9780198840534.013.20>
- Frankenberg, G., & Nicola, F. (2024). *Comparative Law: Introduction to a Critical Practice*. Elgar Publishing.
- GDPRHUB (2024). *Data Protection in Spain*.
https://gdprhub.eu/Data_Protection_in_Spain
- Graziadei, M. (2006). Comparative Law as the Study of Transplants and Receptions. In M. Reimann, & R. Zimmermann (Eds.), *The Oxford Handbook of Comparative Law* (pp. 1, 3, 16). Oxford University Press.
- Intersoft Consulting (2024). *GDPR Data Protection Officer*.
<https://gdpr-info.eu/issues/data-protection-officer/>
- IRIS.BH (2017). *Freedom of Speech and the Brazilian Internet Bill of Rights: Three Years of Regulation*. IRIS.BH.
<https://irisbh.com.br/en/freedom-of-speech-and-the-brazilian-internet-bill-of-rights-three-years-of-regulation/>
- Johnson, A., & Castro, D. (2022) *Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved*. Innovation Technology & Innovation Foundation.
<https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved/>
- Kennedy, D. (2006). Three Globalizations of Law and Legal Thought: 1850-2000. In D. Trubek, & A. Santos (Eds.), *The New Law and Economic Development: A Critical Appraisal* (pp. 19-73). Cambridge University Press.
<https://doi.org/10.1017/CBO9780511754425.002>
- Kenton, W. (2023). *What Is Net Neutrality? Policies and Controversy*. Investopedia.
<https://www.investopedia.com/terms/n/net-neutrality.asp>
- Koch, R. (2023). *What Is the LGPD? Brazil's Version of the GDPR*. GDPR.EU.
<https://gdpr.eu/gdpr-vs-lgpd/>
- Kocharyan, H., & Vardanyan, L. (2024). *The Right to Be Forgotten as a Legal Instrument for Expanding Informational Self-Determination in the Digital Age?* Constitutional Discourse.
<https://constitutionaldiscourse.com/the-right-to-be-forgotten-as-a-legal-instrument-for-expanding-informational-self-determination-in-the-digital-age/>
- Legrand, P. (1997). The Impossibility of 'Legal Transplants'. *Maastricht Journal of European and Comparative Law*, 4, 111-124.
<https://doi.org/10.1177/1023263X9700400202>
- Linebaugh, C. D. (2022). *Net Neutrality Law: An Overview*. Congressional Research Service. <https://sgp.fas.org/crs/misc/R46973.pdf>
- Londoño, J. (2021). *Content Moderation Using Notice and Takedown Systems: A Paradigm Shift in Internet Governance*. American Action Forum.
<https://www.americanactionforum.org/insight/content-moderation-using-notice-and-takedown-systems-a-paradigm-shift-in-internet-governance/>
- Mattei, U. (1994). Why the Wind Changed: Intellectual Leadership in Western Law. *The American Journal of Comparative Law*, 42, 195-218. <https://doi.org/10.2307/840732>
- Oliva, T. (2019). *Responsabilidade de intermediários e a garantia da liberdade de expressão na rede*. InternetLab.

- <https://internetlab.org.br/pt/especial/responsabilidade-de-intermediarios-e-a-garantia-da-liberdade-de-expressao-na-rede/>
- Petrosyan, L., & Ataliotou, K. (2024). *A Tale of Two Policies: The EU AI Act and the U.S. AI Executive Order in Focus*. Trilligent.
<https://trilligent.com/a-tale-of-two-policies-the-eu-ai-act-and-the-us-ai-executive-order-in-focus/>
- Pouget, H., & Zuhdi, R. (2024). *AI and Product Safety Standards under the EU AI Act*. Carnegie Endowment for International Peace.
<https://carnegieendowment.org/research/2024/03/ai-and-product-safety-standards-under-the-eu-ai-act?lang=en>
- Rezende, L., & De Lima, M. (2015). *Governança na internet: Um estudo sobre o Marco Civil brasileiro*. Scielo.
http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-82852016000100006
- Rozenshtein, A. Z. (2024). *Interpreting the Ambiguities of Section 230*. Yale Journal on Regulation.
<https://www.yalejreg.com/bulletin/interpreting-the-ambiguities-of-section-230/>
- Senado Notícias (2024a). *Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA*. Senado Federal.
<https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia#:~:text=H%C3%A1%2010%20anos%20o%20uso,liberdade%20de%20express%C3%A3o%20na%20internet>
- Senado Notícias (2024b). *Regulação do uso de IA tem apoio de debatedores*. Senado Federal.
<https://www12.senado.leg.br/noticias/materias/2024/06/11/debatedores-defendem-regulamentacao-do-uso-de-inteligencia-artificial>
- The White House (2023). *Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*. The White House.
<https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>
- Van Bael and Bellis (2024). *Fundamental Rights Impact Assessment in the EU Artificial Intelligence Act*. Van Bael and Bellis.
<https://www.vbb.com/insights/fundamental-rights-impact-assessment-under-eu-ai-act>
- Watson, A. (1978). Comparative Law and Legal Change. *Cambridge Law Journal*, 37, 313-336. <https://doi.org/10.1017/S0008197300093338>
- Web Foundation (2014a). *Marco Civil: Statement of Support from Sir Tim Berners-Lee*. World Wide Web Foundation.
<https://webfoundation.org/2014/03/marco-civil-statement-of-support-from-sir-tim-berners-lee>
- Web Foundation (2014b). *Welcoming Brazil's Marco Civil: A World First Digital Bill of Rights*. World Wide Web Foundation.
<https://webfoundation.org/2014/03/welcoming-brazils-marco-civil-a-world-first-digital-bill-of-rights/>
- Wolford, B. (2023). *What Is GDPR, the EU's New Data Protection Law?* GDPR.EU.
<https://gdpr.eu/what-is-gdpr/>

Appendix

Brasil (2018). *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília.*

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brasil (2021). *Parecer de Plenário pelas Comissões de Ciência e Tecnologia, Comunicação e Informática, Trabalho, de Administração e Serviço Público e Constituição e Justiça e de Cidadania ao Projeto de Lei nº 21, de 2020. Câmara dos Deputados.*

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2068016&filename=Tramitacao-PL%2021/2020

Brasil (2023). *Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014.*

<https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180>

Brasil (2024). *Parecer da Comissão Temporária sobre Inteligência Artificial no Brasil. Senado Federal.*

https://legis.senado.leg.br/sdleg-getter/documento?dm=9640105&ts=1720798348647&rendition_principal=S&disposition=inline

Brasil (2024). *Projeto de Lei n.º 2338/2023. Senado Federal.*

<https://legis.senado.leg.br/sdleg-getter/documento?dm=9881643&ts=1738768184212&disposition=inline>

Brasil (2024). *Resolução CD/ANPD nº 18, de 16 de julho de 2024. Diário Oficial da União, Brasília.* <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074>