Consultation on Digital Platform Regulation: Systematization of Inputs

CGI.br Platform Regulation Working Group

cgi.br

Consultation on Digital Platform Regulation: Systematization of Inputs

cgi.br

BRAZILIAN NETWORK INFORMATION CENTER - NIC.BR

Executive Board

Demi Getschko (*Chairperson*)
Hartmut Richard Glaser (*Consulting Director for CGI.br activities*)
Ricardo Narchi (*Managing and Finance Director*)
Frederico Neves (*Services and Technology Director*)
Milton Kaoru Kashiwakura (*Special Projects and Development Director*)

PUBLISHING COORDINATION

Digital Platform Working Group – Members

Henrique Faulhaber (*Coordinator*)
Renata Mieli
Rafael Evangelista
Laura Tresca
Bia Barbosa
Marcos Dantas
Percival Henriques
Rosauro Baretta
James Görgen
Luciano Mazza
Demi Getschko
Carlos Manuel Baigorri

RESEARCH AND REPORT DRAFTING

Juliano Cappi and Juliana Oms

TECHNICAL PROOFREADING

Diogo Moyses Rodrigues

TRANSLATION INTO ENGLISH

Bettina Gertum Becker

TEXT PREPARATION AND PROOFREADING

Érica Santos Soares de Freitas

GRAPHIC DESIGN

Maricy Rabelo and Giuliano Galves (Comunicação NIC.br)

LAYOUT

Grappa Marketing Editorial (www.grappa.com.br)

BRAZILIAN INTERNET STEERING COMMITTEE (CGI.br)

Composition in December, 2023

Government Sector Representatives

Carlos Manuel Baigorri, Cláudio Furtado, Débora Peres Menezes, José Roberto de Moraes Rêgo Jr, Luiz Felipe Gondin Ramos, Maximiliano Salvadori Martinhão, Pedro Helena Pontual Machado, Renata Mielli, and Rogério Souza Mascarenhas

Business Sector Respresentatives

Henrique Faulhaber, José Alexandre Novaes Bicalho, Nivaldo Cleto, and Rosauro Leandro Baretta

Third-Sector Representatives

Bia Barbosa, Domingos Sávio Mota, Laura Conde Tresca, and Percival Henriques de Souza Neto

Technical and Scientific Community Representatives

Marcos Dantas Loureiro, Rafael de Almeida Evangelista, and Tanara Lauschner

Representative of Recognized Erudition on Internet Matters

Demi Getschko

Coordinator

Renata Mielli

Executive Secretary

Hartmut Richard Glaser

CONTENTS

FOREWORD

The Brazilian Internet Steering Committee (CGI.br) has historically played a relevant role in building spaces for multi-stakeholder dialogue and in establishing consensus on issues related to the Internet, especially on highly complex topics, such as the discussions that led to the approval of the Marco Civil da Internet (MCI; Civil Rights Framework for the Internet) (Law 12,965) (BRASIL, 2014), the discussions on the General Data Protection Law (LGPD) (Law 13,709) (BRASIL, 2018) and, currently, the ongoing debates on the regulation of digital platforms.

The result of more than two years of work coordinated by the Platform Regulation Working Group of CGI.br, the "Consultation on Digital Platform Regulation" is part of this context. In May 2021, the WG held an international seminar to reflect on and integrate the various perspectives related to digital platform regulation presented by speakers from different countries (NIC.BR, 2021). In that same year, the WG also promoted two sessions at the Brazilian Internet Governance Forum (FIB) and coordinated a workshop at the Global Internet Governance Forum (IGF) held in Poland to discuss regulations from the perspective of the Global South.

In September 2022, the WG held a seminar (NIC.BR, 2022) and a workshop on the topic, resulting in the publication of a report with actions and guidelines for the regulation of digital platforms proposed by the participants (CGI.BR, 2023a). These initiatives contributed to the design of the consultation on digital platform regulation developed by CGI.br. The consultation was conducted between April 25 and July 16, 2023, and aimed to provide a broader space to listen to the different social sectors to deepen the ongoing debate in Brazil, some of the legislative discussions within the scope of the National Congress.

The inputs can be accessed fully through the consultation platform (CGI.BR, 2023b). A wealth of perspectives and ideas provide interesting reflections on that issue. Based on this set of inputs, CGI.br produced a systematization report, organizing critical elements for the design of digital platform regulation. The report provides an overview that covers potential definitions and classifications of platforms, the risks and challenges

presented by their activities, possible mitigation measures, and the actors and institutional structures that should enforce future regulations.

CGI.br hopes that this report systematizing the public consultation results contributes to the progress of ongoing discussions in Brazil on digital platform regulation, considering the different perspectives of the various social groups within our country's context, and the global discussions on this issue.

The report is divided into three chapters. Chapter 1 presents a qualitative summary of the inputs received on **who to regulate** in response to questions about the object and scope of regulation, including different definitions, typologies, and fields of activity of digital platforms.

Chapter 2 summarizes the inputs on **what to regulate**, involving questions about the risks arising from digital platform activities and possible mitigation measures. The risks were organized into four main groups: i) risks related to threats to competition, economic and data concentration; ii) risks related to threats to digital sovereignty, technological development, and innovation; iii) risks related to threats to decent work; and iv) risks related to threats to Democracy and Human Rights.

Chapter 3 presents a quantitative and qualitative synthesis of the inputs on **how to regulate** digital platforms and the possible institutional arrangements to regulate them, considering both state regulation models and different approaches to self-regulation.

With this work, CGI.br hopes to contribute to the continuity of this critical debate on the effects of digital services and platforms on society and on how regulations and agreements on new forms of digital interaction are established.

We believe that one of the merits of the consultation was to allow the different actors and sectors involved in these new digital environments to express their opinions and arguments on the issues presented in a structured manner to mature this debate, identifying consensus and dissents among the different actors and relevant topics that require further discussion in other opportunities.

We understand that the consultation summarized in this report is only a part of a critical process that should continue in further initiatives led by CGI.br itself, public authorities, and other institutions engaged in these critical discussions.

Enjoy reading!

Henrique Faulhaber
Coordinator of the Platform Regulation Working Group

Renata Mielli
CGI.br Coordinator

EXECUTIVE SUMMARY

CGI.br's consultation on digital platform regulation explores definitions and classifications, maps the risks posed by the activities of platforms and the potential regulatory measures to mitigate them, and identifies the measures and actors required to implement them. The consultation systematization presents a map of consensus and dissent among stakeholders, allowing for building multi-stakeholder agreements and solutions beyond those exclusively regulatory. Furthermore, the quality and depth of the inputs to the consultation allow for a more comprehensive understanding of the challenges and opportunities arising from the growth of digital platforms in Brazil.

The consultation was opened to society's participation between April 25 and July 20, 2023, and received 1,336 inputs from 140 individuals and organizations from the four sectors that make up CGI.br (government sector, third sector, business sector, and scientific and technical community.)

In this sense, this report aims at presenting the results of the consultation process to allow the public to understand the different current perspectives, consensus, and dissents on the topics covered, issues to be further explored, as well as occasional singularities and shades in the participants' approaches.

Axis 1 of the consultation (WHO TO REGULATE) advanced the discussion on the regulation scope based on potential critical elements that define digital platforms and possible criteria to determine which platforms should be regulated. The inputs mainly addressed the following topics:

1. **Main elements that define digital platforms**: **i) technological infrastructure**: inputs on this aspect used a set of approaches and terminologies (mentioning "digital," "electronic," and "Internet," among other terms), whose focus was on transactional platforms characterized by connecting groups and producing benefits based on the network effect; **ii) actors and their relationships on the platforms**: it was frequently mentioned that platforms correlate several agents when citing the concept of two- or multi-sided markets, identifying, on the one hand, service or product providers and, on the other,

consumers or users of these services or products; and **iii) platform characteristics**: data-intensive, Artificial Intelligence (AI) technologies and network effects were pointed out as shared or essential characteristics of digital platforms, which were later mentioned as potential risks to competition and of the abuse of economic power, or to human rights and personal data protection.

2. **Platform typology**: the inputs identified digital platform general and specific characteristics that may be used to determine the scope of possible regulatory initiatives or to divide them into sectoral regulations (e.g., specific regulations for ride-hailing platforms, public platforms, etc.) according to the dimensions and categories associated with service types, business model characteristics, legal nature, and activity or market segments.

3. **Asymmetric regulation**: there was a broad consensus that regulation must be asymmetric, i.e., only some actors in the digital ecosystem should be objects of specific regulatory provisions, and therefore, identifying criteria to allow charting these agents is still needed. There was also some agreement that no criteria should be individually applied but defined cumulative and alternative combinations should be used. Generally, **gatekeepers (holders of essential access points)** were mentioned as the main focus of regulation, encompassing other criteria, such as **providing specific types of services with a defined user, revenue, or market share volume**. The details for implementing each criterion must be further explored, including their quantification and the complexities of defining their metrics.

The inputs on **Axis 2 of the consultation (WHAT TO REGULATE)** answered questions about the risks arising from digital platform activities and their possible mitigation measures.

The risks and measures associated with the **abuse of market power and economic and data concentration** were some of the topics that received the most attention, with inputs from all sectors. There was a clear difference in the approach of the different sectors that answered the consultation regarding both risks and measures.

Relative to risk identification, part of the private sector – particularly associations representing digital platforms – argued that digital markets are characterized by fast innovation, intense competition, broad consumer diversity, and constant changes. The private sector stressed the benefits of digital platforms to the economy and considered that Brazil has a robust and comprehensive competition defense system capable of addressing potential anti-competitive behavior.

On the other hand, there was strong consensus among the third sector, the government sector, the scientific and technical community, and other private sector actors (such as media company associations) on the relevance of the risks mapped. That group mentioned platform characteristics (e.g., network externalities) and anti-competitive strategies (e.g., self-preferencing and aggressive acquisitions of competitors) that contribute to establishing monopoly power and its abuse. It also highlighted that data concentration grants substantial economic power to digital platforms, which can leverage them in other markets. Those factors generate a winner-takes-all dynamics and a lock-in effect, to the detriment of product and service innovation and quality, and also affect other areas, such as freedom of expression and data protection.

As for **consensus and dissents on mitigation measures**, there was a striking difference between those two groups. Associations representing digital platforms and some other actors considered the current competition law provisions (mostly *ex-post*, i.e., explicitly applied to an issue after it occurred) sufficient to fight potential abuses. On the other hand, the other actors emphasized the importance of competition law or economic regulation provisions that operate *ex-ante* (i.e., in advance) as a structural part of fighting the identified abuses. Special mitigation measures aimed at conglomerates were suggested, such as prohibiting self-preference for their products on their platforms and data sharing among companies belonging to the same corporation, as well as updating the criteria for notification of concentration acts. Despite disagreements regarding implementation, all groups agreed that interoperability requirements should be established. On the other hand, policies to promote alternative models to those of large platforms, such as not-for-profit or local models, were highlighted by participants from the third sector and the scientific and technical community.

There were conceptual differences about **digital sovereignty risks** and associated measures that directly may affect possible definitions of the regulatory approach. The first approach to the concept of digital sovereignty is related to the notion of control and power of the State, including the different layers that make up the digital environment and the guarantee of national security and data flow. The second approach refers to developing the local industry of technologies, platforms, and various digital services, aiming to reduce the dependence on foreign companies and to achieve economic autonomy. The third approach concerns the autonomy and self-determination of individuals, groups, and social movements, considering their capacity to make autonomous and independent decisions about [the use of] their information according to their interests, values, and culture.

There is a clear overlap between technological sovereignty and international data transfer risks. According to some participants, the provision of public interest services in strategic areas on transnational digital platforms generally implies the external processing of relevant data of Brazilian citizens, generating risks and technological dependence. However, the risks related to international transfers were not recognized by private sector actors, who, on the contrary, pointed out benefits, such as greater security in the storage of those data. The dependence on digital platform applications in education was also stressed in this risk group.

Among the mitigation measures, the importance of investing in public infrastructure in the digital ecosystem and using open-source software was mentioned. The principal dissent observed was between entities representing digital platforms and the academic sector, which advocates giving preference to hiring or investing in national technologies.

The group of **risks related to threats to decent work on platforms** received fewer inputs, which suggests the need to promote this debate internally and in other forums. The private sector, for instance, did not comment on that issue or stated that this is not the appropriate forum for such discussion. Other participants mentioned precarious work risks, particularly transparency issues when processing workers' data and the opaque use of algorithms by platforms, which affects working conditions. Furthermore, some unmapped issues emerged,

such as workers' representation arrangements, communication between the workers and the platforms, and discrimination risks caused by user rankings or algorithms, making it essential to establish measures to ensure opportunity and hiring equality. The specificities of child labor on digital platforms were also identified as relevant risks.

The inputs on the **risks posed by digital platform activities to the protection of fundamental rights and democracy** deepened the discussion on potential harms to freedom of expression, access to information, and cultural diversity mainly due to the advance of extremism, hate speech, and incitement to violence and disinformation in social media.

Relative to the challenges posed by **infodemics**, three elements that contribute to the deterioration of the information environment were identified: i) massive data collection and processing, ii) profiling and micro-segmentation, and iii) algorithmic systems programmed to increase engagement time and monetize posted content primarily through advertising. Digital inclusion challenges, such as the zero-rating practice and digital literacy, were also mentioned.

There was a broad consensus that fighting infodemics involves **strengthening journalism**. The third sector and the scientific and technical community primarily focused on the significant transfer of advertising revenues to digital platforms and the power of these companies over the content circulating on the Internet. On the other hand, the private sector mentioned that the crisis in journalism is not a consequence of platform activities, and it may even be beneficial as their plurality increases.

Regarding **democracy and electoral processes**, several inputs emphasized that digital platforms are channels for disseminating electoral disinformation, involving groups that violate fundamental rights and take advantage of the platforms' business models. There was broad consensus on imposing broader obligations for platforms during election periods.

The main dissent relative to **transparency** was between those who support expanding digital platform obligations – of social media platforms, in particular – and those who defend limiting such obligations in order to protect trade secrets and sensitive information related to business models and claim that the current legal framework and the measures adopted by the

platforms are sufficient. Third-sector entities, however, argued that transparency is not a matter of trade secrets but rather of public interest – of users and society as a whole – as it is a fundamental right in many spheres.

Inputs on **privacy and data protection risks** were dispersed throughout the consultation. However, we highlight the third-sector suggestions regarding restrictions of data-based profiling and the concern of the Autoridade Nacional de Proteção de Dados (ANPD, Brazilian Data Protection Authority) as to the preservation of its powers and adequately aligning any platform regulation policies with those provided for in the LGPD[1] (BRASIL, 2018).

Relative to **children and adolescents**, several inputs addressed their vulnerability to platforms' strategies and business models, emphasizing the precept to prioritize the protection of children and adolescent's rights, including their mental and physical health.

Among the **mitigation measures**, we highlight the debate on the platforms' responsibility for content posted by third parties. The participants' positions draw on a wide diversity of approaches, organized into four groups: i) maintaining the current terms of the Marco Civil da Internet (MCI; Civil Rights Framework for the Internet) (BRASIL, 2014); ii) establishing a regime of objective and joint liability for digital platforms for third-party promoted and monetized content; iii) creating a special liability regime based on the obligation to moderate specific content categories; and iv) establishing obligations to assess and mitigate systemic risks related to the moderation of content posted by third parties. It should be noted that such approaches may be simultaneously applied: the general platform liability regime provided for in the MCI (BRASIL, 2014), for instance, may be maintained, albeit any possible adoption of objective liability for promoted or paid content in Brazil.

The inputs to **Axis 3 of the consultation (HOW TO REGULATE)** indicate some consensus on the principles that should guide the institutions responsible for the regulation and dissents and shades regarding their possible institutional

[1] Lei Geral de Proteção de Dados, Brazilian General Data Protection Law.

designs. The most frequently recommended principles were multistakeholderism, independence, and transparency.

The inputs relative to regulation enforcement and compliance monitoring discussed **the establishment of entities with different legal natures, the role of the State and private institutions, and the concentration level of the decision-making poles**. The proposals are herein divided into the establishment of:

- **An authority to regulate**, enforce, and monitor the policies developed. Such authority should have administrative, financial, and functional autonomy and be established as an indirect public administration agency. Such an entity could be linked to a multistakeholder board with the deliberative capacity to establish a regulatory system.
- **A governance system with no central regulatory body**, whose composition would include institutions with variable nature and attributions. Many mentioned the participation of CGI.br.
- **A self-regulatory entity**, in addition to an autonomous supervisory entity, with multisectoral representation – proposed mainly by the private sector.

Based on the participants' approaches, the regulatory models identified were divided into self-regulation, which may rely on a monitoring regulatory authority with restricted powers; regulation, based on independent regulatory authority models; and governance as a "system," structured essentially in ministerial departments and existing regulatory agencies or authorities. Furthermore, the benefits and risks of CGI.br's participation were mentioned. Overall, respondents disagreed with establishing the National Telecommunications Agency (Anatel) as the main regulatory body, although an association of small/medium-sized telecom operators favored this possibility.

The duties and powers identified include supervisory and monitoring power, normative and regulatory power, sanctioning power, power to receive and resolve complaints, duty to research, educational duty, duty to determine and assess risks, and duty of cooperation and articulation. Although mentioned by the different sectors, each assigned different meanings to duties: for instance, for those who advocate for "regulated self-

regulation" – usually the private sector – the scope of monitoring and standardizing power is narrower than in models with greater State protagonism.

CONCLUSIONS

The analysis of the inputs of the various sectors to the consultation provides solid support for future discussions on digital markets and services governance and the development of consistent regulatory frameworks to address the different identified risks related to digital platforms.

The current report organized the inputs received, associating proposals for regulatory measures on economic, competition, labor, industrial and innovation policies, human rights, and the protection of democracy. It provides a map of consensus, dissents, and shades of the perspectives of the private sector, third sector, scientific and technical community, and government sector identified in the consultation.

It should be noted that the diversity of platform models and types, their different sizes and areas of activity, and the different approaches proposed reveal the complexity and challenges involved in developing and improving regulations.

This report will contribute to the development of a digital platform regulation project to, on the one hand, mitigate risks related to the activities of such organizations and, on the other, protect fundamental rights and national sovereignty.

INTRODUCTION

The CGI.br's consultation on platform regulation explores platform definitions and classifications, mapping the risks posed by platform activities, the regulatory measures capable of mitigating them, and, finally, the governance arrangements required to enforce the regulation. The consultation also aims to contribute to a regulatory process that favors multistakeholder agreements. To this end, its focus was to achieve broad multistakeholder mobilization through a diversity of inputs to support the consensual development of a Brazilian regulatory framework for digital platforms.

This report presents the consultation results to inform the public about the **different perspectives, consensus, and dissents** on the various topics covered and possible **specificities of the participants' approaches**. The report highlights **consensual or majority opinions** within the different sectors whenever possible and relevant.

1 AXES AND TOPICS ADDRESSED

The consultation included 43 questions, organized into three main axes, which sought to answer:

1. **WHO will be regulated**: questions on the regulation scope and object, i.e., the definition and classification of digital platforms. This axis included four questions.
2. **WHAT will be regulated**: questions on the risks arising from digital platforms activities and their possible mitigation measures. This axis included 34 questions organized into four general risk groups related to the following threats, namely:
    - **Competition, consumer rights, abuse of economic power, and economic and data concentration;**
    - **Digital sovereignty, and technological development and innovation;**
    - **Decent work;**
    - **Democracy and Human Rights.**

3. **HOW it will be regulated**: questions on the institutional arrangements required to enforce platform regulation, highlighting the different roles and responsibilities of the various actors involved. This axis included five questions.

2 QUANTITATIVE SUMMARY OF INPUTS

The consultation received **1,336 inputs from 140 individuals and organizations from the four sectors that comprise the CGI.br** (government sector, third sector, business sector, and scientific and technical community) and had 542 registered users. Out of those inputs, 16 were moderated because they did not comply with the consultation terms, and the remaining **1,320 valid inputs were included in the systematization process**.

The third sector and the scientific and technical community sent most of the inputs, with 41% and 39.5% of the total, respectively. The business sector accounted for 15% of the inputs, and the government sector for 4%. It should be noted, however, that many inputs of the business sector were made by business associations representing hundreds of various companies[2].

The Southeast Region submitted the highest number of inputs, with 51% of the total, followed by the Central-West (31%), Northeast (12%), South (4%), and North (2%) regions.

[2] Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais (Brasscom, Association of Information and Communication Technology and of Digital Technology Companies), Associação Latino-Americana de Informação (ALAI, Latin American Information Association), Câmara Brasileira da Economia Digital (Câmara.e-net, Brazilian Chamber of the Digital Economy), and Associação Brasileira das prestadoras de Serviço de Telecomunicações Competitivas (TelComp, Brazilian Association of Competitive Telecommunications Service Providers) are examples of business associations that participated in the consultation and represent several associates.

TABLE 1 – INPUTS TO THE CONSULTATION BY SECTOR

SECTOR	AMOUNT OF INPUTS	% OF THE TOTAL
Third Sector	549	41
Scientific and Technical Community	526	39.5
Business Sector	203	15
Government Sector	58	4.5
Total	1336	100%

SOURCE: PREPARED BY THE AUTHORS.

TABLE 2 – INPUTS TO THE CONSULTATION BY REGION

REGION	AMOUNT OF INPUTS	% OF THE TOTAL
Southeast	682	51
South	55	4
Northeast	152	12
North	32	2
Central-West	415	31
Total	1336	100%

SOURCE: PREPARED BY THE AUTHORS.

Concerning the risk mapping topics, Axis 2 received the highest number of inputs (73%), followed by Axis 1 (19%) and Axis 3 (8%).

TABLE 3 – INPUTS RECEIVED BY AXIS

AXIS	AMOUNT OF INPUTS	% OF THE TOTAL
1) Who to regulate: definition and classification of digital platforms	225	19
2) What to regulate: activity risks and mitigation measures	976	73
3) How to regulate: institutional arrangements	135	8
Total	1336	100

SOURCE: PREPARED BY THE AUTHORS.

3 REPORT COMPILATION METHODOLOGY

Due to the scope of the consultation, the number of topics covered, and the numerous opinions stated in the inputs, compiling the report was challenging. Therefore, we utilized methodological literature references to organize and group the opinions according to their agreement level. In order to support the discussions on each topic, theoretical references were also used to contextualize specific perspectives and point out concepts not addressed by the participants.

Aiming to produce a faithful account of the participants' ideas, direct excerpts of the inputs were transcribed to express their views without mediation. However, some degree of interpretation is inherent to the process of producing the report, particularly on topics of a complex nature. The choice of quotations considered their recurrence in the themes and the plurality of participants, seeking to create a multistakeholder mosaic representative of the consultation and the perspectives presented in the inputs.

The composition of the input panel was created by applying the analytical plan of Mendes and Miskulin (2017), based on the theory of content analysis and on a classification model of the inputs received to answer the consultation questions. **Each unit was separated into content units and subsequently classified based on its nature, according to the consultation structure**, as described below:

- **Axis 1**: 1) Platform definition, 2) Platform typology, and 3) Criteria for platform classification.
- **Axis 2**: 1) Risk Proposal and 2) Proposal of Mitigation Measures.
- **Axis 3**: 1) Rules, Flows, and Tools; 2) Suggestion for the creation of a public body; 3) Suggestion for the creation of other bodies; and 4) Principles, Guidelines, and Values.

Following the same methodology, categories of interest and interrelation were added and applied to all content units: 1) Agreement, 2) Disagreement, and 3) Rationale.

In parallel with the content analysis described, the general rules of qualitative analysis were also applied to provide more detailed meanings and analyses of the consultation inputs. Finally, in addition to the general methodological framework applied for input grouping and analyses, specific literature concepts were used to aid the organization of each axis. Due to their conceptual and theoretical nature, those references were more frequently used to report Axis 1 on "who to regulate." Classic regulatory theories supported the description and interpretation of regulatory approaches.

AXIS 1 – WHO TO REGULATE

1 INTRODUCTION

This chapter presents a qualitative summary of the inputs received in Axis 1 of the consultation on **who to regulate** and includes questions on the scope and object of regulation and, more specifically, the definition and the classification of digital platforms. A total of 225 inputs on the four questions of Axis 1 were received, accounting for 19% of the total number of inputs received in the entire consultation[3].

The issues were organized to achieve the best possible aggregation per theme, i.e., inputs were not necessarily organized according to the axis questions. The aim was to enhance the structural understanding of the topics addressed in the inputs and organize the key issues that require further discussion on how to define and classify digital platforms.

Finally, it should be noted that, due to the theoretical and conceptual nature of the definition and classification of platforms, the inputs to this axis point to a broader dispersion of perspectives among the different actors compared to other axes, despite the high degree of consensus relative to asymmetric regulation. Therefore, the report on the first axis of the Consultation presents some illustrative examples of the existing perspectives. However, they do not necessarily reflect a homogeneous or majority view within the different sectors. Particularly regarding the definition of digital platforms, we sought to overcome terminological heterogeneity using the conceptual and methodological references available in the literature.

2 DEFINITIONS OF DIGITAL PLATFORMS

In order to analyze and identify possible groupings, consensus, and dissents, the content units related to the definition of digital platforms were classified according to structuring elements

[3] Although the inputs are not included in the references of this article, they are available at CGI.BR (2023b).

extracted from the literature[4] to allow the logical grouping of the questions and subtopics addressed in the consultation. Based on those conceptual references and in order to build a framework of the definitions presented by the participants, the Axis 1 report was structured according to the following topics:

1. Platform infrastructure;
2. Actors and their relationships on digital platforms;
3. Platform characteristics, including data-intensive and AI technologies, network effects, and economies of scope; and
4. Challenges to the use of the term '**digital platforms**' in regulation.

2.1 INFRASTRUCTURE

The analysis of the inputs indicates that almost all participants proposed definitions that characterize the platforms according to the purpose of connecting groups and producing benefits based on the network effect. Considering the available conceptual

[4] In this sense, Poell, Nieborg, and Van Djick (2019) define digital platforms as "(re-)programmable digital infrastructures that facilitate and shape personalized interactions among end-users and complementaries, organized through the systematic collection, algorithmic processing, monetization, and circulation of data" (p. 4), which infers that the conceptualization of platforms can be composed of elements that refer to: i) a **basic infrastructure**; ii) **involved and related actors**; iii) **characteristics of their operationalization, such as the processing of personal data and the use of Artificial Intelligence tools**" [*our emphasis*]. Srnicek (2016) added to this definition the classification of the purpose or function of the platforms, stating that platforms are corporate actors that present themselves as mere **technological-communication intermediaries** and that articulate a relation of services and business between individuals or institutions, assuming the elimination of a set of platforms that do not have the purpose of intermediation. Rochet and Tirole (2003) highlight that platforms are characterized by two- or multi-sided markets that generate mutual benefits through the network effect, which is why the network effect was added to the possible characteristics as a variable, alongside data processing and AI.

framework[5], which proposes the division of digital platforms into two groups (transactional platforms and innovation platforms)[6], most definitions mentioned in the Consultation are consistent with the concept of transactional platforms. However, the term was not mentioned explicitly in the Consultation.

On the other hand, the concept of and the actors involved in **innovation platforms**, which are commonly used to group technologies such as Android and iOS, were seldom mentioned in the inputs. However, that does not mean the respondents agreed that such technologies should be excluded from regulation. The few mentions of such platforms (and operating systems) need to be highlighted as the impacts of this market are structurally relevant and include not only competitive issues but also those related to the strengthening of the production of local applications and developer communities.

Relative to transaction platforms, the inputs pointed to aspects of their operations, proposing diverse arrangements to characterize them. Gabriel Capellari, from the scientific and technical community, for instance, mentioned some platform characteristics, such as the possibility of connecting apparently dispersed groups through digital communication technologies: "Digital platforms are online services that **allow the connection** between users and suppliers of goods, services, or information through **digital communication technologies**" [*our emphasis*].

---

[5] For methodological purposes, the contribution of Gawer (2019) is considered, which proposes the principles of "openness," "sharing," and "control" to characterize the configuration of the technological infrastructure of platforms. Gawer analyzes the platforms according to the socio-technical arrangements that define them and establishes two categories: **transaction platforms and innovation platforms**.

[6] In short, **transaction platforms are intended to intermediate transactions between different groups, while innovation platforms act as a foundation for other actors to create new technologies, products, and services** (GAWER, 2019). Gawer proposes a platform classification based on the principles related to their technological design configuration. The more open the code and the more unfinished the technical design, the more the platform could foster distributed innovations.

Roseli Fígaro (USP), from the scientific and technical community, pointed to the aspect related to the business nature of digital platforms and the separation between the set of technologies offered by companies managing digital platforms and the Internet:

> *[...] platforms are* ***companies that use Internet technology to connect their interface applications and structure specific businesses****. They are a new type of company because* ***they use the Internet environment as a web****; that is, they provide dispersed access to goods and services and collect, market, and control data [our emphasis].*

Other inputs to the consultation, such as that of Jonas Valente from the University of Brasília (UnB), reinforced that the idea of connecting groups and individuals is one of the key elements that define digital platforms, proposing that they are active mediators that operate on a connected digital technological base:

> *[...] technological systems that act as* ***active mediators of interactions****, communication, and transactions between individuals and organizations* ***operating on a connected digital technological basis****, especially within the Internet, providing services built on these connections,* ***strongly supported by data collection and processing and marked by network effects*** *[our emphasis].*

Some inputs, such as that of CTS-FGV[7], however, go beyond the concepts of transaction and innovation platforms, associating the modular and flexible nature of the platforms' technological infrastructures with the coexistence and interdependence of multiple actors and products or services under the *ecosystem* concept in the context of digital platforms.

In this sense, two technical characteristics prevail in digital platforms: modularity and interconnectivity, which allow complementarities that benefit the platform, the suppliers of complementary inputs (also called complements), and a

[7] (Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas) Center for Technology and Society of Getúlio Vargas Foundation.

set of participants affected by its infrastructure[8]. From this perspective, it is a unifying structure, viewing the ecosystem as a group of companies dealing with unique or supermodular complementarities in which elements connect and interact.

Therefore, several common aspects relative to platform infrastructure were identified in the inputs, such as the operation on a digital basis, usually connected over the Internet in a flexible and adaptable manner – albeit this only applies to platform owners, as in the case of transaction platforms.

2.2 ACTORS AND THEIR RELATIONS ON THE PLATFORMS

The inputs were grouped into two general categories of actors (**users and complementors**). Literature defines complementors as "developers of complementary products or services" (GAWER, 2014). The CTS/FGV input suggested a similar concept, proposing the term '**complements**,' i.e., those who provide complementary inputs. That is a broader approach and stems from the debate on the digital platform ecosystem proposed by the CTS/FGV.

As part of this definition effort, some participants mentioned that digital platforms mediate diverse agents, and the inputs included references to the "two-sided market" concept[9], identifying, on the one hand, service or product providers and, on the other, consumers or users of such services or products. Telefônica Brasil S.A.'s input illustrates one of these perspectives:

---

[8] According to CTS/FGV's input, modularity may be understood as "a property of the system that measures the degree to which densely linked compartments in a system can be dissociated into separate communities or groups that interact more with each other than with other communities." On the other hand, interconnectivity refers to "how different species within an ecosystem relate to each other."

[9] As explained in the CTS/FGV input, the two-sided market concept, frequently mentioned in the consultation, was introduced by Rochet and Tirole (2003). According to CTS/FGV, "the authors describe such markets as those where the platform may affect the transaction volume by charging higher prices on one side of the market and proportionally reducing the price paid by the other side. In other words, marketplaces for platforms are designed to bring both sides on board. The reason is that platform transaction volume and profits depend not only on the total price charged to the parties but also on the pricing structure."

> *Two-sided markets are economic models where **two groups of economic agents** benefit each other by interacting through an intermediary platform. Such markets are characterized by the presence of two interdependent sides or groups of users, which depend on each other's presence to derive value from the platform. One side consists of the suppliers of a product or service, while the other consists of consumers or users of that product or service [our emphasis].*

Other inputs used similar terms to describe the actors involved. DiraCom[10] stated that "platforms involve different agents, producers, users, and intermediaries," and Tatiana Dourado from INCT.DD[11] wrote that platforms "connect different parties, such as regular users, advertisers, and developers." The input[12] of the media business associations[13] proposed that "in terms of regulation, digital platforms are defined as economic agents operating on the Internet that connect or facilitate interactions between two or more groups of users, individuals, and legal entities."

Although some inputs did not explicitly mention "multi-sided markets" or a similar term, they suggested that digital platforms mediate relations between "users and suppliers of goods,

[10] Direito à Comunicação e Democracia (Communication Rights and Democracy), third sector not-for-profit organization for the promotion of rights on the Internet.

[11] Instituto Nacional de Ciência e Tecnologia em Democracia (Digital National Institute of Science and Technology in Digital Democracy), network of academic researchers on digital democracy and governance.

[12] The input was submitted by ABERT, on behalf of all the organizations listed below and is referred to as the joint input of "traditional media company associations" in this report.

[13] It comprises Associação Brasileira de Emissoras de Rádio e Televisão (ABERT, Brazilian Association of Radio and Television Broadcasters), Associação Nacional de Jornais (ANJ, Brazilian Newspaper Association), Associação Nacional de Editores de Revistas (ANER, Brazilian Association of Magazine Publishers), Associação Brasileira de Rádio e Televisão (ABRATEL, Brazilian Association of Radio and TV Broadcasters), Federação Nacional de Empresas de Rádio e Televisão (FENAERT, Brazilian Federation of Radio and TV Companies), Federação Nacional de Empresas de Jornais e Revistas (FENAJORE, Brazilian National Federation of Newspaper and Magazine Companies), and Confederação Nacional de Comunicação Social (CNCOM, Brazilian Media Confederation).

services, or information," as stated by Gabriel Capellari and the INCT.DD[14] or between "people and companies," according to Fernanda Hoffmann (UFRGS, Federal University of Rio Grande do Sul). DEIN[15] asserted that platforms provide a "connection between individuals and companies."[16] Therefore, this shows that several participants consider the commercial aspect of platforms relevant, at least within the scope of the regulatory debate.

Actors were mentioned in broader terms, such as "multiple sides" or "diverse actors," but their roles in the ecosystem were not specified. IRIS[17], for instance, stated that platforms intermediate interactions and transactions among different user groups, and Idec[18] also referred to the two or more sides of that relationship, proposing the concept of "consumer-users."[19]

Another concept addressed was 'intermediation.' Telefônica Brasil S.A., for instance, said that "telecom operators act as intermediaries between content producers and end consumers, managing the infrastructure and offering telephone, Internet, and television services to users." On the other hand, DiraCom argued that the intermediation carried out by digital platforms, unlike telecom companies, is active, which is precisely one of the central characteristics of digital platforms. Likewise, CTS/FGV's input described how the intermediation of different sides may determine market dynamics and involves a specific relationship among economic agents:

---

[14] Instituto Brasileiro de Políticas Digitais (Brazilian Institute of Digital Policies).

[15] Departamento de Transformação Digital (Department of Digital Transformation and Innovation of the Ministry of Industrial Development, Innovation, Commerce, and Services).

[16] DEIN suggested defining digital platforms according to two primary attributes: connection between individuals or companies and network effects.

[17] Instituto de Referência em Internet e Sociedade (Internet and Society Reference Institute).

[18] Instituto de Defesa dos Consumidores (Institute for Consumer Protection)

[19] Idec's input reads: "Digital platforms are (meta) organizations that mediate and facilitate relations that generate value by reducing procurement and transaction costs by combining and enabling transactions between two or more groups (also known as sides), taking advantage of economies of scope in the demands of the different sides of the platforms and promoting network externalities."

> *[...] two-sided markets differ considerably from multi-product markets, in which consumers internalize indirect network effects by purchasing related products (such as the case of razors and blades); they also differ from markets where buyers and sellers can trade with each other since this would undermine the platform's role in setting the best prices [...] Therefore, the two-sided nature of these markets is a matter of degree, i.e., it depends on the platform's capacity to influence [sales] volume by changing the price structure: companies become platforms not due to their nature, but by conscious choice, as they establish a non-neutral price structure.*

Therefore, this set of inputs implies that, although telecom operators act as the primary infrastructure required for developing digital platform activities, they do not carry out "active" intermediation, which may influence conditions on all sides that characterize such platforms. In other words, the role played by Internet access providers differs from that played by digital platforms.

On the other hand, although not disagreeing with the differences between telecom operators and digital platforms, TelComp[20] suggested considering that such differences present nuances:

> *[...] In some cases, the separation between the services provided by telecom companies and a segment of Internet companies/digital platforms has become flimsy and subtle, notably regarding the provision of communication, which has led to the replacement of traditional voice and messaging services by the use, for instance, of the voice and messaging functionality of OTT instant messaging application by virtually the entire Brazilian population.*

Lastly, CTS/FGV argued that applying the concept of a "two-sided market" – typically used in economic and competition regulations – to digital platforms, companies that "operate on only one side," such as WhatsApp and other messaging applications, may not be covered by the regulation. The inputs

[20] TelComp: not-for-profit organization representing 70 telecom companies.

on this topic did not explicitly state whether they agreed that the regulation should exclude or include companies with that profile. However, the issue raised seems to emphasize the need for an unambiguous definition of digital platforms to establish the regulation scope, should the term be adopted in legal norms.

2.3 PLATFORM CHARACTERISTICS

When conceptualizing the term, the aspects related to a service typology and operating models (commercial or not) mentioned in the inputs were organized into two topics to identify digital platform characteristics: i) **data-intensive and AI technologies** and ii) **network effects and economies of scope**.

2.3.1 USE OF DATA-INTENSIVE AND AI TECHNOLOGIES

The use of data-intensive technologies was frequently mentioned in the consultation participants' proposals for a definition of digital platforms. According to Rafael Evangelista[21], from the scientific and technical community, citing a published definition[22], asserted that digital platforms – despite the diversity of services and functions they provide – are characterized by some common primary functions, such as systematic collection, algorithmic processing, monetization, and circulation of data:

> ***Systematic data collection**: platforms collect large volumes of user data, such as personal information, online behaviors, preferences, interactions, and many others.*
>
> ***Algorithmic processing**: the collected data are processed by complex algorithms that can analyze, classify, and interpret this information for various purposes.*

[21] Professor and researcher at Universidade Estadual de Campinas (UNICAMP, State University of Campinas)

[22] Rafael Evangelista's input reads: "The most consensual technical definition is that presented in the article "Platforms", published in the German journal Internet Policy Review (IPR), where platforms are defined as '(re-)programmable digital infrastructures that facilitate and shape personalized interactions among end-users and complementors, organized through the systematic collection, algorithmic processing, monetization, and circulation of data.'"

> ***Data monetization**: digital platforms use the collected and processed data to generate revenue. This can be done in various ways, such as selling targeted ads, offering premium services, selling data to third parties, and more.*
>
> ***Data circulation**: data not only remains on the platform but is also circulated. It may involve sharing data with other platforms, companies, or individuals or making it available to users in ways that encourage interaction and engagement [our emphasis].*

Other scientific and technical community participants also mentioned the essentiality of data processing for the platforms' business model. Jonas Valente (UnB) asserted that services based on connections between individuals and organizations using connected digital technology are "strongly based on data collection and processing, and marked by network effects." Roseli Fígaro (USP) pointed in the same direction and argued that "data are one of the structural pillars of the operating logic of these new companies." According to Fernanda Hoffman (UFRGS), the business model of digital platforms involves "using algorithms that aim to maximize the use of the platform and the use of people's private information both for the company's actions to generate profit and for third-party actions intermediated by the environment."

CTS/FGV argued that data processing is essential for the personalization of mediated relationships, as well as for the personalization of consumers, thereby becoming critical infrastructures for value generation:

> *The opportunity to capture users' data and attention allows these companies **to intermediate transactions with unparalleled levels of personalization, shape markets around increasingly specific consumer profiles, and leverage their power in secondary markets**. This creates a race among a few market makers, which become key infrastructures to generate value and allow high transaction volumes [our emphasis].*

Such characteristics were also mentioned in the third sector's inputs. According to DiraCom, platforms explore transactions between users and producers to process data and generate

information *about the segments in which they operate,* thereby contributing to optimizing the services and products they offer, reusing the data to create barriers to the entry of competitors, and to expand their business into other segments. Idec also mentioned intensive data processing, highlighting the significance of these assets for allegedly free platforms. According to Idec, in such cases, "the value is extracted from user-consumers through the massive collection and processing of data for marketing and targeted advertising purposes."

In the business sector, media company associations also highlight the role of data as an input:

> *[It] may be proposed that, in terms of regulation, digital platforms are defined as economic agents operating on the Internet that connect or facilitate the interaction between two or more groups of users (individuals and/or legal entities). **Through data processing, they appropriate a valuable, fundamental, and strategic resource**, with direct and indirect network effects, and monetize themselves by selling ads and paying commissions and bonuses, among other forms of remuneration and business models [our emphasis].*

Lastly, José Antonio Galhardo, from the government sector, suggests a parallel with the definition applied for FinTech (Financial Technology) platforms, described as "activities driven by four underlying technologies broadly called 'ABCD': *Artificial Intelligence, Big Data, Cloud Services, and Distributed Ledger Technologies.*"

It is, therefore, noted that, according to the opinions of several participants, massive data processing through the intensive use of AI technologies is an essential characteristic of the definition of digital platforms.

2.3.2 NETWORK EFFECTS AND ECONOMIES OF SCOPE

Some participants said that taking advantage of network effects is an essential characteristic of digital platforms. Network effects may be direct or indirect: the direct effect is produced within the same group of users, i.e., the platform becomes more attractive as the number of users grows, such as in the case

of digital social networks, while the indirect effect is typical of platforms that intermediate transactions (such as Amazon Marketplace and Booking.com) and those whose revenue model is based on advertising (such as YouTube). Platform owners can also choose to exploit both types of network effects (e.g., Facebook) or none at all (e.g., Netflix) (NOOREN *et al*., 2018).

According to DEIN's input, a digital platform is an entity that gathers economic agents and actively generates network effects among them, which means that the value of a network is related to its dimension, i.e., the "impact that an additional user of a product or service, or an additional participant in an interaction, has on the value that other users or participants attribute to this product, service, or interaction." Network effects generate attraction loops, winner-takes-all dynamics, and growth strategies.

Media company associations and Abranet[23] also mentioned that platforms benefit from direct and indirect network effects when connecting users. Likewise, Telefônica Brasil S.A. stated that "the greater the number of users that access the platform, the greater the demand and added value of the product or service offered, which enables greater economies of scale."[24]

CTS/FGV, from the scientific and technical community, mentioned the recognized definition of Rochet and Tirole (2003), who stated that an "essential characteristic is the presence of indirect network effects, particularly its adoption and utilization by users (from one side of the platform to the other), and the absence of internalization of such effects by the users." In this sense, it may be inferred that adopting indirect network effects as a requirement for defining digital platforms would imply the exclusion of some companies typically recognized as digital platforms, such as Netflix, which, although they connect different groups, do not internalize these effects.

[23] Associação Brasileira de Internet (Brazilian Internet Association), a not-for-profit civil organization that provides support to business organizations.

[24] According to Nooren *et al.* (2018), economies of scale mean that the average cost declines as the number of users increases, and this effect is more pronounced in digital platforms as marginal costs are close to zero.

Finally, Idec mentions, in addition to promoting network externalities, the use of economies of scope[25] in the demands of the different sides of the platforms.

2.4 CHALLENGES OF USING THE TERM 'DIGITAL PLATFORMS' IN REGULATION

Some inputs, however, consider that using the term 'digital platforms' is unsuitable for regulation, mainly due to its scope and challenging definition.

According to CEPI/FGV, finding a clear definition of digital platforms that would delimit who will be subject to regulation is challenging due to the changeable nature of platforms' business models. Therefore, over-restrictive definitions may quickly make the regulation obsolete or encourage "perverse innovation," i.e., when a platform changes its business model to escape the rules, preserving the risks. Therefore, it suggests that the regulation "should work with well-defined platform types and does not necessarily require a generic digital platform legal concept." CEPI/FGV states that should a generic platform concept be adopted, it must be sufficiently broad to include different platform types and essential characteristics.

Business associations have also expressed reservations about the use of the term. Abranet argued that the definition of digital platforms is useless for regulatory purposes. It asserted that proper regulation requires acknowledging the plurality of actors in the digital ecosystem, defending using asymmetric regulation, and focusing on actors that provide core platform services or gatekeepers[26]. ALAI and Câmara-e.net pointed out that there are diverse definitions of digital platforms, which are often applied randomly and may have different meanings in different contexts. According to those business associations,

---

[25] According to Nooren *et al.* (2018), economies of scale mean that the average cost declines as the number of different goods and services are offered, and are especially relevant in services based on data mining and processing and when the company operates on multiple platforms, creating synergies through user data.

[26] In Brazil, the term core platform services were translated as 'controle essential de acesso' or essential control access.

the term does not help identify a market or group of markets in competitive analysis either. Therefore, given that companies labeled as digital platforms include several sectors operating in the physical and digital space, a regulation applied solely to online companies or services may have disproportionate effects.

IP.rec[27], from the third sector, proposed abiding by the "classification established in the Marco Civil da Internet (MCI), which divides technological intermediaries into connection or application providers," adding new subtypes to this category and establishing exceptions to the general rule of Art. 19 of the MCI (BRASIL, 2014). It added that their proposal aims at achieving terminological consistency based on the assumption that avoiding antinomies and gaps among legislations is critical.

Therefore, the concerns on the use of the term focused either on its generic use for regulatory purposes and not on the actors commonly considered as digital platforms, or on the assumption that digital platforms do not even need to be subject to regulation. In general, this group of inputs considered it essential to focus on platform types and specific actors and their products and services.

3 PLATFORM TYPES (DIGITAL PLATFORM DIMENSIONS)

The digital platform dimensions mentioned in the inputs were organized, for summary purposes, into four categories, aiming at supporting decision-making as to the scope of possible regulatory initiatives[28]: i) type of service offered; ii) legal nature of digital platforms; iii) business model characteristics; and iv) area of activity or market. These four categories are described below.

---

[27] Instituto de Pesquisa em Direito e Tecnologia do Recife (Law and Technology Research Institute of Recife).

[28] Some inputs proposed other categories that contributed to the organization of the report. Abranet, for instance, mentioned that "Digital services may differ in the size of the community involved, target audience, entry method, sector covered, geographic reach, need for greater or lesser data traffic, as well as offer and payment methods." Everton Rodrigues, from the third sector, listed eight dimension categories: "1) Purpose; 2) Participants; 3) Interactions; 4) Business Models; 5) Technological Architecture; 6) Regulation and Governance; 7) Social and Economic Impacts; and 8) Management of user data."

3.1 TYPE OF SERVICE OFFERED

The "type of service offered" dimension characterizes the functionalities offered by technological design and made available by a digital platform. Some types, such as social media, e-commerce, and messaging services, are widely known. Although well-known, others, such as content providers, news providers, and streaming platforms, significantly intersect, making it difficult to classify them for regulatory scoping purposes. In this respect, Alexander de Souza Moraes, from UEMS[29], asserted that "the term 'digital platforms' should be understood in a broad sense, **encompassing social media, e-commerce, news outlets, search engines, messaging applications, including any business model applied**" [*our emphasis*].

The association of business models with service types made by Moraes illustrates the vast diversity of the terms to name the dimensions proposed by the consultation. Some inputs mentioned the need to consider the diversity of digital platform service types offered and business models for regulation purposes.

Abranet referred to the classification developed in the scope of Bill 2,630 (BRASIL, 2020) as a reference for excluding some services from digital platform regulations. According to Abranet, that bill of law:

> *[...] lists as exceptions to the classification for regulatory purposes providers whose primary activity is a) electronic commerce; b) holding closed video or voice meetings; c) not-for-profit online encyclopedias; d) scientific and educational repositories; e) open-source software development and sharing platforms; f) searching and making available data obtained from public authorities; and g) online gaming and betting platforms. Furthermore, financial and payment platforms are also suggested as an exception to regulation, as they are already subject to sectoral regulation.*

Bill N. 2,630 (BRASIL, 2020) proposes to define the regulatory scope according to the typology of the services offered by companies that manage the technological infrastructure. In this

[29] Universidade Estadual do Mato Grosso (University of the State of Mato Grosso.)

sense, some inputs used the term 'digital services', referring to the Digital Services Act (DSA) or to the Digital Markets Act (DMA) both approved by the European Commission. This was the case of the input of traditional media associations, which directly quoted the core platform services listed in the DMA:

> *[...] 1.1) online intermediation services; 1.2) search engines; 1.3) online social networking services; 1.4) video-sharing platform services; 1.5) number-independent interpersonal communication services; 1.6) operating systems; 1.7) web browsers; 1.8) virtual assistants; 1.9) cloud computing services; 1.10) online advertising services and digital advertising intermediation.*

The input also asserted that some platforms may not fit into the types above because they do not:

> *[...] pose risks to users and markets (such as scientific and educational repositories, not-for-profit online encyclopedias, open-source software development and sharing platforms, platforms that provide access to public authority data, etc.).*

Some entities emphasized the risk of over-specifying service types, creating loopholes that would allow excluding some companies from the scope of a regulatory initiative. For instance, the input of CTS/FGV stated, "Before defining these concepts, it should be emphasized that those are broad definitions and that excluding certain platform types from the regulation scope is not advisable."

On the other hand, some inputs, such as Abranet's, proposed developing clear definitions of service types to prevent legal uncertainty. Abranet again suggests the definitions present in one of the versions of Bill N. 2,630 (BRASIL, 2020):

> *In this sense, "**social media**" is defined as "an Internet application whose main purpose is to allow users to share and circulate works, opinions, and information conveyed as text or image, audio, or audiovisual files, on a single platform through connected or accessible accounts in an articulated manner, allowing users to connect."*

> *A "**search engine**" is "an Internet application that allows the search of content created by third parties and available on the Internet using keywords. It groups, organizes, and classifies the results according to the platform's relevance criteria, independent account creation, user profiles, or any other individual record. It includes content indexers and omits the search tools exclusively intended for e-commerce functionalities."*
>
> *Finally, "**instant messaging**" is "an Internet application whose main purpose is to send instant messages to specific recipients, including the offer or sale of products or services and those protected by end-to-end encryption, except for electronic mail services" [our emphasis].*

Some service types offered by platforms may be considered essential or pose a greater risk to society and, therefore, require further regulatory consideration, such as those described in Bill N. 2,630 (BRASIL, 2020). The inputs show that platform typology is confused with regulatory asymmetry when discussing platform classification criteria.

3.2 THE LEGAL NATURE OF DIGITAL PLATFORMS

A few inputs briefly mentioned the importance of considering the legal nature of digital platforms, such as governmental and not-for-profit platforms. However, several inputs suggested that the scope of any regulatory initiative should include only commercial and for-profit platforms. Felipe Braga, from the scientific and technical community, affirmed that the dimensions of the platforms should be taken into account, including whether they are public or private, as well as their hosting location.

DiraCom, from the perspective of public policy implementation, highlighted the importance of incentivizing public platforms, as the State should democratize "the use of public infrastructure, sharing it with the greatest possible number of agents, and consider other elements, such as data custody in the national territory."

3.3 BUSINESS MODEL CHARACTERISTICS

The characteristics of digital platform business models are essential not only to define the scope of a possible regulatory framework but also for the adequate application of the principle of regulatory asymmetry. In this sense, Rafael Evangelista (Unicamp) referred to the digital platform typology proposed by Snricek (2016), who identifies five main types, namely:

> ***Advertising Platforms**: platforms that realize profit by capturing and storing user data to display related ads. Examples include Google and Facebook.*
>
> ***Cloud Platforms**: companies that build massive computing infrastructures for their operations and later offer this infrastructure as services to other companies. Examples include Amazon, Google, and Microsoft.*
>
> ***Product Platforms**: dedicated to renting physical goods, such as cars, or information goods, such as music, movies, etc. One example is Rolls Royce, which charges a fee for the rental of propellers per hour of use.*
>
> ***Lean Platforms**: do not own the product or service offered. Examples include Uber, the world's largest ride-hailing company, which does not own any cars, and Airbnb, which does not own any hotel rooms.*
>
> ***Industrial Platforms**: present the best possibility for future expansion, given the expectations of technological development of the so-called Internet of Things. They apply what in Germany is called "Industry 4.0", a process of information interconnection of each component involved in the industrial process with no interference of workers or managers, thereby achieving an optimal labor and production cost reduction.*

Some inputs, such DEIN's, emphasized the need to consider

> *[...] in all possible dimensions, [...] their payment methods, their relationship patterns with users, among others."* Other inputs mentioned the undesirable economic effects of the dominant market position of some digital platforms, identifying elements to be considered by legislators when addressing the harmful effects of these companies'

> business models, such as "the value it generates for users and its relationship with customers and competitors."

As such issues involve the classification of the risks posed by platforms, they are further addressed in the item on risk classification and asymmetric regulation.

Traditional media company associations, such as ABERT, ANJ, ANER, ABRATEL, FENAERT, FENAJORE, and CNCOM, affirmed that the differentiation between digital platforms and other media companies is incorrect. According to their joint statement, such differentiation is rhetorical and aims to exempt digital companies from the regulations currently applicable to media companies. They argued that it introduces regulatory asymmetries that favor digital platforms: "In Brazil, this is clearly the case of **digital platforms** primarily living off advertising revenues by selling advertising spaces and placements to advertisers and that **refuse to be considered advertising channels**" [*our emphasis*].

Some inputs suggested analytical approaches to digital platform business models based on the purpose of their activities. CTS/FGV, for instance, considered the dimensions that derive from qualities of the "network effect" and highlighted:

> *[the] importance of differentiating cases in which network externalities flow in a single direction (when the coordinating company is called an "audience-providing platform") from those in which both parties benefit from such externalities (when the coordinating company is called a "matching platform").*

The source of the platforms' funds was also mentioned as a relevant dimension, particularly the relationship between own funds and third-party funds. That entails considering the platform's corporate structure, which aids in evaluating its market position, the source of the funds that finance its operations in a given country, its development stage, its expansion strategies and remuneration mechanisms, etc. (SILVA NETO, CHIARINI, and RIBEIRO, 2023). One of the categories mentioned in the consultation was platform source, but no elements were described to define it. A possible consideration could be the location of the company's headquarters and the territorial externalities driven by it, such as the payment of taxes and fees, the promotion of innovation, effects on research and development, etc.

3.4 ACTIVITY FIELD OR MARKET

Some contributions analyzed the regulatory challenge to assess market failures from a more traditional economic perspective. That was the perspective postulated by ALAI, for example, when considering that:

> ***There are no "digital markets" from an antitrust perspective****. Economic developments are more accurately described as the dissemination of "digital" technologies throughout the economy, such as in the advertising, agriculture, automotive, manufacturing, and retail industries. Companies often called "big techs" are best described as pioneers in adopting technology in very different industries [our emphasis].*

According to Telefônica Brasil S.A., the term 'digital platforms' describes a type of technological infrastructure and proposes the term "digital ecosystem industries" and sectors such as "transportation (Uber, 99), lodging (Airbnb), e-commerce (Amazon), social media (Facebook), and many other traditional markets, such as payments (e.g., credit cards), as well as the telecommunications market itself."

4 RISK CLASSIFICATION AND ASYMMETRIC REGULATION (CRITERIA FOR CLASSIFYING DIGITAL PLATFORMS)

Considering that the term 'digital platform' encompasses multiple actors, several participants suggest adopting an asymmetric regulation, i.e., that only the groups of actors that may exercise market power in the digital ecosystem should be subject to regulatory provisions. According to DEIN, a balanced asymmetric regulation would protect small businesses while not neglecting to oversee the key players. On the other hand, Gabriel Capellari, from the scientific and technical community, stated that classifying digital platforms according to their characteristics and potential risks allows for a more accurate and balanced approach when establishing their regulatory obligations. Therefore, the challenges lie in establishing criteria for identifying which actors deserve greater regulatory attention due to the societal risks they pose.

Some participants emphasized that such criteria must not be individually addressed but be combined in a cumulative or alternative manner and broadly grouped as gatekeepers (Topic 4.5). Abranet, for instance, suggested

> *An asymmetric regulation applicable only to specific companies, i.e., those holding essential access control. The concept is structured around three dimensions: i)* ***provision of an essential platform service****, as set out in a mandatory list; ii) compliance with the* ***criteria for the volume*** *of end users and professional users, in absolute numbers or proportional to the national population, for at least the last three fiscal years; and iii)* ***holding a dominant market position****, also for at least the last three fiscal years [our emphasis].*

Idec pointed out the need for cumulative criteria (such as gatekeeper and number of users) and alternative criteria (such as revenue), in addition to escape valves, when companies with a significant impact on society do not meet these criteria due to market dynamics. DEIN suggested an "assortment of criteria" that allow defining the specific profile of the agent subject to regulation, such as revenue, number of users, essential access control, and company uniqueness in a given market or different economic segments.

On the other hand, Câmara-e.net opposed the broad adoption of such criteria. It considers that since there is no uniform definition of "digital platform," factors such as "market share," "market value," and "number of users" do not, *per se*, provide valuable conclusions on the risks posed by the types of products or services offered by a given provider. ALAI criticized the principle of asymmetric regulation despite not explicitly mentioning it. According to ALAI, regulation should "be neutral and equally applied to foster competition based on merit, encouraging private agents to outperform each other to win customers by providing innovative, high-quality, low-cost products with better services."

4.1 MARKET SHARE

According to LABID/UFBA[30] and Abranet, market share could be used as a market indicator of the platform's relevance in its industry. Therefore, its analysis should be included when evaluating a platform's position in relevant markets. Gabriel Capellari added that platforms with a dominant position in a given market can exercise power and impose unfavorable conditions on users and competitors.

Idec, DiraCom, and Black Women Bloggers[31] agreed that market share is essential to classify digital platforms and identify large platforms or platforms with significant market power, which is essential to understand their impact on users and the digital economy, especially in a context that strongly tends to create monopolies.

DiraCom further suggested referring to the provisions of Law 12,529 (Competition Defense Law) (BRASIL, 2011), which assume that companies or corporations that control 20% or more of the relevant market are assumed to have a dominant position in order to classify companies based on to that criterion in an impartial manner. Idec added that regulation needs to create additional mechanisms that assess vertical integration, particularly the conglomerate effect of the corporate groups involved. According to Idec, the entry of companies or businesses into ecosystems is directly influenced by the direct and indirect network effects of the platforms, such as WhatsApp Pay (currently with less than 20% of the market, but vertically integrated with WhatsApp in a related market), or Meta Threads (integrated to the Meta corporate group and, in particular, to Instagram.)

In a joint statement, the traditional media business associations also stated that applying the 'relevant market' criterion hinders classification as digital markets are closely interrelated, and, therefore, network and scale effects often "go beyond the relevant markets, placing digital platforms in a dominant position even in markets where their market share is not high."

[30] Laboratório de Inovação e Direitos Digitais da Universidade Federal da Bahia (Innovation and Digital Rights Laboratory of the Federal University of Bahia).

[31] Blogueiras Negras, independent black media group.

According to Idec, using 'relevant market' as a classification criterion requires a previous analysis of the market structure before designating the regulatory target, i.e., the market share of a digital platform should be analyzed to determine whether it should be subject to the regulation prior to any illicit act assessments, increasing the complexity of the analysis by the regulating body. Therefore, both Idec and traditional media associations recommend that alternative criteria supplement the market share criterion to aid the definition of the regulatory target.

Other respondents, although agreeing with using relevant market or market share as classification criteria, expressed concerns with their application in the digital context. For instance, Jonas Valente (UnB) highlights that market share is a crucial indicator for understanding platform power, but "the capability of those agents to operate in different markets challenge the traditional delimitation of each market." Valente recommended considering market shares in specific and broader markets, including platform types, digital platforms in general, and Internet applications. Abranet proposed adopting market share as a criterion to determine which platforms qualify for a gatekeeper regulatory regime. It argues, however, that given the dynamic nature of digital markets, a dominant position should be assumed when the agent holds more than 50% of its respective relevant market. According to Abranet, this share must be held for at least the last three fiscal years to demonstrate the stability of its market dominance position.

As previously mentioned, media company associations understand that the initial obstacle to the use of the relevant market is the very definition of the relevant markets in which digital platforms operate:

> *Some elements make this task very difficult: i) some digital markets are highly dynamic or unknown, and, therefore, stringent and tight regulations may quickly become outdated [...] iii) some factors may place a platform in a privileged/dominant position, regardless its market share in digital markets, such as the control of essential infrastructures, intellectual property rights, long-term exclusive contracts with essential suppliers, and even public concessions.*

Therefore, traditional media associations recommended considering elements other than market share, such as the number of users, to establish market dominance. They highlighted that, in addition to the relative presumption of a dominant position when a company has 20% or more of the market share, the Brazilian competition law establishes the presumption of dominance when "a company or group of companies is capable of unilaterally or coordinately changing market conditions," which allows for considering other elements to determine the dominant position of an agent.

CTS/FGV defended that market share and the number of users are essential to determine which companies should comply with the obligations arising from asymmetric regulation based on market power. However, there were differences and shades as to the metrics suggested to measure market power, which is considered to be only one of its defining elements. According to CTS/FGV, alternative metrics may be applied to assess market share[32] and cite as an example the actions of the Brazilian competition authority (CADE), which has already identified some indicators for the presence of a dominant position, such as transaction volume, download of a software application, active user, web visit, and click numbers.

4.2 MARKET VALUE OR REVENUE

In the scope of the discussions on the possible establishment of asymmetric regulation, several participants considered that market value and revenue are relevant for identifying platforms that hold significant power.

As explained in LABID's contribution, the market value criterion considers the perceived market value of a digital platform, reflecting its performance and position relative to its competitors. On the other hand, revenue represents the sum of the amount the company collects from exercising its commercial

[32] CTS/FGV stated that "Broadly, the following metrics alternative to market share could be used: share in the number of production assets (in terms of shares in items sold, purchased, or produced), share in capacity (in terms of total or available capacity), total market revenue share, workforce share, and share in the number of consumers."

activity during a given period[33]. Some actors, however, expressed reservations or the need to explore those criteria further.

DiraCom, for instance, maintained that market value and revenue "should be considered when assigning the classification of significant market power [to a company], establishing further responsibilities and attributions accordingly." Moreover, such criteria must be regularly assessed, taking into account the figures of the holding company and specific companies that comprise it. Likewise, Jonas Valente (UnB) considered market value a necessary criterion; however, it should be combined with platform revenue in its specific market.

However, other participants maintained that market value and revenue criteria are inadequate or insufficient. According to Elaine Marques and Leonardo Tavares from the scientific and technical community, such criteria should be used only to advise the imposition of fines and sanctions.

Idec observed that, despite being relevant, market value or revenue must not be considered alone, as such criteria are very dynamic, considering the network effects and the tendency towards monopoly in particular in the digital context. Idec illustrated these dynamics with the acquisition of WhatsApp (Meta) by Facebook, which, despite not having sufficient revenue in Brazil to be notified for concentration, already had a market share and a significant number of users.

Accordingly, media business associations argued that individual market value or revenue considerations may omit several economic operations involving digital platforms, which have their headquarters and carry out their transactions primarily abroad. Therefore, their revenues in Brazil tend to be low or zero, even though the platforms are hugely popular among Brazilian users and new entrants that may compete in related markets. The inputs also provided examples of operations that were not covered in the competitive analysis based only on revenue, such as Waze and YouTube acquired by Alphabet; Musical.ly by the TikTok group (ByteDance), and the partnership between Meta and Cielo to launch WhatsApp Pay. In this respect, the traditional media associations discussed that:

[33] There are several ways to define market value. In general, the inputs did not delve deeper into this definition.

> *Despite being more volatile, the concept of* ***market value, when combined with other criteria, may reveal the relevance of assets whose revenue and turnover are not significant yet*** *and identify acquisitions of entrants or emerging competitors by platforms already established and dominant in the sector. However, the challenge is establishing specific market value criteria [our emphasis].*

Abranet also claimed that revenue metrics are debatable. It argued that the revenue criterion fails to capture the specificities of market agents that go beyond price issues, especially in digital markets, where small companies often have significant assets and offer several services at zero prices.

In agreement with traditional media business associations, Abranet asserted that, in addition to revenue, "the concept of 'market value' allows for a less rigid assessment of digital platform size, identifying still unrecognized assets in terms of revenue/ business volume."

4.3 NUMBER OF USERS

Many respondents considered the number of users a central or relevant element for defining the regulatory scope.

CEPI/FGV asserted that number of Brazilian users is a more suitable criterion than market value, revenue, or market share, as, in general, a high number of users is directly correlated with strong platform economic power – allowing it to bear the compliance costs – and with a greater risk to Brazilian rights and institutions, because more users may be affected by moderation or come into contact with harmful content. LABID/UFBA considered that the number of users allows for evaluating and measuring the impacts of a digital platform on the public, such as disinformation and platform negotiation power vis-à-vis the advertisers, as highlighted by Alex Camacho from the scientific and technical community. Furthermore, DiraCom argued that this is a particularly relevant criterion in the context of digital markets, which are characterized by network effects, favoring the dominance of a few platforms with a high number of users.

Abranet agreed that the number of users is a relevant criterion for measuring market relevance, enabling classifying and determining which digital platforms qualify for the regulatory regime, such as the European Digital Markets Act (DMA) and the current version of Bill 2,630 (BRASIL, 2020). Abranet proposed establishing thresholds according to average numbers of:

> *[...] a) more than forty-five million end users and b) more than twenty million professional users cumulatively during the last three fiscal years. Alternatively, 20% of end users and 10% of professional users living in Brazil, according to official national statistics, in the last three fiscal years.*

Other inputs took the discussion further, proposing other metrics in addition to the number of accounts to operationalize that criterion. Traditional media associations, for instance, recommended using metrics usually associated with the audience, such as the "number of regular (daily, weekly, monthly, annual) accesses/visits, time spent on the platform, number of searches/clicks." Jonas Valente (UnB) suggested including, in addition to the number of users ***per se***, "the number of monthly active users in the country," therefore, this information should be mandatory for regulation purposes.

IP.rec, from the third sector, proposed considering the number of users for exacting fines. Lastly, the researcher Felipe Saraiva (Federal University of Pará – UFPA) pointed out that such a criterion, nevertheless, should not exempt small platforms from regulation. He argued that because many digital platforms, "notably those related to far-right extremism, despite their diminutive sizes, are able to convene and mobilize communities, impacting the society." Therefore, he defends combining other criteria with the number of users to avoid excluding relevant platforms from the regulation.

4.4 CORE PLATFORM SERVICES

Core service definitions differed among[34] participants, with some disagreements on using the criterion of 'core digital

[34] The adjective 'core' is translated as 'essencial' (essential) in Portuguese, and hence the potential confusion of 'core services' with 'essential [public] services.'

service' provision for platform classification and regulatory scope definition. However, many inputs – such as those of media company associations, LABID/UFBA, and Alex Camacho – define core digital services as those that are relevant to the country, essential for everyday life and economic operations, or essential for different actors that have no other available alternatives, thereby constituting a situation of dependence. Such a situation increases the platforms' responsibility and the need for regulation.

Idec defined core services as those "whose purpose is related to the exercise of citizenship, which should be a regulatory priority." It proposed that users' best interests should guide such services and prohibit users' data from being used for platform profit. Defining core platform services depends on the purpose of the regulation.

Abranet, in line with other regulatory initiatives such as the European DMA, argued that only a few service types require particular regulatory scrutiny. DMA provides a list of what it understands as core platform services, and only those that have a critical role associated with the concept of gatekeeper are subject to regulation, as in the case of Bill 2,630 (BRASIL, 2020), which identifies social media, search engines, and instant messaging as critical services. Abranet proposed using a similar strategy as a reference for the Brazilian regulation.

DiraCom noted, however, that the core service concept was formulated in the European context. Therefore, its applicability in Brazil requires further discussion because, in the Brazilian context, essentiality is commonly associated with providing public services that are indispensable to meeting the community's needs, which may result in obligations such as guaranteeing access provision and universality. Consequently, DiraCom stressed the importance of referring to all Brazilian legislation when defining concepts.

Researchers from the scientific and technical community also expressed reservations about using the criterion. Jonas Valente (UnB) proposed that, as platforms can spread to other markets, their regulation should include, in addition to their core services, the competitive, political, and social dimensions of corporate groups and the influence generated by this power. Murilo Ramos (UnB) stated that essentiality cannot be a defining criterion for a

digital platform unless the provision of products and services is included in the scope of public law administrative regimes.

Câmara-e.net disagreed with using the criterion as it understands that as essentiality has no single definition, the term is imprecise, increasing the risk of excessive intervention and hindering competition and innovation.

4.5 GATEKEEPERS OR ESSENTIAL ACCESS CONTROL

Many participants consider gatekeeper a central criterion for defining asymmetric regulation. Traditional media company associations, inspired mainly by the EU DMA, this approach encompasses large companies that provide core platform services and have considerable economic power, including, for instance, the capacity to connect many professional users[35] and end consumers through their services, allowing the companies to leverage their advantages, such as access to a large volume of data.

In order to be subject to this regulatory regime, Idec added that the provided services must have a significant impact on the domestic market, operate one or more gateways[36] important for customers, and enjoy an entrenched and durable position in their markets. Consequently, it is structurally difficult for competitors to challenge or dispute the position of these dominant platforms, regardless of their innovation or efficiency levels, which justifies special regulatory attention. Idec considered, however, that the criteria that classify a platform as gatekeeper are presumptions, i.e., a company that fulfills such criteria may refute them. Moreover, the criteria may designate a platform providing core services as a gatekeeper despite not meeting the presumed thresholds (as in the case of the EU DMA). According to Idec, this safety valve is critical to ensure that relevant platforms are

[35] In its input to the consultation, Abranet defined professional users as "individuals or legal entities that use the respective platform for business or professional purposes, to provide goods and services to end users – for instance, a retailer that has a business account to communicate with its customers."

[36] In Internet-related discussions, the term 'gateway' is understood as an asset that acts as an intermediary for exchanging information between two or more devices connected to the network.

not excluded from the regulation. Idec emphasized the need to combine the gatekeeper criterion with other criteria and to relate the definition of access controller to the above criteria covering service essentiality and risks to fundamental rights, particularly the number of users in the national territory and platform type.

Abranet, from the business sector, argued that only actors who hold essential access control should be subject to regulatory provisions since the other actors do not pose relevant risks and should not be subject to this specific regulation, ensuring balance and fairness and fostering innovation. It mentioned that other international laws apply similar parameters. For instance, the EU DSA establishes obligations according to activity type, size, and impact of the different market agents on the digital ecosystem, the so-called 'very large digital platforms,' and the UK Digital Markets Unit (DMU) regime, which only applies to companies holding a strategic market status, which involves having substantial entrenched lasting market power, and a significant strategic position.

As a scientific and technical community member, Jonas Valente (UnB) also stressed that it is essential to identify "the 'access control points' at which platforms operate as key regulators of information and economic flows and exercise their gatekeeper role." Valente highlighted, however, that the gatekeeper concept should include further control dimensions and anti-competitive practices, considering the agents' vertical and horizontal integration structures and strategies and how they affect other dimensions in addition to competition. Moreover, the Internet Governance Research Network (REDE) defends that the gatekeeper role should be assessed by considering the infrastructure power of platforms and not only their actions in the web layers.

4.6 SERVICE TYPES

The inputs on this subject stated that the regulation should focus on platform typologies or relevant types that significantly affect users and other social spheres (such as the economic and political spheres), which deserve greater regulatory attention. Therefore, the comments related to the specific question of the consultation on service types (Question 3, item IV) are interwoven with those made on platform types or core platform

services and, therefore, in this report, are included and described in the topics mentioned above.

5 CONCLUSION OF AXIS 1

The inputs to Axis 1 of the consultation explored the effects of adopting the term 'digital platforms' on the approaches proposed to generate solutions to the challenges posed by a sociotechnical phenomenon. Although there is broad consensus on the need to regulate platforms, establishing elements and criteria that accurately identify the object to be regulated involves a wide range of possibilities linked to different perspectives, interests, and objectives. The primary challenge is to organize the different approaches and seek agreements to make a future regulatory framework effective in addressing the identified issues.

Regarding the definition of digital platforms for regulatory purposes, the transversality of their actions mentioned in the consultation suggests that, in addition to discussing a general definition of digital platforms, a modular classification scheme that allows exploring the different regulation and public policy possibilities needs to be developed.

In that regard, based on the qualitative systematization of the consultation inputs, it is suggested that, for regulatory purposes, digital platform definition should be based on three key elements: i) **critical defining elements**, including their technological infrastructure, the actors involved, and the main characteristics of their business model; ii) their **typology**, based on the social relationships they establish (with whom they relate with and who connects with whom); and iii) their general and specific characteristics that pose significant **risk to society**.

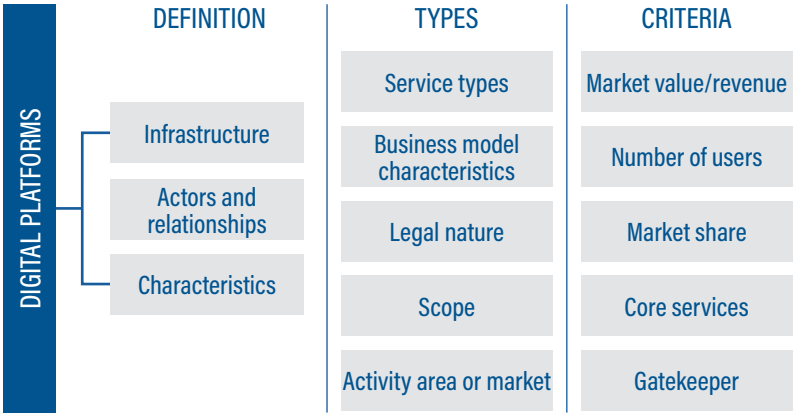
The first element (technological infrastructure) refers to platform architecture type and technological design and considers their **openness, modularity, and governance structure**. Despite their relevance in the literature, those elements were seldom mentioned in the consultation, as the inputs on infrastructure usually applied more generic terms, such as 'digital,' 'electronic,' and 'Internet.' The inputs generally focused on platforms centered on transactions between parties and did not address the so-called innovative platforms, including the application market and public infrastructures that may drive distributed innovation processes.

The second element is related to the agents' general and specific characteristics that can be used to define the scope of a possible regulatory initiative or to separate regulations by sector (for instance, establishing a specific regulation for ride-hailing platforms, another for public platforms, among other possibilities), based on the dimensions and categories associated with **service type, business model characteristics, legal nature, and areas of activity or market**.

Lastly, the third element allows for establishing **practical criteria** to determine which agents should be subject to the regulation based on the analysis of their **revenue, market value, number of users, service essentiality, and access control**. When combined, such criteria may contribute to establishing a regulation that appropriately addresses the risks of their activities without prejudice to other possible criteria and exceptions.

The diagram below seeks to organize the different categories under discussion in Axis 1 of the consultation and answer the question "who to regulate" based on the different elements that make up the definitions of digital platforms, platform types, and the criteria to identify actors that pose a greater risk to society and should be the main target of the regulation.

FIGURE 1 – CATEGORIES TO DEFINE "WHO TO REGULATE



SOURCE: PREPARED BY THE AUTHORS

5.1 CONSENSUS AND DISSENTS ON ASYMMETRIC REGULATION

The inputs received show a clear consensus that the regulation should be asymmetric, i.e., that only some groups of actors that may exercise power in the digital ecosystem should be subject to regulatory provisions. However, the challenge is clearly determining the criteria for identifying those needing greater regulatory attention.

Many participants agreed that no criteria should be individually applied to determine which digital platforms should be objects of the regulation, advocating for using cumulative and alternative criterion combinations. In general, gatekeepers were considered the main target of regulation, and the definition of this category needs to include other criteria, such as number of users, revenue, or market share. However, some participants pointed out that political, social, and technological power is exercised not only via access control but also by controlling the actions of other agents. Therefore, the gatekeeper concept should include the competitive dimension and its power in other dimensions. In this sense, a gatekeeper definition that goes beyond what was formulated in the European context (core platform service provider) should be developed to adapt it to the Brazilian regulatory needs.

In this regard, the **number of users** was the criterion that achieved the highest level of consensus. Inputs pointed out that user volume, besides measuring economic power, allows for assessing platform activities' impact and risk potentials. Moreover, the reported number of users should distinguish end users from professional users because they can shape the market on different sides and require different metrics.

The **market share** criterion – commonly applied in the competitive environment to assess dominant positions – also showed some degree of consensus. However, despite significant reservations given the complexity of the digital context, many inputs mentioned the need to develop alternative metrics to measure it other than market share based on price and to consider it another element (and not the only one) to determine market power.

Revenue was also pointed out as an essential criterion to identify market power but should not be used alone, given digital market specificities, such as zero-price markets and assets that are difficult to quantify, such as data and number of users. Some

participants, therefore, argued that the market value criterion is more appropriate than revenue; however, the definition of which elements comprise market value is complex and was not addressed in depth. According to other respondents, revenue should only be considered an alternative or additional criterion due to its limitations.

There was some degree of consensus that only some service types require particular regulatory scrutiny; however, some inputs expressed dissent on the definition of core services. It was pointed out that **core platform service** is an imported concept and could be confused with existing Brazilian legal regimes, such as essential public services. Moreover, the complex scope of digital markets would make its use difficult. Nevertheless, there is ground to believe such disagreements may be solved by formulating a more precise definition of core services and harmonizing this new concept with previous Brazilian law regimes to prevent overlaps or gaps.

Lastly, in addition to the combinations of criteria, there was a suggestion of a safety valve to prevent platforms with significant impacts on society – such as small but high-risk platforms that do not meet established criteria – from being addressed in regulation in an exceptional and justified manner.

AXIS 2 – WHAT TO REGULATE

1 INTRODUCTION

This chapter summarizes the inputs received on Axis 2 of the consultation on "what to regulate," involving questions on the risks arising from digital platform activities and their possible mitigation measures. This axis included 34 questions, organized into four major risk groups related to threats to:

i. Competition, consumer rights, abuse of economic power, and economic and data concentration;

ii. Digital sovereignty, technological development, and innovation;

iii. Decent work;

iv. Democracy and Human Rights.

Axis 2 received the highest number of inputs, with 967 total, representing 73% of the inputs. Protecting human rights and democracy received the highest number of inputs to this Axis (44% of the total), followed by the group of questions of economic nature (33%).

TABLE 4 – INPUTS ON AXIS 2

AXIS 2 TOPICS	NO. OF INPUTS	% OF THE TOTAL
Competition, consumer rights, abuse of economic power, and economic and data concentration	305	32%
Digital sovereignty, technological development, and innovation	142	15%
Decent work	67	7%
Democracy and Human Rights	453	47%
Total	967	100%

SOURCE: PREPARED BY THE AUTHORS.

2 RISKS RELATED TO THREATS TO COMPETITION, CONSUMER RIGHTS, ABUSE OF ECONOMIC POWER, AND ECONOMIC AND DATA CONCENTRATION

In general, the third sector and the scientific and technical community agreed on the relevance of the mapped risks. The government sector, despite the smaller number of inputs submitted, presented similar perspectives in recognizing these risks, while the private sector, in most cases, was divided as to whether or not recognizing those risks as relevant or existing.

Part of the private sector – such as ALAI, Câmara.e-net, and the Interactive Media Association (IAB Brasil) – argues that digital markets are characterized by intense innovation and strong competition, and in which consumer diversity and the rapid evolution of online habits offer countless opportunities for market entry. In addition, associations such as Brasscom and the Information Technology Industry Council (ITI) mentioned the benefits digital platforms bring to the economy. They emphasized that the Brazilian competition defense system is robust, comprehensive, and well-equipped to address potential anti-competitive behavior through the Administrative Council for Economic Defense (CADE) and exercises broad regulatory powers in all industries. However, they cautioned against the risks of "over-regulation," which could slow economic growth and hinder technological innovation and foreign investments.

The private sector inputs of Abranet and the media business associations pointed out other economic risks, stating that digital markets offer few contestability opportunities to smaller agents, have high exchange costs that discourage the use of other services or platforms, and "generate monopolies that hold control over the flow of information and digital services, harming competition, innovation and general well-being, which are protected legal values" (Abranet). Such opinions largely agree with those of the third sector and the scientific and technical community – with occasional disagreements, such as IBRAC (Brazilian Institute for Studies on Competition, Consumption, and International Trade).

Idec's input provided a brief list of the economic risks posed by digital platform operations, emphasizing the platforms'

> *[...] disproportionate economic power, to the detriment of 1) competition, 2) consumers, 3) innovation, and 4) protection of other rights, including fundamental rights", as well as violations "committed by 1) abusing a dominant position through exclusionary conduct (excluding current and potential competitors), 2) exploitative conduct (without necessarily excluding competitors, but harming competition and consumers), and 3) acquisition of current and potential competitors."*

Another aspect mentioned by several respondents was the effect of economic power concentration and abuse on other risk groups. For instance, the NGO Artigo 19 and Intervozes asserted that the lack of actor diversity directly affects freedom of expression. Flávia Lefèvre, in a broader sense, pointed out that market concentration in the hands of the so-called big techs has unequivocal effects on the fundamental rights guaranteed by the Brazilian Constitution (BRASIL, 1988) and increases consumers' vulnerability, "extensively harming the dignity of the human person and the safety of citizens/consumers, both individually and collectively, as well as democratic institutions in a diffuse manner."

The consultation also revealed overlaps among the mapped risks. According to some participants, data concentration may be considered one of the causes or a factor determining the risk of economic concentration and abuse of economic power, indicating they may be an "umbrella" for other risks. Moreover, potential damages to innovation have also been associated with a decline in product and service quality, as innovation is relevant when it generates product and service improvements, and the abuse of economic power may cause both risks.

2.1 RISKS ASSOCIATED WITH THE CONCENTRATION OF DATA (PERSONAL OR OTHERWISE) PROCESSING AND CRITICAL INFRASTRUCTURES FOR DATA COLLECTION, STORAGE, ANALYSIS, AND PROCESSING

Some inputs disagreed that data processing concentration is a risk, arguing that it is not the sole condition for a platform's

success. Câmara.e-net argued that access to big data is not required for market entry nor a condition for the development of a successful product, mentioning that the most popular digital platforms (Meta, Apple, Google, Amazon, Microsoft, and TikTok) initially did not have significant data volumes, as well as other services launched later (Snapchat, Twitter, Pinterest, Zoom). IAB Brasil agreed that data processing concentration is not a risk because data are non-rival goods or non-excludable goods, i.e., data are products or resources that can be consumed or used by several individuals simultaneously without reducing their availability to or usability by other individuals.

IBRAC recognized that, in some scenarios, the non-rival nature of data makes it impossible for a single platform to control its collection and processing, and, therefore, the risk of data processing concentration cannot be presumed. According to IBRAC, assessing if data is non-rival goods in a specific market should be done on a case-by-case basis.

On the other hand, traditional media company associations criticize the claim that data are non-rival goods; consequently, it is not a competitive advantage or a barrier to entry, arguing that:

> *Facts and reality clearly contradict such claims and counter the urgent concerns of governments, legislators, and competition authorities worldwide, who have devoted considerable efforts to* ***hold back or limit the leverage exerted by monopolistic platforms to the detriment of society and free competition*** *[our emphasis].*

Several participants agreed that the risks posed by the concentration of data processing and the infrastructures required for such processing are relevant for platform regulation. As highlighted in the inputs, data are essential to the economy of digital platforms, so understanding their role in the production chain is also relevant to assessing their concentration's impacts. As explained by DiraCom, data collection, storage, processing, and analysis are different stages of a production chain that, together, make up a critical infrastructure. Therefore, according to DiraCom,

> *As digitalized data, whether personal or not, is a key asset for producing, distributing, and consuming goods and*

> *services, the* ***private concentration of data processing and its critical infrastructure means submitting the capacity for the commercial or social development of goods and services to a market logic*** *[our emphasis].*

Therefore, as traditional media associations argued, data became an essential asset for the development of specific online activities, and their concentration consequently confers considerable economic power to platforms, allowing them to use data to monetize their power in other markets or indirectly sell them. Those associations explained that data usually consubstantiates the price and quality of the services provided in zero-price markets for **users** or **customers**. Hence, the abusive data collection by digital platforms when providing a service is **equivalent to overpricing or poor-quality services** in ordinary markets.

From a similar perspective, Abranet highlighted how the concentration of data collection, storage, analysis, and processing favors a few economic agents, who come to **hold valuable information that may influence the personalization of the services offered**. Using economies of scale and scope, such agents can **improve and develop new products at lower costs**, significantly raising the barriers to market entry. Jonas Valente (UnB) pointed out the capacity of those agents to use the collected data to map demand, develop new products and services, and strengthen their dominance both in specific and in broader and adjacent markets. In this context, Abranet asserted that **verticalization – common to large platforms – offers even greater data collection advantages** via interaction with their services or products and offering functionalities to third-party services that collect further data. Intervozes illustrates that situation using the recent case of the integration of Threads into Instagram, in which:

> *The focus on data (personal or otherwise) processing (collection, storage, use, analysis, etc.) impacts the ranking of a product in the platform and application markets. By linking data,* ***Meta's new social media app entered the market at an exponentially higher rank (in number of users and engagement capacity) than any other platform or app*** *aspiring to enter the same market. That constitutes unfair competition as it prevents the entry of new players [our emphasis].*

Some participants mentioned that data concentration is related to critical data processing infrastructure concentration and poses threats to national security and technological development. The NGO Artigo 19, for instance, considered that the risks of data processing concentration generate systemic risks, such as the disruption of entire national systems by a potential failure of a service, such as WhatsApp. Leonardo Cruz, from the Laboratory of Sociotechnical Studies at UFPA, also stressed the impact of such risks on data security, considering that concentration "negatively influences the technology market structure, as it affects the diversification of prices, services, and the business model itself, which values technological development."

Likewise, the researcher Tarcízio Silva (Mozilla Foundation) affirmed that data processing concentration promotes "economic, technological, and political inequalities between the large technology companies and the population of countries subject to capital and data flows." Therefore, data concentration is also related to digital sovereignty risks, as explained by Instituto da Hora:

> *Critical data collection, storage, analysis, and processing infrastructure may be subject to technical failures or outages. Failures in centralized systems may cause loss of data, service interruptions [...]. The concentration of data in the hands of a single vendor or service provider creates significant dependency.* ***When a provider runs into financial trouble, ceases its operations, or decides to discontinue services, the organizations that rely on that infrastructure may be negatively affected****, which has already happened with some educational institutions using Google Drive [our emphasis].*

The NGO DiraCom mentioned similar issues, considering that "this is a matter of the sovereignty of the people and the country; therefore, measures to prevent the concentration of this infrastructure and to require data stewardship in the Brazilian territory."

Thus, several inputs pointed out that data processing concentration may pose not only economic risks but also to sovereignty and technological development, as well as to Human Rights.

2.1.1 MITIGATION MEASURES FOR DATA CONCENTRATION RISKS

Two measures were extensively debated: i) data interoperability and ii) restriction or prevention of data sharing among companies in the same corporation. Interoperability enjoyed strong consensus among participants despite the disagreements over its implementation and scope. The restriction or prevention of data sharing among companies of the same corporate group was an object of stronger dissent and was opposed particularly by the private sector. The general argument is that potential damages and risks may be timely remediated based on the current legal framework, particularly in the competitive context.

In addition to those two mitigation measures, inputs suggested other measures.

2.1.1.1 DATA AND DIGITAL SERVICE INTEROPERABILITY

According to most inputs, digital markets are characterized by low contestability, high exchange costs, and the formation of monopolies that control information flow and digital services, potentially harming competition, innovation, and public well-being, among other assets and protected rights. Abranet argued that implementing mechanisms and business models that feed on large volumes of data makes it "virtually impossible for entrants to achieve the critical mass required to make them attractive or even to survive in digital platform markets." Likewise, traditional media business associations argued that establishing obligations that ensure the interoperability of digital services, such as data portability, reduces switching costs and enables users to try out other digital services with the least inconvenience.

According to Abranet, it allows "the user to take advantage of the data already provided to a single company to try out other digital services with the least possible inconvenience." The understanding that interoperability is an important remedy – both to prevent companies and consumers from being subject to abuse and to enable the emergence of alternative business models) is shared by several participants, such as DiraCom, Artigo 19, Electronic Frontier Foundation (EFF), Telefônica Brasil S.A., and ITI, among others. ITI, however, considered that such an obligation has a narrower scope and should not be prescriptive.

Abranet and media business associations argued that interoperability obligations must be asymmetrical, i.e., mandatory for large platforms with a significant market share and a high number of users, but applied as a good practice for other agents.

One of the most discussed topics on interoperability was the importance of **structuring and standardizing data in machine-readable formats** to make interoperability feasible. The topic was addressed by several organizations and actors, such as Abranet, Artigo 19, business media associations, Idec, DiraCom, and the researcher Tarcízio Silva. Idec cautioned that not prioritizing open protocols creates an additional exclusionary and concentrated standard in the market. Abranet advocated the establishment of data structuring obligations that support real-time portability, allowing the content to be instantly and automatically read and processed by computers and digital systems.

Artigo 19 also highlighted that the rules set out in the interoperability procedures should prioritize the standardization of such inputs to ensure the feasibility of these measures by using Application Programming Interface (API) and middleware – instruments highlighted by both Artigo 19 and Abranet. DiraCom asserted that such standards must not be proprietary and that personal data must be accessible to holders.

Another issue mentioned in the inputs was the balance between the interoperability mechanism and the multiple interests involved. Several inputs, including those of Intervozes, Idec, Tarcízio Silva (Mozilla Foundation), and Abranet, asserted that the measure must respect freedom of choice and privacy and be used as an active instrument for their protection. Abranet stated that, although interoperability benefits the market, its ultimate purpose is to ensure users' rights, especially their autonomy and self-determination, and should be available when explicitly demanded by the data owner. Idec emphasized that interoperability is essential to ensure consumers' **right to choose** and requires balancing the "use of interoperability to promote competition with the protection of personal data and consumer rights." Likewise, the researcher Tarcízio Silva proposed that interoperability rules should be centered on users and their autonomy to move data and resources to the applications and platforms they choose without labor or financial costs. Rafael

Evangelista (Unicamp) stated that content, in addition to data, needs to be interoperable within the Web.

EFF, agreeing with the mentioned protection and security reservations, affirmed that before such legal obligations are implemented, it is essential to identify platform types that offer more suitable conditions in terms of usability and security and proposed initially imposing such obligations on traditional social media applications. However, it advocated establishing barriers to the commercial exploitation of user data obtained from this interoperability.

Despite recognizing the importance of the mechanism, IBRAC expressed some reservations due to the complexity and sensitivity of that issue, particularly regarding the technical challenges and liability involved. It referred to the "Data Portability, Interoperability, and Digital Platform Competition" (2021) report of the Organization for Economic Co-Operation and Development (OECD), stressing the need to "develop of minimum standards that establish at least: i) mechanisms for identifying the data to be included, ii) the format in which they should be provided, and iii) the timeline and nature of the transfer process."

The last aspect raised in the inputs concerns the institutional arrangements required for the enforcement of interoperability, in particular, the authorities and competencies involved. Several participants underlined that the measure must comply with the provisions and principles of the Brazilian Personal Data Protection Law (LGPD; BRASIL, 2018). As IBRAC pointed out, the LGPD establishes that **the National Data Protection Authority (ANPD) is the body with the power to regulate issues related to data interoperability**. It mentioned that, per Art. 40 of the LGPD, the ANPD can establish interoperability standards for data portability, free access, security, and record retention periods, considering need and transparency criteria in particular.

According to Abranet, portability via API should be implemented by private agents regulated and supervised by the competent authorities, consisting of a private self-regulatory authority and a new multistakeholder regulatory entity (Axis 3). However, Abranet did not detail how the new authority would interrelate to ANDP's portability powers. On the other hand, traditional media business associations argued that, despite

the specific interoperability provisions of the LGPD under the responsibility of the ANPD, there is no overlap when it comes to regulation aimed exclusively at big techs, whose primary vector should not be privacy, but instead the promotion of free competition and the limitation of monopolies.

Some private sector associations, however, expressed further reservations on interoperability obligations and advocated a narrower implementation compared with the approaches above. ALAI, for instance, explained that interoperability obligations involve defining the data and service types included and the data required to render such services useful, and consequently, privacy and competition regulators should interact to share their experiences.

Câmara.e-net supported an interoperable digital environment but emphasized that the term 'interoperability' is broad and may have a wide range of meanings, making it challenging to apply and generating risks. Both associations (ALAI and Câmara.e-net) therefore suggested that the regulation should not:

> *i) Force a company to compromise its capacity to adopt measures that ensure [data] integrity and improve user experience and ii) prescribe how to build interoperability, which would pose the risk of applying outdated, unfair, uninformed, inflexible, and punitive standards. Instead, it should i) ensure flexibility in different contexts and situations to balance the interoperability costs with the political objectives of a given policy, establish clear liability rules for the parties involved, and iii) balance interoperability with privacy, security, and integrity.*

Therefore, there seems to be a consensus among participants' inputs on the benefits of applying interoperability to mitigate the risk of data processing concentration. However, different approaches regarding its scope and its mandatory nature were used. Most participants – at least those who took a more detailed approach – highlighted that achieving the effective exercise of the right to interoperability requires establishing minimum standards that ensure data standardization, openness, and structure to allow their transfer. The need for harmonization with the LGPD and ANPD's powers was also emphasized.

2.1.1.2 LIMITING OR PROHIBITING DATA SHARING AMONG COMPANIES BELONGING TO THE SAME CORPORATE GROUP

Measures to limit or prohibit sharing personal and non-personal data among companies of the same corporation were not consensual among the respondents.

Abranet, for instance, asserted that such measures are not required or reasonable, whether in the competitive arena or for the protection of personal data. Abranet, Câmara.e-net, and ALAI pointed out that the LGPD allows data sharing among processing agents, provided it does not deviate from the initial purpose of their collection (in compliance with the principle of purpose), comply with the established legal framework, and ensure data transparency to their owner. ALAI and Câmara.e-net argued that such limitations may also undermine fraud prevention efforts to detect potential fraud patterns by sharing and combining consumer data.

Regarding competition law, Abranet and IBRAC mentioned that there are already possible restrictions on sharing competitively sensitive information, even among companies of the same corporate group. IBRAC explains that Cade (Brazilian Administrative Council for Economic Defense) already has the power to limit and prohibit data sharing among companies of the same corporate group when analyzing concentration activities, and therefore, no new mechanisms need to be developed. Therefore, IBRAC argued that drafting *ex-ante* legislation on the subject must be preceded by assessing its objectives and which problems it seeks to address, indicating why the present mechanisms are insufficient.

Traditional media associations refute that perspective because data sharing among companies of the same corporation, despite seemingly being "a matter of free initiative or even of personal data privacy and protection, there is an evident antitrust issue involving Big Data in digital platform conglomerates." In this regard, the associations explain that data-sharing prohibition should target actors in monopolistic or dominant market positions stemming from concentration operations. The associations also mentioned that such a mechanism exists in other regulations, such as the EU DMA.

Third-sector organizations and scientific and technical community members supported the measure in line with media company associations. DiraCom and Alex Camacho asserted that mitigating the risks of disproportionate economic power concentration in different markets and creating closed ecosystems is essential. According to Idec, data sharing poses a risk of abuse of a dominant position, allowing market position leverage by data cross-use in a related market, increasing barriers to entry, and generating insurmountable advantages. Idec emphasized that this threat is even more severe in the context of large platforms with vertical operations (operating in complementary markets within the same consumer and supply chain) as a conglomerate and within ecosystems.

Idec illustrates such risks by referring to Google's acquisition of FitBit and WhatsApp's privacy policy change. In the first case, the consumer protection organization considers that by sharing data, Google may leverage its position in other markets, both for profiling in advertisements, such as the health product market; in the case of WhatsApp, data sharing may pose risks to consumers. Therefore, Idec argued that abuses and the unsatisfactory solutions adopted by the Brazilian authorities demonstrate the need for an economic regulation prohibiting data sharing among companies of the same corporate group without informed, prior, explicit, and specific consumer consent. Tarcízio Silva (Mozilla Foundation, IP.rec) and Rafael Evangelista (Unicamp) also support users' explicit and informed consent, adding that this authorization should not be used to the detriment of their ability to continue using the service.

Intervozes proposes segregating product databases of the same company or corporate group in data silos (isolating the information collected by company division, making it inaccessible to all levels of the company's hierarchy). Jonas Valente (UnB) questioned whether user data not directly obtained through platform use and navigation can be disputed within the scope of data protection, mainly when stricter interpretations of legitimate interest are applied.

2.1.1.3 OTHER MITIGATION MEASURES FOR DATA CONCENTRATION RISKS

Abranet suggested, in addition to interoperability exercised through the data owner rights, "imposing obligations of sharing data with competing market agents according to specific competitive remedies decided by the competent authority," aiming to enhance the contestability of digital platform markets for large personal data owners that hold a dominant position in their markets.

In the government sector, DEIN/Ministry of Development, Industry, and Foreign Trade suggested that physical data collection and storage infrastructures should be subject to inspection by a pertinent regulator, either periodically or upon demand by the designated competent authorities. In addition to prohibiting or demanding data sharing, DiraCom proposed establishing regulatory mechanisms to ensure or encourage access distribution through public infrastructure to collect, store, analyze, and process data, guaranteeing data protection and privacy. Jonas Valente (UnB) emphasized the oversight of non-personal data processing, as such data strengthens platform power, advocating that regulations adopt a collective data management perspective.

Likewise, Tarcízio Silva (Mozilla Foundation) argued that the State must be responsible for fostering public national infrastructure and limiting economic abuses. Silva considered that providing strategic services, such as digital communication, hosting, e-mails, cloud computing, work management suites, and similar services, by foreign digital solutions undermines national sovereignty and wastes State resources when invaluable national and strategic data are lost. He argues, therefore, that national actors should manage such strategic resources.

2.2 COMPETITION RISKS ASSOCIATED WITH THE NEGATIVE EFFECTS OF MARKET CONCENTRATION AND THE ABUSE OF ECONOMIC POWER BY PLATFORMS

Some participants considered that the risks associated with the adverse effects of market concentration and platforms' abuse of economic power are irrelevant to regulation. IBRAC and Abranet reiterate that market concentration is not a problem *per se* since concentrated markets can be competitive and

generate positive effects, such as efficiency or innovation, so much so that only competition legislation abuses of economic power are subjected to government intervention. Câmara.e-net agreed that "the current competition legislation is fully capable of remediating risks associated with market concentration and abuse of economic power."

According to IAB Brasil – which does not recognize such risks either –, the acquisition of emerging competitors and the high cost of barriers to entry – which are competition-related risks – are not observed in Brazil, referring to a Cade report that indicates a low number of concentration acts in digital markets. IAB Brasil considered that the high cost of barriers to entry is a minor issue in Brazil but more significant in the USA and the EU, where large digital companies are based. Therefore, depending on the regulation proposed, the barrier to entry may increase, hindering the presence of new Brazilian players. This concern was also raised by Abranet, who argued, however, that such risks could be remedied by adequate asymmetric regulation.

On the other hand, Flávia Lefèvre, from the third sector, considered that the lack of cases analyzing digital platforms indicates the need to update the legislation, considering the platforms' market power and the challenges emerging from the development of AI and the Internet of Things (IoT). Idec expressed a similar opinion, reminding that, to date, the Brazilian competition authority has not prioritized digital markets, whereas other authorities worldwide have recognized their relevance. Media company associations mention some examples of economic players excluded from their original markets or that were or are still exploited by monopolistic digital platforms. Instituto Alana also highlighted the concentration of the digital platform market:

> *[...] large private corporations greatly influence the design and success of digital products and services. Seven big techs (Microsoft, Apple, Amazon, Google, Facebook, Tencent, and Alibaba) account for two-thirds of the total market value of the 70 largest digital companies, predominantly concentrated in the Silicon Valley, USA, while Europe's share is 3.6%, Africa's 1.3%, and Latin America's 0.2%. Google holds 90% of the global Internet market, and Facebook is the leading social media platform in over 90% of the world's economies.*

As Idec and the media business associations represented by ABERT explained, **some platform characteristics contribute to and tend to generate market concentration**, leading to the consolidated and entrenched formation of monopolies and, consequently, power abuse. Economies of scope and scale, network externalities, and the comparative advantages of agents holding large amounts of data are the main factors causing market concentration and abuse. In this regard, Idec pointed out two relevant effects of this context: the "winner takes all" dynamics and the lock-in effect.

According to traditional media company associations, referring to a report of the Australian Competition and Consumer Authority, the market power positions of large platforms encourage them to engage in **anti-competitive strategies to expand and strengthen their monopoly power** through self-preferencing practices, such as "tying, exclusivity agreements, denial of interoperability, and limiting access to hardware/software/data." According to Idec, the abuse of economic power is exercised through the:

> *i) **abuse of a dominant position** through exclusionary conducts (excluding current and potential competitors), ii) **exploitative conduct** (without necessarily excluding competitors, but harming competition and consumers), and iii) **acquisition of current and potential competitors** [our emphasis].*

Abranet emphasized the unilateral exclusionary conduct, deemed by the association as one of the main issues within the scope of this risk, which is facilitated by some platforms' high market share and includes self-preferencing, predatory pricing, tying, and refusal to deal. According to Abranet, self-preferencing – which gained prominence with the European Commission's investigation into the "Google Shopping" case – may harm competition by excluding competitors, reducing incentives for innovation, increasing prices, and reducing product quality and variety. Abranet stated that most competition problems emerge when **a platform controls specific markets and, simultaneously, is a competitor of other agents operating in the same markets**, thereby abusing their power in their primary markets and extending it to adjacent markets.

Regarding competitor acquisition, Filipe Saraiva (UFPA) mentioned relevant concentration movements, such as the acquisition of Instagram and WhatsApp by Meta. According to Saraiva, "Meta's moves to clone features from other apps, such as implementing Stories on Instagram, virtually eliminating Snapchat, which first introduced this feature," can be considered "exploitative conduct."

Jonas Valente (UnB) stated that another element used to exercise anti-competitive practices is precisely the risk discussed above, i.e., **data processing concentration**, particularly at access control points and when platforms are gatekeepers.

According to Idec, such platform characteristics and strategies "harm 1) competition, 2) consumers, 3) innovation, and 4) the protection of other rights, including fundamental rights", as mentioned by other participants. Therefore, Idec considers that the abuse of economic power should be central to competition law and economic regulations.[37]

As the EU model, the ITS (Technology and Society Institute) considered that digital platform regulation should consider market concentration and abuse of dominant position risks in different digital markets. It recalled that Decree 8,771 (BRASIL, 2016), which regulates the MCI (BRASIL, 2014), emphasizes, within the scope of Internet regulation inspection and transparency assignments, the role of the Brazilian Competition Defense System (SBDC) in the "investigation of violations of the economic order," also highlighted by Flávia Lefèvre.

Tarcízio Silva (Mozilla Foundation) stressed that the oligopolistic tendency of digital platforms' business models allows them to: "i) establish a myriad of points of contact with customers, employees, and suppliers that are used to offer new services, applications, or terms; ii) use capital to generate dumping in certain areas or activities until their establishment in the market; and iii) enjoy disproportionate advantages due to zero-rating practices, which violates network neutrality." Several

[37] According to Idec's contribution, it is possible to recognize "that competition law will not resolve all cases because, i) despite having tools to curb the abuse of economic power, it still needs improvements for effective enforcement in digital markets, ii) some topics are more likely to be analyzed by other authorities, such as consumer law and data protection."

participants mentioned zero-rating as a frequent practice to build platform power and economic concentration.

Flávia Lefèvre, for instance, considered that the free-access plans, associated with zero-rating, strengthen Meta's market power and harm competition, as they allow collecting and processing data on a large scale, unparalleled to that of other economic agents – in addition to deleterious effects on democracy by encouraging disinformation. Lefèvre recalls that zero-rating, although condemned internationally, has not yet been addressed by Brazilian authorities. Therefore, there is a strong association between platform power formation and Internet access limitation. Andressa Siqueira[38], from the scientific and technical community, and IP.rec and Intervozes, from the third sector, also stated that zero-pricing is an anti-competitive practice. Associating economic risks with Human Rights risks, Artigo 19 emphasized that excessive market power concentration and abuse of economic power change market dynamics so that "the supply of services that have become essential for society was divided among a few actors in digital environments, with direct impacts on the exercise of Human Rights, such as freedom of expression and access to information." Likewise, Black Women Bloggers stressed that "market concentration engender abuse of economic, business, and ideological power." Telefônica Brasil S.A. makes a similar correlation, highlighting that:

> *[...] the high market power of those companies provides them with a high capacity to manipulate users and develop solutions to maintain user engagement and the longest possible screen time to generate value and high business profits.*

Intervozes compared the broadcasting market concentration with that of digital platforms. It recalls that at the time broadcasting concentration was discussed, cross-ownership, i.e., the ownership of more than one media outlet by a single business group, was considered detrimental to Democracy, and several countries

[38] According to Andressa Siqueira's contribution, "although Cade has already expressed its opinion, in 2017, on the practice of zero-rating in light of competition law, in a decision to archive the aforementioned investigation, it is noted that there is still room for review of the understanding from perspectives that have not yet been analyzed."

established thresholds for market and audience shares and territorial coverage. In this sense, digital platforms establish a kind of cross-ownership concentration, which, "in practice, means the need to develop rules to prevent the same conglomerate from simultaneously operating messaging services, social media, search engines, e-mail, etc., which, therefore, should be offered by different companies."

According to Instituto Alana, market concentration and the presence of private monopolies, which benefit from their dominant position, generate dependence on the use of dominant platforms to interact, communicate, socialize, and exercise the rights to culture, information, and leisure, having direct impacts on children's rights. According to that organization,

> *[...] the access to those global interaction spaces is often tied to a business model that benefits from targeted advertising and the collection, extraction, and analysis of personal data for business purposes, increasing the vulnerability of children and adolescents and creating the false perception of 'freedom of use' due to the low prominence of alternative platforms.*

Based on the issues identified above, a series of regulatory measures are suggested in the following items, ranging from the update of antitrust legislation to address the challenges posed by large platforms to new economic law regulations.

2.2.1 MEASURES TO MITIGATE ECONOMIC AND MARKET POWER CONCENTRATION

As previously noted, some associations, such as Câmara-e.net, argued that the concerns expressed in the consultation are covered by the current competition legislation. However, some participants proposed other measures to mitigate these risks, ranging from competition law changes to economic regulation instruments.

Next, mitigation measures other than those initially mapped by the consultation were suggested, including broader approaches both to antitrust and economic regulations, including those addressing economic risks in other sectors, and media regulation, which should seek to promote alternative, regional, and popular media, as pointed out by Tarcízio Silva (Mozilla Foundation).

2.2.1.1 SBDC (BRAZILIAN SYSTEM OF COMPETITION DEFENSE) OBJECTIVES

The Competition Defense Law (BRASIL, 2011b) and the SBDC are governed by the constitutional dictates of freedom of initiative, free competition, the social function of property, consumer protection, and repression of abuse of economic power. A set of inputs (six participants) proposed the expansion of the SBDC to encompass other objectives, such as personal data protection or, more broadly, the protection of other fundamental rights.

ALAI stressed that the current competition legislation can fully remedy market concentration and abuse of economic power risks. According to ALAI, "the enforcement of the competition laws should not incorporate tangential issues, including privacy protection, which should be addressed by a specific and comprehensive data protection legislation." It added that substantial risks to the resilience of the competition legislation may arise if the authorities consider factors beyond the scope of the competition law when analyzing competitive harm.

Câmara.e-net supported that perspective, arguing that neither the competition legislation nor platform regulations should "attempt to remedy issues of other public policy areas, such as privacy, data security, taxation, critical infrastructure, labor rights, electoral processes, threats to Democracy and Human Rights, journalism, and protection of minors, etc.," as these require specific regulatory structures.

On the other hand, IBRAC asserted that "factors, such as the protection of privacy (and of other elements) should be **understood as quality elements** already addressed by the analysis model of competitive effect assessment, focused on maintaining consumer well-being" [*our emphasis*]. As IBRAC explained, competition works as an instrument that ensures consumer well-being by reducing prices, encouraging innovation, and providing more alternatives and higher-quality products and services. Therefore, the tools available to the antitrust authority can be broadly used when such interests are relevant.

Idec also stressed that the consumer well-being parameter allows for incorporating other interests into the competition law. Although the competition law has tools that allow the effective enforcement of rules in digital markets, it is guided by the dictates of the Chicago School, i.e., by price and economic efficiency criteria. In this sense, Idec emphasized the need to

update the antitrust toolkit considering other factors identified in its analyses, such as processing personal data in an exclusionary or exploratory manner and taking into account "i) privacy and data protection as **elements of product or service quality**," or (ii) "irregularities in personal data processing as evidence of the **abusive exercise of a dominant position**" [*our emphasis*] as applied by the German competition authority.

2.2.1.2 UPDATE OF CRITERIA FOR ANALYZING CONCENTRATION ACTS

Per Brazilian legislation, concentration acts are defined as mergers of two or more companies, control or partial acquisitions of other companies, incorporation of one or more companies by one or more companies, and associative, consortium, or **joint venture** agreements between two or more companies. New forms of expressing value in the digital economy, primarily data, and strategies of abuse of economic power through competitor exclusionary practices, such as **killer acquisitions**, have generated discussions on the need to change the criteria for notifying acts of concentration to the competition authority. Currently, Cade needs to be notified of concentration acts when at least one of the groups involved has registered annual gross revenue or turnover in Brazil equal to or higher than BRL 750 million and at least another group involved in the operation has registered an annual gross revenue or total turnover equal to or higher than BRL 75 million.

ALAI stated that the global revenue and number of users criteria do not determine market concentration or dominant position and, therefore, should not be considered notification criteria as they are arbitrary, and if applied, private agents could stall their innovation investments to avoid regulatory scrutiny. Therefore, ALAI argued that the assessment of a dominant position should "focus on the analysis of market power, indicated by [the company's] capacity to control competitive outcomes and dictate prices," considering its corresponding product or service market and the competition dynamics of that market.

According to IBRAC, the review of notification criteria can be discussed by: i) simply reviewing the current criteria applied in the assessment of concentration acts, reducing the aforementioned legal thresholds (BRL 750 million and BRL 75 million) to capture new mergers and acquisitions; or ii) "developing asymmetric

regulatory instruments, by which economic agents become objects of regulation based on criteria such as revenue and the number of users," as provided by the DMA in the scope of the European competition regulatory system.

IBRAC stressed that reducing the legal thresholds for Cade notification is essential, given the relevance of acquisitions of new entrants and technologies in the context of digital platforms. It should be noted, however, that Cade can analyze cases beyond its mandatory submission criteria and may, at its discretion, evaluate transactions it understands may potentially raise competition concerns by invocation, per Art. 88, §7º of Law 12,529 (BRASIL, 2011b), functioning as a safety valve.

However, according to media business associations, that legal provision establishes:

> *[...] a limited timeframe of only one year after the transaction is effected for exercising such power. However, this period may not be sufficient to allow the authority to identify issues arising from a transaction and request its analysis.*

Nevertheless, there are precedents. Due to successive concentration acts committed by dominant agents, Cade temporarily prohibited new acquisitions or operations in specific industries and markets or required specific agents to notify their operations prior to their conclusion despite not being legally binding. For this reason, media associations stated that such measures may be considered for Big Techs.

Idec made similar suggestions, arguing that this safety valve is more valuable to "require the notification of concentration acts that do not meet the current revenue criteria but that raise concerns, including data concentration leading to possible abuse of economic power." It recalled that this mechanism has seldom been used since the law came into force; moreover, it requests Cade to be less lenient with potentially harmful concentrations in general.

Regarding **assessing large platforms applying asymmetric regulatory instruments**, IBRAC again stressed that the Brazilian antitrust toolkit already partially fulfills the functions sought by other regulations, such as the EU DMA, and that economic concentration elements should not be understood as indicators to presume anti-competitive conduct.

Idec, on the other hand, argued the mandatory notification of gatekeeper operations, i.e., "when the entities participating in the merger or the concentration target provide core platform services and any other digital services or allow data collection," as in the EU regulation. In addition to the current criteria, Idec proposed including new alternative criteria for the notification of concentration acts by "updating the gross revenue criterion in Brazil, and providing alternatives," as this criterion, besides being quantitatively outdated, is insufficient because it does not cover relevant digital market operations. Idec, therefore, supported updating the legislation to include criteria other than revenue:

> *Other legislations apply: i) total revenue, ii) shared revenue of the parties, iii) number of users (for digital markets), and iv) resulting market concentration, among others. It should be noted that* ***those criteria are not exclusive or additional to the revenue criterion****; however,* ***an alternative criterion*** *covering operations whose complexity cannot be measured by the current terms and, for this reason, overlook meaningful operations,* ***is needed*** *[our emphasis].*

Likewise, DiraCom referred to "Guia para Análise de Atos de Concentração Horizontal" (Guide for the Analysis of Horizontal Concentration Acts) (OLIVEIRA JÚNIOR et al., 2016), which establishes that "when the concentration increases the CR4 index (the market share ratio of the 4 largest companies in an industry) to 75% or higher, the possibility that the operation may allow or not the abusive exercise of coordinated power should be further analyzed" (p. 43).

Lastly, mentioning the acquisition of Fitbit by Google, Idec argued that, although such a situation does not occur within the same corporate group, a relevant provision should be adopted prohibiting the use of sensitive personal data for profiling and advertising targeting purposes, as well as the use of children's and adolescents' personal data for personalization and advertising targeting.

2.2.1.3 PROHIBITING SELF-PREFERENCING PRACTICES

Another topic addressed in the inputs, which has become a focal point of digital platform regulations, is self-preferencing, i.e., when a platform favors itself (or its business partners).

As explained by IBRAC, vertical integration is a frequent business practice in which a company operates in different steps of its value chain, allowing it to internalize outsourced activities, offer products and services internally, reduce production and transaction costs, in addition to increasing the options available to the consumer and fostering innovation. It cautioned, however, that, in some instances, "verticalization may generate anti-competitive effects, such as increased costs for rivals, discrimination, and market foreclosure." In other words, IBRAC asserted that it cannot be assumed that self-preferencing, in general, is detrimental to consumers' well-being and must assessed on a case-by-case basis, as verticalization can result in significant efficiencies.[39] Therefore, Cade should "establish guidelines for analyzing anti-competitive practices and preventing possible abuses" per the parameters established in Law 12,529 (BRASIL, 2011b). IBRAC recalls that Cade specified a series of factors to be considered for the analysis of this practice.[40]

Likewise, Câmara-e.net and ALAI argued that, in addition to preventing private agents from promoting their products, a

> *[...] A blanket ban on "self-preferencing" will lead to the scrutiny of highly pro-competitive and consumer-benefiting activities, including marketing, promotion, and advertising that give consumers visibility to innovative products and services.*

Those business associations stated that the measure would discourage private agents with economies of scale from offering such services to other market agents. They added that the current prohibitions on exclusionary conduct apply to self-preferencing risks, such as restricting access to essential facilities to exclude competitors.

---

[39] According to IBRAC's contribution, "Cade itself has already recognized possible positive effects of self-preference, such as i) an increase in total sales in the market; ii) recovery of investments made; and iii) a reduction in the possibility of collusion (by making it difficult to monitor the market and detect deviations from a possible agreement)"

[40] According to IBRAC, these factors indicated by Cade are: "i) the existence of market power on the part of the vertically integrated company; ii) the characteristics of the markets involved (for example, rivalry; barriers to entry; existence of substitutes and alternatives to customers; bargaining power of customers; switching costs); iii) the incentives to promote market closure; and iv) the negative competitive effects in the specific case".

However, other private sector actors, such as Abranet and media company associations, in addition to Telefônica Brasil S.A., and third-sector organizations, such as Idec, DiraCom, and Instituto Vero, supported some form of restriction. According to Abranet, platforms consolidate their market power in their primary and adjacent markets by vertically controlling integrated ecosystems, often favoring their products and services to the detriment of the competitors. This conduct may close the market to new entrants or reduce competitiveness.

As explained by traditional media associations, although self-preferencing is a common practice in verticalized markets, it takes on specific configurations in the digital context. According to those associations, it introduces "a new form of abuse of dominant position specific to digital markets – generally referred to as self-preferencing, abusive leverage, or differential treatment" by adopting strategies to leverage their dominant position from one market to another. Such practices may be subtle, "such as manipulating digital advertising auctions, as in the case of Google ad tech tools, or biased algorithmic programming, as in the case of Google Shopping," making their analysis and investigation difficult.

To address such challenges and mitigate the risks, traditional media associations refer to Art. 6 of the EU DMA (EU, 2022), which expressly prohibits the practice of self-preferencing by gatekeepers in an ***ex-ante*** regulation. Moreover, the German Competition Act states, "the practice is presumed to be unlawful when adopted by agents with cross-industry power (e.g., in more than one related market)." In this sense, Idec mentions that competition authorities of other countries, such as Japan, Korea, and Australia, are considering regulations on that matter, as well as the American Innovation and Choice Online Act (AICO) (UNITED STATES, 2022), Bill under draft in the USA.

The traditional media associations argued that the ***ex-ante*** nature of such prohibition is relevant, as traditional antitrust analyses admitted that legal exceptions to the law are based on efficiency generation arguments. According to those associations:

> *[...] the long path treaded by antitrust investigations based on the rule of reason (relevant market definition, investigation of dominant position in the affected market, efficiency analysis)* ***did not provide timely and satisfactory responses to the self-preferencing conduct of digital platforms****, which*

> ***was, therefore, prohibited*** *ex-ante* ***for digital platforms categorized as gatekeepers*** *[our emphasis].*

For instance, the case of Google Shopping analyzed in Brazil was investigated and dismissed due to lack of evidence; however, as Idec highlighted, in the European context, this was precisely what influenced the DMA. Idec considers that digital platforms abuse their economic power by advancing their power in an adjacent market to the detriment of competitors and commercial partners. Furthermore, self-preferencing may also indicate an "abusive practice under the Consumer Protection Code if there is manipulation of the free will and legitimate expectations of consumers by taking advantage of their lack of knowledge on the practice." Instituto Vero also highlighted the risks of influencing consumers.

Therefore, according to Abranet:

> *[...] the enforcement aimed at non-discrimination/fair treatment on digital platforms is essential since the design of many internal markets negatively impacts competition among companies that need to use the platform ecosystem of a dominant player.*

In this regard, prohibiting self-preferencing, as provided by the DMA, may mitigate the risks of platform monopoly and verticalization.

Therefore, participants dissented on that matter. On the one hand, some private sector inputs supported maintaining the current antitrust rules, which would deal with possible abuses of verticalization by applying traditional tools ***ex-post*** on a case-by-case basis. On the other hand, based on previous cases, other private sector participants and the third sector considered such analyses insufficient and recommended asymmetrically applying self-preferencing rules only to platforms categorized as gatekeepers.

2.2.1.4 RESTRAINTS ON VERTICALIZATION OR BUNDLING OPERATIONS

In addition to the debate on the effects of verticalization, the inputs also addressed possible restrictions on verticalization or bundling, especially in platforms that act as gatekeepers.

According to Idec, bundling or verticalization operations – for instance, providing more than one complementary service/ product, such as being an advertising and social media platform, owning a restaurant and being a delivery platform for third parties, or having a marketplace and selling its products – deserve special attention in the economic regulation of digital platforms. The institute highlights that data-centric acquisitions go beyond vertical and horizontal acquisitions, which guide classic antitrust analyses since digital platforms' bundling operations are **transversal** or **scattered**. It recommends, in addition to the aforementioned measures, "in some cases, to demand unbundling," i.e., the structural segregation of businesses.

According to traditional media associations, several competition authorities started to consider adopting more drastic measures, such as the compulsory division of giants, with the prohibition of integrated and vertical operations in related or adjacent markets and possible obligation to exit specific markets, as in the well-known cases of Standard Oil and AT&T. Furthermore, there are sectoral regulations in place in Brazil that limit or prohibit verticalization in determined markets[41]. The associations also mention international experiences that show possibilities of limiting *ex-post* verticalization, such as requesting the separation of Google's Ads digital advertising division as a remedy to reverse its current dominant position.

Third-sector organizations also supported ownership restrictions. Idec and Intervozes mentioned Artigo 19's proposal to separate platforms into two distinct services: content server and content curator. This separation would allow, for example, to dissociate advertising from the hosting service, potentially increasing users' decision-making power. DiraCom stated, "Market share must be both horizontally and vertically limited to prevent the formation of monopolies and oligopolies, whether at the infrastructure or application layers."

[41] The associations also cite as an example the Conditional Access Service Law (SeAC) (BRASIL, 2011a), which regulates the pay TV market: "it prevents telecommunications or conditional access service operators from having control or equity interest exceeding 30% in audiovisual content producers or programmers". Another example cited is ANP Ordinance N. 41: "it prevents fuel distributors from being partners in fuel reseller stations" (BRASIL, 2013b).

On the other hand, Câmara-e.net and ALAI reiterated that current competition legislation and international best practices provide regulatory agencies with the power to remedy competition problems arising from vertical integration. They considered that arbitrary restraints, stipulating which agents can offer specific services and how they are offered, would allow "the public administration to choose the winners and the losers," limiting economic freedom.

2.2.2. CONCENTRATION IN THE ADVERTISING MARKET

Although digital platforms apply different business models, as IBRAC explained, ad funding is the most common system companies use to ensure financial viability. Therefore, that market is dominated by large platforms, as pointed out in several inputs, attracting regulatory and competitive attention in many countries. As ad funding involves risks associated with market concentration and abuse of economic power in a particular market (advertising), this report decided to systematize it into a specific topic.

According to ALAI and Câmara.e-net, "the current competition legislation and the application of international best practices create an optimal balance between preventing private anti-competitive practices and encouraging the evolution of economic sectors." IAB Brasil agreed that the risk is not relevant, as "online advertising is one of the largest and most complex ecosystems, with thousands of companies participating in the value chain between the advertisers and the media."[42] Furthermore, it added that advertising on large digital platforms does not exclude it from traditional media, smaller digital platforms, blogs, etc. However, other participants argued that the concentration of advertising on large platforms widely affects traditional media and journalism (as per Axis 2, item 5.1.2.3, on risks to journalism).

IAB Brasil mentioned that personalized advertising potentially benefits i) consumers by aiding consumers to choose and identify their interests, saving time and transaction costs, among other

[42] The association states that the diagram produced by Luma Partners helps to understand the different categories of companies that play a variety of roles in the sector (LUMA PARTNERS, n.d.).

benefits; ii) advertisers by providing easy reach and connection with consumers, even in the case of smaller brands; and iii) society by stimulating economic growth, boosting competition by expanding consumer's reach, enabling new business models, and other benefits ranging from journalism to public campaigns.

Although Idec recognized that transaction costs may be reduced by integrating advertising with other services, it maintained that platform regulation needs to decentralize advertising offers because platforms are at the center of all ad sales and purchase stages.

Abranet stated that the most significant risk of concentrated advertising markets is "the distortion of the ranking of the search results displayed to platform users, as the criteria that guided this ranking are not transparent, as illustrated in the European Commission investigation on Google Shopping," which Google was fined for that conduct (item 2.2 of Axis 2). Abranet mentioned the case of Google AdWords tool operations in Brazil, specifically the purchase of keywords associated with a competitor's trademark. The Superior Court of Justice (STJ) deemed the advertising company guilty of unfair competition for using another company's trademark as a keyword for sponsored search purposes.

According to Abranet, there is a considerable risk that this distortion of organic search results – amplified by the concentration of advertising offers – generates undesirable impacts on the market and society. DiraCom also stressed the risk posed by concentration when all market agents are subjected to advertising mechanisms unilaterally established by a few companies that generally operate in an opaque manner with non-auditable results.

Intervozes mentioned the emblematic trajectory of Google (which used its search system and the data obtained to create its advertising service, AdWords) to emphasize the need for regulation. The organization considers it detrimental to society to allow the same company that provides the search service – which should be considered a public interest service today – to offer advertising services, ranking search results according to the advertising company investments, i.e., combining ads with search.

According to Idec, Google's influence in the advertising market is so significant that the European Commission believes the most

effective solution is to separate part of the company's services. In this context, traditional media company associations referred to the diagnosis published in the report on digital advertising and platforms by the UK Competition and Markets Authority (CMA) (GOV.UK, n.d.), pointing out that, although Google and Meta have grown by offering better products than their competitors, they are protected by broad advantages, hindering fair competition.

Artigo 19 highlights the risks involved in the availability of a **unified business model for content curation and promotion based on targeted behavioral advertising** driven by user profiling. As the model is focused on engagement, users are exposed to content that stimulates impulsive interactions, exposing them to false and extreme content and those that violate human rights, in addition to infringing informational self-determination. Therefore, the proposed mitigation measures, which involve the structural separation of giants such as Google, are rooted both in economic risks and risks to human rights and democracy.

Lastly, traditional media associations and DiraCom mentioned that low competition in search engines and social media undermines innovation and freedom of choice, forcing consumers to provide more personal data than they wish to.

2.2.2.1 MITIGATION MEASURES FOR ADVERTISING MARKET CONCENTRATION

Artigo 19 asserted that digital platform regulation should prohibit integrated business models of content curation, promotion, and targeted advertising. It suggested separating hosting from content curation in large digital platforms, which, together with interoperability requirements, would allow users to choose the content displayed in their feeds. Intervozes criticized the integrated model, which combines ads with search and supported the economic-structural separation of the companies that offer such products/services, or, at least, the segregation of user databases (data silos) when the same company offers different services.

Traditional media associations represented by ABERT alluded to the ongoing investigations in the US and EU underway into the abuse of Google's dominant position in the digital advertising market, and many have required the **compulsory transfer of ownership of its digital advertising division**. In summary, according to traditional media associations, Google is accused of:

1. ***Neutralizing or eliminating current and potential competitors*** *in the ad tech tools market through acquisitions (such as AdWords, DoubleClick for Publishers, DoubleClick Advertising Exchange – AdX, AdMeld, AdMob).*
2. ***Abusing its dominant position*** *in the ad tech market to constrain more publishers and advertisers to use its products while harming the capacity of these agents to use competing products. That abuse involves several* ***interoperability/multihoming restrictions, manipulation of digital advertising auctions*** *to the detriment of competitors, and several* ***self-preferencing practices****, such as "last-look."*
3. *The collusion with Facebook (a deal known as Jedi Blue), in which Google allegedly offered favorable terms to Facebook in exchange for Facebook's word that it would not contract competing ad tech tools (such as Header Bidding) or act as a direct competitor to Google's ad tech tools [our emphasis].*

According to those traditional media associations, as a result of the UK investigations, a new division to evaluate digital platforms was created, called DMU, "to carry out interventions to oppose Google's and Facebook's market power," applying measures related to open data, separation of the vertically-integrated digital advertising complex, interoperability, and personalized advertising options.

IBRAC mentioned that detecting signs of economic concentration in a given industry requires precisely defining which markets are relevant, which is a complex task in digital markets. Therefore, according to Idec, the definition may need to consider "platforms in segments that are not necessarily correlated may **compete for the user's attention and time**, influencing the definition of relevant market" [***our emphasis***]. Moreover, it is necessary to evaluate in depth whether there is rivalry in the attention market overall, which may expand, in some cases, the competitive space and potential competition between technology companies and the advertising sector.

Lastly, DiraCom proposed limiting the share of agents in each specific segment and overall, in the advertising "pie," in addition to establishing advertisement transparency measures and

restricting the use of sensitive personal data. From the scientific and technical community, Alex Camacho proposed encouraging the diversification of advertising models, such as native ads, contextual advertising, and models based on explicit consent.

2.2.2.2 COMBATING THE ABUSE OF DOMINANT POSITION IN NEGOTIATIONS WITH DEVELOPERS

Only four participants submitted inputs on mitigation measures for the abuse of the dominant position. ALAI and Câmara.e-net reiterated that current competition legislation and international best practices can remedy the risks of market concentration and abuse of economic power.

Associations of traditional media companies mentioned that several authorities have investigated anti-competitive arrangements among operating systems, app stores, and payment methods. In Brazil, for instance, Cade initiated an administrative inquiry to i) evaluate Apple's anti-competitive conduct in the app distribution market by "preventing the distribution of third-party applications and restricting the use of other payment systems in its app store and in-app purchases"; ii) investigate Google's agreements with mobile device manufacturers and mobile network operators to leverage Google Android's dominant position. Investigations abroad were also cited. Lastly, they referred to the example of the *ex-ante* regulation in South Korea, "which enacted a law that requires Apple and Google to open up their app stores to alternative payment systems."

Other than those associations, only DiraCom, from the third sector, contributed to this topic, agreeing with the need for mitigation measures.

2.2.2.3 OTHER MITIGATION MEASURES TO ADDRESS MARKET CONCENTRATION AND ABUSE OF ECONOMIC POWER

Also within the scope of competition law, Idec suggested "fostering greater social participation of third-party stakeholders who do not operate only in the affected market" and "creating a General Coordination of Antitrust Analysis (CGAA) specialized in the technology sector" – in addition to requesting Cade be attentive to competition issues in digital markets and further cooperate with authorities with powers in complementary

matters. The institute also calls for greater cooperation among foreign authorities and attention to the worst performance of companies in the Global South.

Abranet suggested other mitigation measures for these risks, such as: "i) structural separation of activities; ii) elimination of *de facto* or *de jure* of the exclusivity clauses in effect; and iii) the guarantee of non-discriminatory access to critical infrastructures by competitors, at least as regards self-preferencing."

Given the asymmetry among agents, media company associations suggested as a risk mitigation measure, the adoption of an explicit provision for mandatory negotiation, for instance, between large platforms and

> *[...] journalism websites or content producers relative the remuneration for using their content during a specific and limited period, with the introduction of alternative dispute resolution mechanisms, such as mediation or arbitration, to resolve deadlock or intransigence in negotiations.*

Intervozes observed that digital platforms have become the public sphere proper, mediated by technological devices. Therefore, in addition to confronting the consolidation of digital monopolies, platforms need to be identified as private entities that provide a public service in order to develop regulations consistent with the principles and obligations for the provision of these services, establishing more stringent rules on player diversity, user reach thresholds, and audience.

In this context, Tarcízio Silva (Mozilla Foundation) stressed the need to contemplate media regulation, in addition to antitrust and economic regulation, when developing digital platform regulation. According to Silva, it is necessary to consider how market concentration "hampers the evolution of the Brazilian media ecosystem, including the necessary diversification of themes and populations not only in terms of representation but also of ownership and management." He added that digital platforms entered the media and advertising market under unfair conditions without considering their content's quality or its strategic nature for the country's sovereignty. Therefore, Silva argued that mitigation measures targeting market concentration and abuse of economic power should seek to promote alternative, regional, and popular media initiatives.

2.3 RISKS ASSOCIATED WITH INHIBITING ALTERNATIVE DIGITAL PLATFORM ECONOMIC MODELS WITH NEGATIVE IMPACTS ON INNOVATION

The participants considered that issues related to the decline of innovation and product and service quality are consequences of the risks previously discussed, i.e., data concentration, market concentration, and abuse of economic power. Furthermore, many of the inputs addressed those risks jointly, stating that an environment that hampers innovation – and favors the business model of large platforms based on the massive exploitation of data and network effects – hinders the emergence of better quality services and products and that respect Human Rights, such as personal data protection. For those reasons and summary purposes, those two risks are addressed together.

IAB Brasil mentioned that digital services often create alternative business models that promote innovation, such as micropayments, crowdfunding, freemium, digital product licensing and sales, commissions, and partnerships, and added that any regulation may affect the operations and the existence of such models. Likewise, Câmara.e-net pointed out that innovative services attract a significant number of users, and the growth of other services shows that the presence of consolidated agents in the market does not prevent the growth of alternative services that provide innovative solutions for users.

Most inputs on this issue, however, asserted that alternative model inhibition poses a significant risk to the digital platform economy, and it is strongly related to economic and data concentration and the abuse of economic power by large platforms. Abranet explained that such risks are related to the effects arising from the abuse of a dominant position, such as exclusionary practices involving preventing market entry, increased costs for rivals, and barriers to entry, resulting in the exclusion of current or potential competitors. Idec and Jonas Valente (UnB) also highlighted the effects of exclusionary and exploitative practices by large conglomerates, such as Meta, Alphabet, and Microsoft, on innovation.

Idec, Artigo 19, and media company associations pointed out a strategy of abuse of economic power that is particularly harmful to innovation: the systematic acquisition of current, emerging, and future competitors, known as **killer acquisitions**. According to the

media associations represented by ABERT, the anti-competitive strategies to 'buy or bury' any competitor applied by digital platforms, combining predatory strategies, systematic acquisitions, and even mimicking competitors' innovations, are evident.

Artigo 19 also noted that the characteristics and strategies of abuse of economic power carried out by digital platforms favor the lock-in effect, the formation of business conglomerates, and the domination of entire markets (not just part of them), inhibiting the emergence of new competitors with different business models.

Traditional media associations considered particularly harmful the practice of scraping to take advantage of content produced by third parties, especially news websites, diverting the traffic from content or news producers' websites to Google by increasingly concentrating ad funds, which increases content producers' remuneration dependence on Google or other less efficient methods, such as subscriptions and paywalls. While IAB Brasil considers [that model] a positive innovation, media associations see it as a sign of market deterioration, arguing that:

> *[...] Cade Counselor Victor de Oliveira Fernandes, in his book "Direito da Concorrência das Plataformas Digitais" (Competition Law on Digital Platforms), warns that* ***dominant digital platforms tend to appropriate third-party contents, prevent the use of multiple platforms, and, finally, promote anti-competitive innovation and self-preferencing****. Such exclusionary conduct may cause damages, including i)* ***limiting contestability and appropriability conditions****, ii)* ***creating obstacles to the development of disruptive innovations****, and iii)* ***hindering competitors' access to strategic resources for dynamic competition*** *[our emphasis].*

Several concerns were expressed regarding concentrated and closed platform markets, in addition to those commonly addressed in antitrust regulations. Many participants, such as the researchers Leonardo Cruz (UFPA) and Tarcízio Silva (Mozilla Foundation), Intervozes, and DiraCom, pointed out the negative impacts of the lack of competition and abuse of economic power on the emergence of more diverse digital services that include a broader representation of views, and more consistent with the national interests, in addition to alternative business models. Leonardo Cruz, for example, stated that:

> *Today, the data economy is the hegemonic model used to appraise digital services and content production. The centralization of that market and its key companies' capital and investment power* ***prevent information technology development from being valued by business models other than data collection and processing****. It has a negative impact not only on the market but also on the production and circulation of information on the Internet [our emphasis].*

Cruz also considered that market concentration by foreign companies hinders the emergence and growth of **national technological developments,** which may generate income and jobs within the country. The Mozilla Foundation expressed similar concerns.[43] This situation negatively reinforces similar practices in the media ecosystem that can only be overcome by regulating and promoting an alternative platform economy and innovation models and applying sovereignty metrics, such as cultural heritage circulation, job generation, universal access, and others. Intervozes also stressed the "low diversity of voices and perspectives" in this closed ecosystem.

Idec emphasized that the context prevents using Internet models not based on exploiting personal data, which are essential in public services or services with high social and political interest. Likewise, DiraCom points out that the business model developed by large platforms limits the initiatives of other agents, particularly not-for-profit and smaller private agents, submitting them to the private exploitation of services with a higher potential to infringe privacy and data protection. Moreover, Slowphone, a third-sector organization, mentioned the risk of inhibiting sustainable business models. Lastly, the Internet Governance Research Network (REDE) recalled that diversity and innovation, which are put at risk due to the expansion of the infrastructure of some platforms, are Internet principles in Brazil.

[43] According to the contribution, "The close relationship between the business of global digital platforms and financial capital and the economic and political objectives of their home states allows them to develop and implement products, services and resources that cannot compete. The globalization approach has favored companies in hubs, such as Silicon Valley, limiting local innovation."

2.3.1 RISKS TO PRODUCT AND SERVICE QUALITY

According to Abranet, large companies that collect and process more data are able to improve their products at lower costs than smaller companies, enabling their entry into adjacent markets and the development of new products at lower costs, which discourages economic incentives to promote innovation and may negatively impact digital product and service quality.

Tarcízio Silva (Mozilla Foundation) mentioned that another platform characteristic that may impair the product and service quality is the network effect, as user, customer, and supplier communities have become dependent on platforms to access other people and financial resources. Consequently, changing platforms requires additional efforts to recreate their networks, content, or practices. According to Silva, that privileged position allows large platforms "to gradually reduce the quality of their services, products, or customer service, as well as to increase prices for consumers, reduce employee wages, and, in short, generate substandard conditions for all those involved." Under reduced-quality conditions, Article 19 added, no competitors can absorb consumer demand due to the lack of competitiveness in the digital market. Rafael Evangelista (Unicamp) associated market concentration and service quality deterioration with a disproportionate increase in profitability.

For traditional media associations, because data on zero-price platforms generally consubstantiate the price and quality of the services provided, privacy and data protection can be understood as relevant quality dimensions, as discussed in the amendment to WhatsApp's Privacy Policy, an example provided by Idec.

Flávia Lefèvre highlights that service quality, per the Consumer Protection Code (CDC) (BRASIL, 1990), is not limited to regulation compliance and entails safety obligations. Thus, according to the theory of quality, the binomials quality-adequacy and quality-safety emerge based on what can reasonably be expected from products and services, and, in addition to the safety related to consumers' physical integrity, includes respecting "their dignity, health, and safety, protecting their economic interests, improving their quality of life, as well as consumer relations transparency and harmony."

Following this broad concept of quality, Instituto Alana emphasized that the unique condition of children and adolescents as developing persons must be considered when defining "digital

product and service quality." Black Women Bloggers argued that attacks on users due to their very existence and values must be considered when analyzing service quality.

Lastly, Câmara.e-net and ALAI reiterate that the current legislation allows for the rigorous enforcement of sanctions against these concerns.

2.3.2 MITIGATION MEASURES FOR RISKS TO INNOVATION AND PRODUCT AND SERVICE QUALITY

Several participants defended developing measures to support alternative collaborative, national, and local business models to those of large platforms. Rafael Evangelista (Unicamp), from the scientific and technical community, measures to foster the coexistence of services with multiple business models and collaborative, not-for-profit services should be adopted. He argued that maintaining not-for-profit services relevant to the public interest should receive support.

Likewise, DiraCom stated that it is essential to develop public policies to foster models alternative to US private digital platforms, especially those developed by local agents for the communities in which they operate, thereby reasserting that the Internet is a common good. Slowphone proposed establishing public funding and incentives for "organic" technologies offering open services and alternative platforms.

Alex Camacho, from the scientific and technical community, asserted that measures such as technical service guarantees and special credit incentives create an environment that fosters the development of alternative models, promoting diversity of choices and stimulating innovation. Such measures can be implemented "through support and guidance programs, such as startup incubators, innovation centers, or accelerators," providing resources, expertise, and mentoring.

On the other hand, considering the dynamic nature of the digital markets and the fiscal context of the Brazilian State, Abranet opposed measures that rely on continuous public aid to remain economically viable. Instead, it proposed focusing on reducing the barriers to the entry of new agents, as it leaves it up to the private agents to define which alternative models are the most viable and comply with the demands of society.

Artigo 19 stated that the regulation should focus on fighting economic concentration and promoting competitiveness among market agents to maintain the quality of platform services, thereby empowering consumers to migrate to other platforms when product quality or supply declines.

Flávia Lefèvre stressed that measures to mitigate quality loss risks should reaffirm and enhance consumer protections stated in the CDC and consider safety obligations to determine service quality. Lefèvre mentions that several laws, such as the CDC (BRASIL, 1990), the MCI (BRASIL, 2014), the LGPD (BRASIL, 2018), the Electoral Law (BRASIL, 1997b), the Civil Code (BRASIL, 2002), the Statute of Children and Adolescents (ECA) (BRASIL, 1990) apply to digital platforms for damages caused by acts associated with their commercial activities.

Lastly, Idec suggests measures to prevent and remedy the negative impacts on the supply and quality of digital products and services resulting from high market concentration, such as the transparency obligations addressed in item 5.5 of Axis 2.

2.4 RISKS ASSOCIATED WITH THE ABSENCE OF A TAXATION MODEL SUITED TO THE SPECIFICITIES OF DIGITAL PLATFORM BUSINESS MODELS

Most organizations that commented on digital platform taxation highlighted the disproportionate advantages of large foreign platforms, recognizing the risks of the absence of an adequate taxation model. However, some private sector participants defended the principles of the current taxation system.

IAB Brasil stated that there is a taxation model in which each digital platform is taxed according to its business model, such as the Service Tax (ISS) for advertising and providing cloud services. Therefore, it considers that "substantial tax burden changes may render personalized advertising unviable for small players and advertisers in different markets" by increasing value chain costs and its consequent transfer to advertisers.

According to Câmara.e-net, ALAI, and ITI, the current Brazilian taxation system, and the system conceived in the tax reform in progress at the time of the consultation provide for the taxation

of digital services.[44] The Brazilian Revenue Service (Receita Federal) has already expressed its opinion, demonstrating that "companies that provide digital services in Brazil pay as much or more taxes than those that provide non-digital services." According to those inputs, this approach contemplates long-standing international tax principles, such as neutrality, efficiency, fairness, and simplicity. In this sense, levying a tax exclusively on digital services is redundant and excessively burdensome for the current Brazilian taxation system. In addition, it does not reflect the fact that the entire economy is becoming digital.

According to IBRAC and Abranet, this discussion should be specific and separate from discussions on digital platform regulation models. Abranet mentioned that legislative proposals on the subject, notably establishing a digital Economic Domain Intervention Contribution (CIDE), have been guided towards taxing and reducing the alleged "tax asymmetries" with telecommunications.

José Antonio Galhardo, from the government sector, asserted that the taxation of digital platform business models should be conceived as a parafiscal policy to equalize the conditions of competition with traditional business models. Ricardo de Holanda, from the scientific and technical community, considered that the existing tax asymmetry increases unfair competition and the disparity between Big Techs' customer service physical-technological infrastructures and those of traditional companies in other industries, such as broadcasting (television, radio) and telecommunications.

DiraCom maintained that "digital platforms appropriate the wealth produced in other sectors and do not reinvest the wealth acquired in Brazil, creating further imbalance." DiraCom added that the current tax model favors labor exploitation in countries and regions with fewer labor rights guarantees. Finally, it

[44] According to statements by ALAI and Câmara.e-net: "Currently, Brazil levies a Tax on Services (ISS), a Contribution for the Social Integration Program (PIS) and a Social Contribution on Revenue (COFINS) on digital services, in addition to corporate income tax and withholding taxes on the remittance of profits abroad. We understand that the proposed tax reform would levy a Value Added Tax (IVA) on products and services throughout the economy, regardless of whether a product or service is delivered physically or digitally."

emphasized the importance of defining a taxation model "suitable to the specificities" of digital platforms' business models.

Rafael Evangelista (Unicamp) highlighted that the opacity of the digital platforms' business models (and their earnings in each specific activity) prevents the development of an adequate taxation system, including considering the negative externalities of each operation, which need to be taxed. In this sense, transparency measures can also impact the taxation model.

2.4.1 MITIGATION MEASURES

Tarcízio Silva (Mozilla Foundation) proposed the possibility of a specific taxation regime, "taking into account digital platforms' characteristics and dimensions, such as business types, whether they are part of a big tech group, country of origin, and market dominance." Given the disproportionate advantages of large platforms, the researcher also suggested special taxation of small and medium-sized players, especially Brazilian players.

Ricardo de Holanda, from the scientific and technical community, mentions the possibility of creating a democracy and digital citizenship fund to "mitigate the digital gap between Brazil and other technological nations, consider copyright, culture, and digital regional communication financing and remuneration, and promote cyberculture and digital literacy for the youth and the elderly," similarly to the Universalization Fund for Telecommunications Services (FUST).

2.5 OTHER RISKS RELATED TO ECONOMIC AND COMPETITION ISSUES AND THEIR MITIGATION MEASURES

Other economic and competitive risks not initially listed in the consultation were mentioned and will be presented in this topic for reporting purposes.

Abranet emphasized that it is difficult for agents whose processed data is stored exclusively abroad – particularly small and medium-sized agents – to comply with judicial and administrative decisions. Therefore, the association defends asymmetric regulation in several instances.

Telefônica Brasil S.A. pointed out a new market failure due to the growth of the operations of platforms that use the network infrastructure in a massive and concentrated manner without fair remuneration. Therefore, the telecom operator stated that regulatory-competitive actions to address such negative externalities are needed and advocated for implementing "mechanisms that contribute to the sustainability of telecoms through the payment by digital platforms for the received services to balance the financial burden of telecom service providers."

Instituto Alana mentions the risks of profiling children and adolescents that, although addressed in other items, are connected to the risks posed by digital platforms, "as such risks are amplified when personal data processing is concentrated in a few companies, as well as by data sharing among actors in the same corporate group."

2.6 CONCLUSION ON ECONOMIC AND COMPETITION RISKS

The risks associated with the abuse of market power and economic and data concentration were some of the central topics addressed by the participants, with inputs from all sectors. Some consensus was observed among the third sector, the government sector, and the scientific and technical community regarding the relevance of the mapped risks, while the private sector was divided as to whether or not to recognize these risks as relevant or existing. Mitigation measures for such risks followed the same direction, albeit with a higher level of dissent.

In summary, part of the private sector, such as ALAI, Câmara.e-net, Brasscom, ITI, and IAB Brasil argued that digital markets are characterized by intense innovation and strong competition, consumer diversity, and constant change. Those organizations highlighted the benefits brought by digital platforms to the economy and claimed that, in general, Brazil already has a robust and comprehensive competition defense system capable of addressing potential anti-competitive behavior. However, most participants considered the risks relevant to regulation (except for the taxation model, which received fewer inputs). This perspective was shared not only by civil society and the academic and government sectors but also by private sector actors, such as Abranet and associations of traditional media companies.

On the one hand, part of the private sector considers that there is **no systemic risk of data concentration on digital platforms**, as this is not the only condition for the success of a platform, in addition to data being understood as "non-rival goods." On the other hand, many inputs consider that, as data are an essential input for the development of the platforms' business models, their concentration confers significant economic power to the platforms, as they can use it as leverage in other markets to improve and develop new products at lower costs, or to sell them indirectly. Therefore, data concentration may increase barriers to entry and market concentration, particularly in verticalized markets.

Part of the private sector does not consider the **risk of market concentration and abuse of economic power** as relevant to regulation, as concentration may also have positive effects, such as innovation, and the adverse effects (abuses) are already addressed by the competition law. In contrast, the remaining actors considered market concentration highly relevant in the digital market due to the platform characteristics contributing to establishing monopoly power and its abuse. In general, the primary factors that lead to market concentration and abuses are digital platform characteristics (e.g., economies of scope and scale and network externalities), anti-competitive strategies to expand monopolistic market power (e.g., self-preferencing and aggressive acquisitions of competitors), and exploiting of the comparative advantages of agents that hold large amounts of data. Those factors result in a **winner-takes-all** dynamics and a **lock-in effect**.

The **deterioration of innovation and product and service quality** was frequently addressed and considered a consequence of the previous risks. According to a significant number of inputs, environments that hinder innovation – by creating barriers to entry, for instance – prevent the emergence of better quality services and products, resulting in fewer alternative service options that respect human rights and have a greater diversity of opinions. The reason is that data on zero-price platforms consubstantiates service price and quality: it was pointed out that abusive data collection by digital platform services may cause overpricing or the provision of poor-quality services in typical markets. On the other hand, some of the private sector mentions the benefits and innovations brought by digital platforms.

The relationship with the **advertising market** – a regulatory and competitive focal point in several countries – was also highlighted in the inputs. Many of the proposed regulatory measures were initially debated considering that market.

Platform **taxation** received fewer inputs, but a group of participants considered it a relevant risk for regulation, whereas another group (some of the private sector business associations) stated that taxation should not be discussed within the scope of platform regulation.

This scenario indicates that there is an **overlap with the previously mapped risks**. The risk of market concentration and abuse of economic power may be understood as an 'umbrella' for other risks: it was pointed out that the risk of abuse of economic power has negative effects on innovation and product and service quality and that data concentration is one of the factors that contribute to market concentration and its abuse. For discussion purposes, economic risks may be organized as follows:

FIGURE 2 – DYNAMICS OF ECONOMIC AND COMPETITIVE RISKS OF PLATFORM ACTIVITIES

SOURCE: PREPARED BY THE AUTHORS.

As to the measures to mitigate the risks above, **data interoperability** was the measure with the highest level of consensus within the economic group. However, there was significant dissent regarding their implementation, scope, and mandatory nature for digital platforms. Most participants highlighted the importance of establishing minimum standards that ensure data standardization and openness to facilitate their transfer. Some business associations, however, support a greater flexibility of interoperability standards, which should not be mandatory in all cases. Other topics addressed were compatibility with the ANPD's powers and the establishment of asymmetric obligations (for gatekeepers only or not).

The **future expansion of the objectives of the Brazilian System of Competition Defense - SBDC** (BRASIL, 2011b) was less discussed. Those in the private sector who submitted inputs on the matter argued that expanding SBDC objectives would risk making the competition law vulnerable and that emergent issues need to be specifically addressed. Participants from the third sector and the scientific and technical community, on the other hand, argued that other objectives, such as personal data protection or market diversity, may be incorporated as a consumer well-being parameter, including product or service quality elements, or, conversely, as an element of the abusive exercise of a dominant position.

Regarding mitigating risks to innovation, **fostering alternative platform economic models** that apply sovereignty and diversity metrics was highlighted. Third-sector organizations, in particular, advocated measures to support both national and local collaborative business models. However, some of the private sector opposed measures that rely on continuous public aid to remain economically viable and proposed focusing on reducing barriers to the entry of new agents.

Other mitigation measures suggested to address the risks generated by vertically integrated ecosystems include structural measures, such as market separation, or conduct measures, such as database segregation or self-management.

- **Data sharing among companies of the same corporate group** was the subject of the highest disagreement, particularly by the private sector, which states that measures to limit and prohibit such data sharing already exist. The other sectors (with a few exceptions) understand that these measures are essential to mitigate the excessive concentration of economic power and the formation of closed ecosystems, given that data sharing allows companies to leverage their position by cross-referencing data in related markets, gaining an unrivaled advantage.
- Regarding the criteria for **notification of concentration acts**, part of the private sector understands that total revenue and number of users are not indications of a dominant position and should not be used as notification criteria, arguing that such criteria are arbitrary, leading to innovation stagnation by private agents. Some participants mentioned that the safety valve could be better used to analyze concentration

acts that do not meet the current revenue criteria. Another group of participants, however, advocated using asymmetric regulatory instruments to review safety criteria and establish the mandatory notification of gatekeeper operations, considering that the revenue criterion does not cover relevant operations in digital markets.

- **Self-preferencing** mitigation measures were one of the main focus of the discussion. Part of the private sector argued that self-preferencing is a standard business practice that may reduce costs and increase efficiency, and therefore, suggested assessing possible abuses on a case-by-case basis. Most participants, however, stated that it is a new form of abuse of a dominant position, specifically in digital markets, and recommended that it be prohibited to mitigate platform monopoly and verticalization risks.
- The **prohibition of integrated and vertical operations** and the compulsory division of giants were highlighted by some organizations in the private and third sectors. Third-sector organizations supported potential ownership restrictions, such as separating platforms into two distinct services: content server and content curator. However, part of the private sector maintained that such measures impose arbitrary limitations on economic agents.

Lastly, **several inputs linked economic and competitive risks to rights and digital sovereignty threats**. Several participants argued that market concentration directly jeopardizes fundamental rights, increases consumer vulnerability, and affects service safety and quality, pervasively harming individuals and democratic institutions, as addressed in the other risk groups of this axis. Moreover, the lack of diversity of actors, common in concentrated and closed markets, directly impacts freedom of expression.

3 RISKS RELATED TO THREATS TO DIGITAL SOVEREIGNTY, TECHNOLOGICAL DEVELOPMENT, AND INNOVATION

Inputs on **digital sovereignty** sought, in addition to discussing the risks and their mitigation measures, to explain the conceptual challenges and the multidimensionality of the

concept of digital sovereignty, a term still under dispute. ISOC Brasil warned about the risks of "establishing a single, fixed definition of digital sovereignty hinders the understanding of other actions/policies" that may also integrate the concept. The entity listed different approaches to the term. Firstly, it asserted that digital sovereignty may be

> *[...] associated with the concept of* ***State control and power over the entire digital environment****, concerning the different layers that make up this environment (physical infrastructure, codes, software, hardware, operating protocols, among others) and the protection of national security, data and information flows, and the establishment of digital environment policies (and the means to ensure their enforcement) [our emphasis].*

Another approach suggested by ISOC Brasil, which also assumes the State's capacity to develop and manage digital actions and policies, is the "development of the local industry of technologies, platforms, and different digital services," aiming to reduce the dependence on foreign companies, achieve economic autonomy, and promote the competitive capacity of the domestic market. The third approach mentioned by ISOC Brasil refers to the "autonomy/self-determination of individuals, groups, and social movements," considering their individual and collective capacities to "act and make decisions on their information and data flows autonomously and independently, according to their interests, values, and culture."

CTS/FGV questioned the digital sovereignty perspective adopted in the consultation, arguing that it is limited to "the country's capacity to independently protect and develop its digital infrastructure and ensure the protection of personal and strategic data of its citizens." Instead, it has adopted a broader approach, which allows grasping the "relevance and interconnection of i) data, ii) software, iii) hardware, iv) education and training, and v) governance." Furthermore, CTS/FGV emphasized the importance of multi-stakeholderism and establishing a "governance model that allows cooperation and collaboration among actors, as well as sharing information on cyber risks, threats, and incidents."

In line with one of the definitions mentioned by ISOC Brasil, CTS/FGV defines digital sovereignty as the "capacity to exercise power and control over digital infrastructures and data, and

implies understanding the effects – positive and negative – of each technological choice." It observed that it is essential to adopt a systemic vision that considers the different elements of the digital ecosystems and their interrelationships to regulate technology "instead of being regulated by it." Considering that digital technologies are transversal, it argues that such challenges should mostly be addressed "by specific regulations, not precluding certain cases to be specifically addressed by digital platform regulation."

ALAI cautioned that using such a vague term, "which may encompass several different concerns," poses conceptual challenges. It considered the "security and resilience of products and services intended for Brazilian users, including the confidentiality of public and private information, as well as the protection of the confidentiality and integrity of personal data" risks related to digital sovereignty.

REDE asserted that digital sovereignty is one of the "essential elements of what has been termed in the literature as digital colonialism," a phenomenon that harms the country's social development and is directly associated with digital platform activities.

In addition to those previously listed in the consultation, other risks were mentioned. CEPI/FGV, for instance, warned of the possibility of the dismantlement of the critical national communication infrastructure due to a lack of investments. It highlighted that the growing need for bandwidth of new Internet applications requires significant investments by telecom companies that are difficult to transfer to the end consumer, thereby creating barriers to effective investments.

The Technology Center of the Homeless Workers Movement[45] (MTST) asserted that digital sovereignty should be democratic. It emphasized the need for establishing mitigation measures that consider the "social appropriation of technologies that foster people's organization and empowerment, which demands substantial access to the real Internet, critical digital and technological education, and which develops and promotes worker-owned platforms." Likewise, the Mocambos Network[46] proposed:

[45] Núcleo de Tecnologia do Movimento dos Trabalhadores Sem Teto.

[46] Rede Mocambos.

> *[...] fostering community and civil society initiatives closer to the people. Tainã Cultural Center (Casa de Cultura Tainã) created a community data center to host services to meet the Center's and its partners' demands [...]. That methodology and model could be adopted as a national public policy.*

Therefore, the discussion on digital sovereignty was strongly connected with economic and infrastructure concentration, particularly regarding data collection and processing infrastructures, as analyzed in the previous risk group, and infrastructure development, usually addressed within the scope of telecommunications regulation or industrial and technological development policies. However, the discussions have in common the need to oppose large platforms' power abuse and the concern about unequal control over data, which are why they were also addressed in the debate on platform regulation despite being multidisciplinary.

3.1 RISKS ASSOCIATED WITH THREATS TO BRAZILIAN TECHNOLOGICAL SOVEREIGNTY OVER CRITICAL INFRASTRUCTURES

Most inputs pointed to the advance of digital platforms on different aspects related to Brazilian critical technological infrastructures to operate their applications. CTS/FGV emphasized **the need to define the concept of critical structures**, the dimensions to be considered, and how they relate to the services provided to citizens:

> *Once a group of services related to the public interest, which can be provided through digital platforms, is defined, the regulator needs to adopt measures to mitigate those risks to maintain the effective control of digital infrastructures and data and to prevent national dependence on foreign companies and digital colonization.*

Concepts related to colonialist theories were mentioned to explain the new wealth and labor exploitation process in foreign territories, which may affect their authority to define markets and cultural and political aspects. Tarcízio Silva (Mozilla Foundation) pointed out the moderation role played by digital platforms in the public sphere and "their disproportionate communication power,"

which is occasionally exerted to pressure governments and that may put the population at risk. Silva referred to cases of "news blockade in countries they operate," such as Australia and Canada.

CEPI/FGV, analyzing the data reported by the Surveilled Education Observatory[47] (2021), part of Open Education Initiative on elementary education, found that out of 76 Brazilian education departments (at the state and municipal level, capital cities, and municipalities with more than 500,000 inhabitants), "38 use Google/Microsoft, and 38 use alternative systems." Of the 144 higher education public institutions in Brazil, "79.17% use the services provided by Google/Microsoft, and only 20.8% use alternative services." According to CEPI/FGV:

This situation raises three intersecting concerns:

> *1)* ***Big Techs*** *have access to large amounts of personal data, including that of children and adolescents, in addition to academic behavioral and performance data; 2)* ***scientific data and other knowledge produced in the country are stored in foreign companies*** *and increasingly depend on this infrastructure to continue to be produced and stored; 3) the lack of transparency on how data are processed by the company, which directly impacts the privacy and data protection of the data owners who are subject to these services, prevents risk assessment and informed decision-making about their adoption and use [our emphasis].*

Several participants expressed concerns regarding the use of digital platforms in education and research in Brazil. REDE, for instance, reported that:

> *[...] platform operations in strategic areas for the exercise of sovereignty not only in technology but in areas that have become digital, such as education, pose* ***threats to sovereignty over strategic and national interest data****, such as scientific data [our emphasis].*

Citing the National Research Network[48] (RNP) as an example of a strategy to strengthen technological sovereignty, REDE

[47] Observatório Educação Vigiada.

[48] Rede Nacional de Pesquisa.

emphasized that the RNP can "address other needs of the Brazilian academia in terms of communication software and hardware."

Also, in education, the Alana Institute considered that the agreements signed between state education departments and Big Techs may enable "the collection of children's and adolescents' data in the education setting for commercial purposes by the contracted companies," whose inadequate privacy policies may "allow the inappropriate use of those data." The institute suggested including other criteria, such as "fostering the development of alternative models, platform cooperative systems, national infrastructure, and respect for children's rights."

ITI asserted that addressing the threats to Brazil's critical infrastructure requires a "flexible, risk-based cybersecurity structure that uses international standards based on consensus and public-private partnerships as references." For the institute, the collaboration between the government and the private sector is essential "to build trust and improve cybersecurity, as the private sector owns and operates most of the critical infrastructures." Based on that perspective, ITI mentioned two examples:

> *[a] The Joint Cyber Defense Collaborative of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which gathers cybersecurity experts from the public and private sectors to work on holistic cybersecurity planning, cyber defense, and incident response; and [b] the National Institute of Standards and Technology – NIST Cybersecurity Standards, which compiles standards, best practices, and guidelines for managing cyber risks.*

3.1.1 PREFERENCING CONTRACTS OR INVESTMENTS IN NATIONAL TECHNOLOGIES THAT COMPLY WITH THE CRITERIA OF A TECHNOLOGICAL SOVEREIGNTY DEFINITION

Brasscom highlighted the benefits of the expansion of the digital ecosystem, which drives economic growth and innovation and creates opportunities "in addition to promoting the Digital Transformation of society." However, it warned against the increase of "constantly evolving risks and threats to networks, systems, and data." It considers that "cybersecurity efforts must

be equally dynamic, highly interoperable, and adaptable, seeking to address the constantly changing threats that pose risks to those new technologies." However, **Brasscom, ALAI, and ITI warned that subsidies to invest and to hire national labor and technology do not necessarily "mitigate risks to the Brazilian technological sovereignty and lead to distortions of competition** among providers to the detriment of users" [*our emphasis*]. Brasscom pointed out that:

> *By introducing a regulatory framework that favors one set of providers over others, competition based on merit is reduced, eventually resulting in fewer economic incentives to invest and compete, potentially compromising the quality levels currently available in Brazil. Instead, regulation should be neutral and equally applied to allow free competition per constitutional provisions.*

Furthermore, Brasscom argued that the "Brazilian government should refrain from imposing preferences in contracts or investments in national technologies that comply with the criteria of a technological sovereignty definition, and, instead, should consider cost-benefit ratios, innovation, and security."

On the other hand, Filipe Saraiva (UFPA) and Rafael Evangelista (Unicamp) asserted that imposing preferences for national software and infrastructure is perfectly legitimate and desirable; furthermore, when associated with hiring local labor, it contributes to the "national control of technology." According to Evangelista, "sovereignty must supersede any efficiency considerations."

Tarcízio Silva (Mozilla Foundation) proposed measures that, if implemented, may benefit the country's digital sovereignty:

> *a) collaboration among providers for the development of universal access policies and plans; b) robust data centers in the national territory; c) investing and consulting the civil society and academia; d) using open-source software when appropriate; e) prioritizing national third-party providers; f) adhering to good practices of algorithmic system communicability and explainability; g) regional distribution; h) management diversity and inclusion policies.*

3.1.2 INVESTING IN CRITICAL PUBLIC COMMUNICATION INFRASTRUCTURES

Some participants, such as Filipe Saraiva (UFPA), supported investing in public infrastructures, pointing out that high-speed connection infrastructures are essential. REDE stressed the importance of "low-orbit satellites to serve indigenous populations and hard-to-reach regions for small providers" and suggested investing in "routers, antennas, and radio technologies to promote the development of urban and rural autonomous and community networks."

Rafael Evangelista (Unicamp) mentioned that the State can support cultural content distribution platforms in the role of provider of "interoperable content distribution infrastructures on the Web," which, in addition to promoting technological development, also contributes to the creation of suitable spaces "for the publication and distribution of national content to its citizens."

The Activism and Communication Lab of the School of Communication of the Federal University of Rio de Janeiro[49] (ECO/UFRJ) emphasized the need to build "national computing capacity in order to meet the volume currently required for the development of Artificial Intelligence" as the supercomputers currently existing in Brazil "do not have a fraction of the capacity required for the development of Chat GPT by Open AI." It added that having the "databases required" for the development of AI is essential and that these databases should be public, using anonymized data, and "shared by all platforms that provide services agreed upon with public bodies, such as health and education organizations."

3.1.3 INCENTIVES FOR THE DEVELOPMENT OF QUALITY, SECURE, AND AUDITABLE OPEN-SOURCE SOFTWARE BY NATIONAL COMPANIES

Regarding measures to promote the development of national software companies, Rights in Network Coalition[50] (CDR) proposed, as a guideline, that "choosing free and open licenses and technologies should be a State policy, promoting and

[49] Laboratório de Ativismo e Comunicação da Escola de Comunicação da Universidade Federal do Rio de Janeiro.

[50] Coalizão Direitos na Rede.

prioritizing their development and implementation." CDR stated that this measure will lead to the "incremental and continuous collective development of technologies and systems used by public authorities," resulting in higher "security, harmonization, interoperability, and transparency levels."

Alex Camacho highlighted that open-source software grants access to the source code, allowing its adaptation to specific needs. "In addition, it promotes transparency and collaboration among developers, allowing independent audits and increasing the reliability of the security and integrity of the software used in critical infrastructures." To this end, Camacho suggested funding projects in partnership with universities in addition to giving tax incentives. Hora's Institute[51] added that free software development can be supported by "establishing interoperability standards, cybersecurity guidelines, or licensing requirements favorable to open source."

ALAI proposed adopting the "Open Security" concept based on "open and interoperable systems, built according to international standards." That strategy would be permeable to security innovations and take advantage of the "globally distributed infrastructure, which is much more resilient and resistant to the denial of service attacks." Another issue mentioned by ALAI is related to governance, that is, the need to define "multistakeholder governance processes, open debate, and the global engagement of security researchers."

3.2 RISKS RELATED TO THE CROSS-BORDER FLOW OF BRAZILIAN CITIZENS' INFORMATION AND DATA

Inputs on the risks posed by international data flow were divided into two approaches: i) concerns about its impacts on personal data protection and ii) economic and technological development and collective self-determination strategic issues.

Regarding concerns about the **impacts of international data flows on personal data protection**, ITS referred to prominent EU cases to illustrate the conflicts on that subject, such as when the Irish Data Protection Authority "fined Meta 1.3 billion euros

[51] Instituto da Hora.

for irregularities in the international transfer of the personal data of EU Facebook users to the US", and the "Court of Justice of the European Union decisions that invalidated bilateral agreements, such as the Privacy Shield (EU-US)." Although that is primarily a data protection issue, regulated by instruments such as the GDPR (EU, 2016) and the LGPD (BRASIL, 2018), ITS asserted that there is still much legal uncertainty. In Brazil, explained CTS/FGV, international data transfer mechanisms have not yet been regulated by the ANPD.

These risks were also recognized by DEIN insofar as

> *[...]* ***the cross-border flow of information and data may threaten the protection of the privacy and security of Brazilian citizens****, such as potential violation of privacy and misuse of Brazilian data by third parties, especially in light of the regulatory framework already established in the country, such as the General Data Protection Law (LGPD) [our emphasis].*

According to DiraCom, because processing data outside their country of origin is the basis of digital platforms' operations, **data leakage risks**, **disputes over the jurisdiction** of data processing regulations (which often results in disregard of the legislation in force in Brazil) and **unjustified obstacles to access to data** by Brazilian authorities and data owners. Regarding leakage risks, Tarcízio Silva (Mozilla Foundation) illustrated the "decision of the Court of Justice of the State of Maranhão condemning Facebook to compensate eight million Brazilians" for leaking their data. IP.rec also discussed the risks related to the **lack of transparency** regarding how Brazilian citizens' data are stored and which parties can access them.

However, ALAI and Câmara.e-net argued that privacy protection and data flow could be compatible by promoting international consistency among privacy systems, such as the GDPR and regional and bilateral trade agreements. They noted that the "LGPD already covers international transfers of personal data, and the ANPD will soon adopt a secondary regulation to specify better the regime that applies to them."

Several organizations also expressed concerns about **the impact of international data flows on sovereignty**. CTS/FGV argued that, considering that the main driver of the digital

platform business model "is the use of data and the formation of large databases, which, in most cases, are processed on servers not located in Brazilian territory," the consequences of the location of these servers – not addressed in the LGPD (BRASIL, 2018) – should be explored. It pointed out that "data location policies have been recently adopted in more than seventy countries, driven by the example of Russia, which, from 2015, has adopted restrictive regulatory provisions for the cross-border data flow in response to Edward Snowden's revelations about the global surveillance scheme orchestrated by the US National Security Agency."

José Galhardo, from the government sector, also mentioned personal data flow risks, particularly concerning IoT development and national defense strategic facilities.

REDE mentioned other risks that motivate data location policies. Examining data circulation from an ethnographic perspective, it stated that "the circulation of Global South data in the Global North is evident, whereas the opposite is not true." Therefore, REDE argued that "the cross-border characteristics of the Internet affect global populations differently according to where we are located in this infrastructure" and, as previously mentioned, there is "the **risk of losing sovereignty over strategic sectors**, such as science, which is inseparable from the cross-border characteristic of data circulation" [our emphasis]. In that regard,

> *Google and Microsoft's operations in Brazilian universities, such as e-mail management and content storage, make scientific sovereignty vulnerable to data transfer to other jurisdictions. Such* ***data may be processed by and assimilated into US infrastructures, and their extraction may be imperceptible*** *[our emphasis].*

In addition to the educational and academic research sector, participants mentioned that hiring multinational companies to manage public administration information[52] could undermine

[52] In its input, REDE mentioned cases "such as the adoption of Microsoft Artificial Intelligence by the National Employment System to profile unemployed citizens aiming at finding appropriate jobs for each profile [...]. Another appalling example was the attempted privatization of SERPRO (Federal Data Processing Service) during Bolsonaro's administration, halted by government decree by [President] Lula in 2023."

both national and individual sovereignty, as it compulsorily subjects the population to the monetization of their data, a vital component of the platforms' business model.

Likewise, ECO/UFRJ referred to the risks of hosting "in territories subject to other legislation [...] a large volume of scientific and strategic information." It provided the example of Sweden, which prohibited "its public institutions from adopting Google systems." In Brazil, Decree 8,135 (BRASIL, 2013a), issued by President Dilma Rousseff and revoked by the Temer administration in 2018 (which, in turn, was revoked by the Bolsonaro administration in 2021), established that "data belonging to federal direct administration, autarchies, and foundations must be transmitted through telecommunications networks and information technology services provided by bodies or entities of the federal administration, including state-owned companies."

However, several business associations, such as Abranet, Brasscom, ALAI, and Câmera.e-net, as well as CEPI/FGV, of the academic sector, refuted the relevance of that risk, as they consider that international data transfers are required for Internet operations, benefit users, and are safer than local storage. CEPI/FGV, for instance, mentioned risks related to digital sovereignty, arguing that "depending on the types of data and information circulation limitations imposed by other countries [...], the right to information and free access to the Internet of Brazilian citizens may be harmed."

According to Brasscom,

> *[...] the technological and procedural methodology of data storage and transfer, the technology employed, user experience, knowledge of those involved, and good institutional practices determine how secure the information is, not the location where the data is stored.*

Brasscom argued that locating data locally does not enhance cybersecurity, and employing less advanced technologies could threaten national security, as it may allow attacks and compromise relevant information because criminals would know where the data are located.

Câmara.e-net and ALAI stated that "regulation should allow and promote international data transfers, rather than prohibiting

or restricting them," as they are technically required for the Internet to function[53] and directly benefit citizens, allowing them to access multiple information and socially connect worldwide by reducing data latency, for instance. Instead of risks, they listed the benefits brought by international transfers of:

> *i. driving international and local trade and development. [...]*
>
> *ii. supporting innovation, research, and development across multiple sectors. [...]*
>
> *iii. fostering international cooperation, including international trade, law enforcement, and national security*
>
> *iv. allowing us to remain emotionally and socially connected.*

The same benefits were highlighted by ITI. Regarding possible harms, ALAI and Câmara.e-net said that preventing cross-border data flows "harms cybersecurity and data protection, generates significant damage to local economies, and harms Internet users' rights to privacy, freedom of expression, and access to information."

Likewise, Abranet argued that excessive data location obligations may harm the usability and scope of the services offered. According to that organization,

> *Although arguments, such as "enhancing enforcement" and "data security and privacy," are commonly put forward in this discussion, they still need to be weighed according to the specificity of the agents in Brazil and their actual effects. In this sense, considering that the implementation of such mechanisms imposes high technical and financial costs on the controllers – in addition to potentially reducing efficiencies by restructuring specific data segments of a global structure (for example, regional clouds) – it harms economic growth and development by placing an excessive burden on smaller agents.*

[53] According to ALAI and Câmara.e-net inputs, "Considering how the global Internet was built and evolved, data processing across national borders are part of almost all online communications or activities and often include those that are entirely domestic. The networks over which data travel are typically unaware of the data physical 'journey,' and instead optimize real-time routing to reduce latency, increase network resilience, and enable real-time connections."

In this sense, the burdens on smaller agents should also be considered in a possible asymmetric regulation of cross-border data transfer.

3.2.1 MITIGATION MEASURES

ALAI and Câmara.e-net stated that Brazil should ensure that data transfer preconditions do not cause excessive [financial] burden, leading to *de facto* data location requirements, as "a structure or guidance that is impossible or extremely onerous to comply with in practice will harm Brazilian citizens and companies."

According to ITS, platform regulation in Brazil should consider those risks (particularly to social media, search engines, and private messaging applications), and "contribute to develop robust regulatory solutions and take into account their interaction with other regulatory systems."

CTS/FGV also argues that, relative to data protection risks, "the most appropriate means of addressing them is to develop a solid data protection regulatory framework that can be effectively and efficiently enforced."

3.2.1.1 MECHANISMS FOR LOCATING STRATEGICALLY RELEVANT DATA CATEGORIES IN THE BRAZILIAN TERRITORY

According to DEIN, "defining data categories and establishing mechanisms for locating those data in the Brazilian territory may be relevant to mitigate the risks associated with the cross-border information and data flows." However, according to the Brazilian government department, it is necessary to consider technical, legal, and economic issues and balance the protection of sensitive data with the need to promote innovation, information flow, and economic and technological development.

CTS/FGV and DiraCom also agreed that requiring some data categories to be stored in the national territory is a mitigation measure, including possible processing and access to databases located abroad. REDE, recognizing the risk cross-border flows pose to sovereignty in strategic sectors, such as science and public administration, stated that a legal measure to prevent the sale of national data and data infrastructure is required.

Furthermore, the Sociotechnical Studies Lab of UFPA[54] emphasized that the "Brazilian State should invest in data storage infrastructure (datacenters) for public universities and public research and technology institutions." It argued that the fact that "80% of institutional e-mails of Brazilian public higher education institutions" are hosted by Google and Microsoft increases "the dependence of institutional operations on a few large companies." Therefore, as a guideline, it proposed that national public services should not use "digital services offered by private companies whose servers are located abroad" since "data generated by public services should not be the basis to increase the value of private companies."

However, as previously mentioned, business associations, including Câmara.e-net, ALAI, Abranet, and Brasscom, opposed data location rules in a broad sense. Abranet, for instance, referring to the LGPD (BRASIL, 2018) and the MCI (BRASIL, 2014), asserted that there are no reasonable grounds for establishing such obligations and that the argument of "strategic importance" is disproportionate, as it does not provide for sufficient efficiencies or protections that justify such burden to agents and holders.

ITI suggested applying the measures to mitigate potential personal data protection risks contemplated in the Brazilian legal system (LGPD), such as the "compliance model," including a list of countries that offer "compliant" privacy protection levels or alternative data transfer mechanisms.

3.2.1.2 BUILDING FEDERATED NETWORKS FOR DATA TRANSMISSION IN THE NATIONAL TERRITORY AND ABROAD

Only two participants contributed to this topic.

According to Alex Camacho, the purpose of building federated networks[55] is to strengthen data communication and transmission infrastructures, allowing the safe and efficient exchange of information and ensuring data integrity and confidentiality. Camacho stated that "federated networks may support the

[54] Laboratório de Estudos Sociotécnicos da Universidade Federal do Pará.

[55] Broadly speaking, federated networks are decentralized data-sharing infrastructures.

implementation of control and governance mechanisms over data flows, providing greater transparency and protection of national interests." DiraCom supported that measure.

3.3 RISKS ASSOCIATED WITH ESPIONAGE, PRIVACY INVASION, AND INFLUENCE OPERATION THREATS

CTS/FGV illustrated those risks by mentioning the revelations made by Edward Snowden, which unveiled the dimension of espionage, privacy invasion, and influence operation challenges and are "closely associated with cybersecurity and digital sovereignty studies." CTS/FGV pointed out that "cyber incidents, which often occur when using digital platforms," affect the "provision of essential services to the population" and undermine personal data protection and citizens' trust in public institutions. It emphasized the risks related to "technology device invasion practices and unsafe behaviors by the users themselves or adopted by technology developers, software, and digital systems," in addition to issues related to privacy and data protection risks.

Regarding cyber incidents, Hora's Institute mentioned "cyber attacks on financial institutions," pointing out their growth in recent years in Brazil, in which hackers use "advanced techniques to obtain unauthorized access to systems, steal personal data, and perpetrate financial fraud." The institute added that "Brazil holds important strategic sectors, such as energy and oil," and companies in these industries had information stolen and used by "foreign agents or competitors to obtain competitive advantages." Likewise, Rafael Evangelista (Unicamp) argued that State strategic and official communications should only use "technologies, including hardware and software, over which it has full control and ensures the confidentiality of communications." MTST Technology Center proposed "prohibiting the use of proprietary software in the Federal Public Administration, including the repositories in which source codes are stored."

Privacy violations received a significant number of inputs. CEPI/FGV proposed using the concept of surveillance capitalism to analyze the massive collection and processing of personal data carried out by platforms, which are often not strictly necessary but represent the primary input of their services and are "useful for their commercial interests." According to CEPI/FGV, regardless

of the efforts made to enforce the LGPD principles (BRASIL, 2018) to mitigate such risks, digital platforms "can still process non-personal data and information that are strategic for the development of companies and even to governments," resulting in possible privacy violations, which, collective, pose risks to the country. Furthermore, it mentioned the clash between the US and China regarding TikTok, in which the US government expressed reservations about the application, arguing that

> *i) it would be used by the Chinese government to spy on US citizens because the company that owns the app is Chinese and is required to pass on data to the Chinese government, and ii) the app's algorithm would be exploited to influence public opinion. Other countries have chosen to suspend the use of the app in the public sector due to cybersecurity concerns [...] under the justification that politicians and civil servants have access to potentially sensitive information on their professional cell phones. The suspension was adopted in Canada, Denmark, the Netherlands, Latvia, Norway, the United Kingdom, New Zealand, France, and Belgium.*

DiraCom warned against the "processing of Brazilian citizens' data abroad, particularly in countries targeted by espionage and influence operations," which may lead to undue access to information, "even if Brazilians are not the direct and primary targets of such operations." These concerns were also raised in the previous item. In contrast, according to ITI,

> *[...] The technological and procedural method of data storage and transfer, the type of technology used, user experience, stakeholder awareness, and good institutional practices determine the security and protection of information, not the geographic location where the data are stored.*

ITI asserted that data location should not be regarded as one of the pillars of Internet security, leading "to a false perception of security." It stressed the importance of encryption, mentioning that the "technology sector incorporates strong security features into its products and services to build trust, including the use of algorithms for default encryption." In this sense, ITI encouraged governments to employ strong, "globally accepted and deployed" cryptography and other security standards that provide trust and interoperability."

Regarding influence operations, Tarcízio Silva (Mozilla Foundation) reported that large digital platforms have "capacities to perform influence operations in different contexts," as shown "in 2012, when Facebook scientists published the paper 'A 61-million-person experiment in social influence and political mobilization'," demonstrating that:

> *[...] A test with 61 million users in 2010 increased voter turnout. The experiment used the "social influence" mechanism by adjusting the platform to display or not the "number of friends who voted" cards. In 2014, the article "Experimental Evidence Of Massive-Scale Emotional Contagion Through Social Media" reported a massive study with more than 600,000 users who did not grant their consent. Facebook demonstrated that it was able to influence users' emotions through changes in its feeds.*

CTS/FGV mentioned that disinformation activities on digital platforms "a) negatively affect electoral processes; b) promote hate speech, intolerance, racism, sexism, and other discriminatory behavior; c) lead to political, institutional, and economic destabilization of a country; d) undermine relations among different nations; and e) threat collective health and people's physical integrity." It added that digital platforms should conduct systemic risk analyses and observe the duty of care to mitigate such effects.

3.3.1 MITIGATION MEASURES

Ricardo de Holanda Melo Montenegro considered that "strengthening national information and communication technology market" is critical to mitigating Internet security risks and mentioned "services provided directly by the State or public-private structures." According to Montenegro, the State is a driving force of technology development and, therefore, should establish "technology islands in different regions of the country," expand the "technological workforce, create opportunities, substantially generate technological jobs," and develop quality technology services able to compete with those offered by "foreign Big Techs."

CTS/FGV proposed several mitigation measures regarding the risks listed in its input. Regarding espionage threats, it points out that it is necessary to: "i) contract device intrusion control software; ii) promote an information security culture; and iii) [adopt] incident prevention policies." Relative to the invasion of privacy, it suggested "i) sharing information on vulnerabilities and cyber incidents" that allow for accountability; ii) encouraging the reporting of "all cyber incidents; iii) establishing practices that respect Human Rights." Finally, concerning influence operations, it proposes: "i) developing systemic risk analyses, considering platform size; ii) [observing] duty of care when adopting measures to mitigate those risks, or be liable for omission."

IRIS proposed organizing mitigation measures according to three main pillars: "a) regulatory measures; b) users' education; c) positioning based on the use of digital tools, i.e., digital solutions." The pillars are divided, according to the institute, into:

> *[...] data protection and encryption; platform accountability and transparency for data processing [and regular audits]; [informing] users about the use, storage, and sharing of their data; user education and awareness [by promoting] digital literacy; international cooperation in order to establish common standards and share information to mitigate espionage risks.*

3.4 CONCLUSION ON DIGITAL SOVEREIGNTY, TECHNOLOGICAL DEVELOPMENT AND INNOVATION RISKS

The concept of digital sovereignty, still under dispute, can be understood as an umbrella for the other risks discussed in this group. There is a significant interface between the risks associated with technological sovereignty in critical infrastructures and those related to international data transfer, in which the latter may be part of the former, i.e., service provision in strategic sectors by multinational companies generally implies processing relevant data of Brazilians abroad. Moreover, storing and processing data generated in those strategic sectors abroad entails higher risks. Threat and espionage risks can also be part of the digital sovereignty debate if a broad approach is adopted.

Regarding the risks associated with international data transfer, some private sector participants opposed data location requirements and defended the benefits of free data flow. On the other hand, participants in the third sector, academia, and the government sector expressed concerns about the possible risks posed by unrestricted international data transfer to personal data protection and digital sovereignty. Although private sector participants argued that measures to remedy risks to personal data protection are already in place, such as the ANPD suitability model or model clauses for data transfer, the third sector mentioned the challenges of implementing such measures, as illustrated by the cases under debate in the EU.

Finally, the few mentions of infrastructure development solutions for risk mitigation, such as federated networks, indicate that further discussions are needed.

4. RISKS RELATED TO THREATS TO DECENT WORK

Some participants pointed out aspects of building a regulatory framework on digital labor that they considered relevant. For instance, the digital platform business association Digital Innovation Movement[56] (MID) stressed that the regulatory debate on labor and digital platforms should be grounded on data and research by applying a Regulatory Impact Analysis (RIA) and actively listening to all workers involved. ITS mentioned the need for "workers' participation in decisions that affect their working conditions through surveys, discussion forums, or representation on committees or advisory boards," in addition to multi-sectoral participation.

Workers and other actors have participated in relevant discussions within the scope of the Working Group (GT) of the Federal Government on labor in digital platforms (BRASIL, 2023b), as mentioned by ALAI. According to ALAI, given the existence of this WG, the CGI.br consultation "is not the appropriate forum to discuss labor matters as companies in specific industries are subjected to specific labor legislation," explaining why it would not comment on this risk group.

[56] Movimento Inovação Digital.

ITS argued that any specific regulation may restrict or obstruct the presence of companies in some segments. However, if labor issues are not discussed at all, no incentives for developing standards by the private sector are created, and no guidelines pointed out by the public sector are offered. Consequently, those issues are episodically decided by the Judiciary, and no public policies on the subject are developed.

According to CEPI/FGV, whose inputs were based on a mapping of 128 federal bills proposed between 2015 and 2021, specific labor legislation, harmonized with general laws and rules applicable to platforms, is required.

4.1 RISKS ASSOCIATED WITH PRECARIOUS WORK

A significant number of inputs on this topic highlighted that the regulation should consider the diversity of forms of work on (or around) digital platforms.

According to research carried out by CEPI/FGV CEPI/FGV (CAMELO, 2021b), several studies indicate a decrease in formal job generation and labor platformization, which includes a wide variety of types of platform work. Some categories, such as delivery and transportation, are more visible and well-known, while others are less visible and known, such as web-based ones. However, CEPI/FGV argued that the risk is not necessarily posed by the emergence of new forms of work but by the **difficulty of regulating them or applying potentially pertinent regulations**.

ITS highlighted that the outsourcing and microwork ecosystem used by digital platforms are rarely addressed in regulatory initiatives. It added that the debate about platform workers generally focuses on app drivers and delivery workers and overlooks "a whole universe of microworkers, who train Artificial Intelligence (AI) applications by performing data annotation, image classification, and audio transcription." Likewise, discussions on content moderation in PL 2,630 (BRASIL, 2020) do not address the activities of content moderators *per se*. Broadly, DiraCom considers essential:

> *To establish measures to guarantee labor rights on digital platforms, both when **workers are engaged by platforms** (who today are usually outsourced and subject to precarious work) and in processes of **engaging workers for the provision of services** (such as transportation and delivery platforms) and of **purchase and sale of labor power mediated by platforms** (the so-called freelance platforms) [our emphasis].*

Some inputs stressed that the regulation should consider gender bias. As CEPI/FGV pointed out, a study by the International Labor Organization (ILO) identified that "many women are attracted to crowdworking[57] due to time flexibility, which allows them to reconcile work with home tasks, such as raising children."

The CEPI/FGV research also pointed out that, despite the diversity of platform business models, some practices are more common, such as "classifying the workers as **self-employed**; calculating **task-based rates and not negotiated** with the workers; and non-negotiation of service provision conditions, among others" [*our emphasis*].

Alex Camacho, from the technical and scientific community, mentioned that some digital platform practices, such as low wages, lack of social protection, unstable contracts, and lack of labor rights, establish an asymmetric relationship that may lead to abusive practices by exploiting workers' vulnerability and compromising their labor rights. Gustavo Paiva, from the business sector, stated that precarious work is not a mere side effect of digital platform operations because significantly reducing labor costs on a large scale and dismantling previous labor structures reduces competition and is an essential part of their strategy.

Filipe Saraiva (UFPA), Gustavo Paiva (business sector), and Slowphone agreed with the risks described in the consultation as "associated with precarious working conditions – involving payment terms, contracts, labor rights, and work management, as

[57] Crowdworking is understood as a "form of work performed remotely on digital platforms, and it is commonly used by companies whose business model is linked to the Internet and which demand access to a global pool of workers intermittently and sporadically" (KALIL, 2019 apud CAMELO et al., 2021a).

well as the risks arising from the activities performed due to the asymmetrical relationship between workers and digital platforms."

4.1.1 MITIGATION MEASURES

4.1.1.1 TRANSPARENCY

According to some inputs, because labor relations on digital platforms are mediated by data and algorithms, transparency rules need to be adopted to mitigate precarious work. Instituto Vero stated that "such rules should consider the use of personal data under the terms of the Brazilian General Data Protection Law (LGPD), and provide higher **algorithmic transparency**, allowing workers to **understand better the activity they perform**, thereby, be able to make better work decisions" [*our emphasis*]. It added that rules relative to vulnerable groups, such as children and adolescents, must be explicit and communicated to the workers:

> *Other risks that should be considered are related to the transparency of digital platforms and misuse of personal data. Firstly, the lack of algorithmic transparency of the applications that connect workers with service providers creates* ***an unstable and unpredictable work environment for workers who do not understand how intermediation is carried out****. This causes a significant asymmetry between technology and workers, leading to precarious work and threatening decent work [our emphasis].*

CEPI/FGV emphasized some issues to be considered in the gig economy context[58]:

- ***Access to the platform's terms of use and services****, their availability to users, and conditions for their access, such as the requirement to register and provide personal data;*
- ***Access to communication mechanisms and channels to request information and clarifications****, period of time*

[58] Gig economy can be understood as "work on demand through digital platforms/applications" (CAMELO et al., 2021a).

workers are available (for example, during the period of time workers are using the platform), and the existence or not of human support;

- *The **language** of the terms of use and of the platform's interface is sometimes not clear, understandable, and available in Portuguese; and*
- ***Training workers on using and operating the applications** [our emphasis].*

Within the scope of corporate social responsibility and the right to information/transparency, CEPI/FGV suggested some actions to ensure social well-being:

- ***Disclosure of general platform figures**: number of workers, number of services provided/mediated, average duration of the work performed by workers, average wage, number of accidents during the provision of the service, number of insurance policies and coverage for hired workers, etc.; and*
- ***Disclosure of social responsibility** (corporate, business, and environmental) **practices** adopted by the company [author's emphasis].*

CEPI/FGV also mentioned the possible establishment of information rights on the algorithmic system used to manage work in delivery apps, such as in Spain.

Finally, José Antonio Galhardo, from the government sector, argued that transparency regarding the quantification and classification of cross-border or foreign-based labor is essential to prevent companies from applying strategies to evade regulations. According to Galhardo, the regulation should require transparency regarding platforms' registration criteria and algorithmic demand distribution to ensure workers' equality. Slowphone, Alex Camacho, and DiraCom defended the adoption of transparency measures.

4.1.1.2 MINIMUM WAGES AND WORKING CONDITIONS

Filipe Saraiva (UFPA) and Leonardo Cruz (UFPA) agreed with the transparency measure, stating that, considering precarious

work examples, regulation is essential to hold companies liable for labor relations and wages and to improve working conditions. Like DiraCom, Saraiva and Cruz stressed particularly the so-called task-rate wage, one of the forms of labor precarity and exploitation.

According to CEPI/FGV, hundreds of bills address issues related to working conditions, "in particular, provision of meals, rest breaks, scheduling working hours, provision of Personal Protective Equipment (PPE), provision of support desks and channels, access to information, minimum health and safety conditions, etc." The bills also propose establishing a minimum wage, usually per hour. However, as CEPI/FGV explained, its implementation faces some challenges, such as "working on multiple platforms and determining engaged time (the entire active login period, only the time spent performing the task, or other criteria)."

Interedes from the business sector opposed such measures, arguing that payment rules should be stated in the contract to be signed between the parties and be observed, granting freedom of contracting and negotiation.

4.1.1.3 PROMOTE (VIA TAXATION, INVESTMENT, EDUCATION, RECRUITMENT, ETC.) DIGITAL PLATFORMS THAT PROVIDE FAIRER WORKING CONDITIONS

CEPI/FGV considered relevant measures to encourage fair working conditions to prevent platforms from taking advantage of precarious working conditions to adopt unfair competition practices or cause market imbalances. Such measures include offering training to workers and adopting hiring policies that consider diversity indicators and their specific demands. Furthermore, it stressed the need to adopt control instruments to assess the companies' policy consistency to prevent them from adopting unequal remuneration standards and working conditions for different countries[59].

[59] According to CEPI/FGV, "Uber is an emblematic case. In compliance with the ruling of the UK Supreme Court, Uber started to offer local workers minimum hourly wages, paid vacations, social security contributions, and other rights and benefits; however, such measures were not extended to other jurisdictions."

DiraCom, in line with its inputs on innovation (item 2.3 of Axis 2), asserted that "taxation policies should favor worker cooperatives in order to stimulate diversification in the universe of platforms and digital appropriation by the public." Likewise, MTST's Technology Center supported "creating mechanisms that prioritize worker-owned platforms in public procurement."

According to José Antonio Galhardo, from the government sector, the proposals should not focus on incentives from a traditional perspective of labor protection but on measures that ensure transparency and worker equality and added that taxation should be considered a parafiscal policy.

Rosa Vicari (UFRGS) argued that platforms should be taxed according to the number of workers they dismiss, considering that a significant part of human work has been replaced by technology.

4.1.1.4 ENCOURAGING DECENT WORK CERTIFICATIONS

CEPI/FGV stressed the need to establish mechanisms and metrics for comparing and discussing platform performance, referring to Fairwork and Instituto Ethos initiatives, which, however, are not certifiers.

According to Rosa Vicari (UFRGS), the next critical debate on the changes generated by technologies in education will be about certification at all levels.

4.1.1.5 PROMOTING PLATFORM WORKERS' DIGITAL LITERACY AND DATA PRIVACY EDUCATION

CEPI/FGV suggested expanding the digital literacy and privacy education programs offered by some platforms and developing public education and digital literacy policies. DiraCom, from a broader perspective, proposed developing policies to "promote digital appropriation and sovereignty, encourage the development of new applications by workers, and recognize the demand for rights by workers and their representative entities."

4.1.1.6 OTHER MEASURES TO MITIGATE PRECARIOUS WORK

Recognizing labor relations, which is related to all other mitigation measures, was also emphasized. For instance,

DiraCom and Mothers of Resistance[60] mentioned the need to recognize labor relations workers by delivery and transport platforms, among others.

Worker representation and communication of/with the worker were also mentioned. Pedro Pinheiro, from the government sector, advocated for workers' participation in platform decisions. The MTST's Technology Center argues that "the participation of worker representatives in digital platform technology development councils should be ensured." Considering the difficulties of collective organization and representation, Alex Camacho suggested promoting the creation of specific associations or unions for digital platform workers, providing them with mechanisms for representation and collective bargaining" as a mitigation measure.

Relative to communication, Tarcízio Silva (Mozilla Foundation) argued that "worker service, negotiation, and information channels should be established" in addition to providing human-to-human communication channels for users. The reason is that:

> *[...]* ***using chatbots or other automated means to assist*** *workers, customers, and users who are facing problems or seeking information is cruel and* ***generates additional workload and time****, as well as moral damages when rights, information, or troubleshooting are demanded [our emphasis].*

CEPI/FGV mentioned the need to establish data portability and mechanisms that encourage cooperation among platforms, which is essential for controlling working hours limits, given that workers may be simultaneously connected to several platforms – [multiplatform work]. That measure would also simplify the payment of compulsory social security contributions and social benefits shared by companies.

Regarding social security contributions, CEPI/FGV pointed out that:

> *[...] although it is mandatory that gig workers, even when self-employed, be insured under the [Brazilian] General*

[60] Mães da Resistência.

> *Social Security Regime (RGPS), there seems to be a mismatch between what is set out in the legislation (what should be) and reality [...] Therefore, platforms could facilitate, and, to a certain extent, even monitor contribution payments, regardless of the work regime to be defined by legislators. In a data portability context, it would allow the establishment of a system to record and calculate the proportional distribution among multiple actors.*

Alex Camacho considered that, to mitigate the lack of access to social benefits, the regulation should establish "minimum social protection requirements for platform workers, ensuring that their access to adequate benefits and the responsibility of platforms for providing them."

Camacho also proposed mitigating the risks associated with the **lack of workplace safety** by establishing "occupational health and safety requirements for activities performed on platforms, including the provision of protective equipment and clear guidelines to ensure a safe working environment." Mothers of Resistance said that platforms should offer "medical, dental, psychological, and psychiatric treatment" in addition to "work tools such as cell phones, computers, vehicles, energy, and Internet connection." Regarding workplace health and safety risks, CEPI/FGV stated that "the Covid-19 pandemic intensified this debate, particularly concerning the delivery and transportation categories. There are demands regarding the supply and use of PPE, social benefits, working conditions, etc."

4.1.2 TEACHERS AND COMMUNICATION PROFESSIONALS WORKING ON DIGITAL PLATFORMS: RISKS AND MEASURES

Among the sectors affected by platformization, participants mentioned education, which was not previously mapped in the consultation. Researchers of the Praxis Community[61] listed the following risks related to teaching working conditions: "disregard the complexity of the teacher's role; disrespect for teachers' copyrights; job elimination; and excessive regulation precluding oversight and hindering creativity."

[61] Comunidade Práxis.

The researcher proposed the following measures to mitigate the precarity of teachers' work:

- *Complying with the legislation governing teachers' employment relations;*
- *Complying with the current legislation on copyrights, acknowledging teachers' content production and its association with the teacher's work;*
- *Adopting authentication technologies to ensure copyrights;*
- *Levying taxes on automated work to generate a universal basic income, as automated work may lead to job losses.*

Rosa Vicari (UFRGS) highlighted the need to revisit work relations in education, considering that teachers are responsible for more students in online contexts, and their wages are not increased accordingly.

Finally, Narratives Network[62] mentioned changes in the work of communication professionals brought about by digital platforms. It noted that professionals must adapt their designs to comply with the platforms' trends and content production rules, including incomplete information, tight deadlines, and content that incites hate due to engagement dependence.

4.2 RISKS ASSOCIATED WITH THE EMERGENCE OF NEW NOT RECOGNIZED OR REGULATED FORMS OF WORK AND THEIR MITIGATION MEASURES

As Alex Camacho (technical and scientific community) explained, expanding digital platforms has produced new work forms that are often not socially recognized or regulated and may lead to a lack of social protection and labor rights. In general, CEPI/FGV suggested the implementation of:

> *[...] mechanisms for social dialogue and promotion of dialogue between the judiciary, legislature, civil society, and the digital work platform ecosystem (as well as between*

[62] Rede Narrativas.

ordinary courts and labor courts to solve jurisdictional disputes and issues regarding new forms of work).

Mitigation measure proposals for the risks associated with each new form of work are presented below.

4.2.1 PAYMENT FOR ATTENTION AND DATA

Black Women Bloggers argued that using and remaining on digital platforms should also be considered work since they contribute to platforms' profits by generating or sharing their data or consuming advertisements. Therefore, users need to be informed about those processes and duly remunerated. According to Victor Lippi Zaccariotto, from the scientific and technical community, social media are fed by the community that uses them and, therefore, should provide monetization mechanisms to users.

4.2.2. CHILD LABOR ON DIGITAL PLATFORMS

Instituto Alana mentions a new form of child labor, the **child digital influencers**, who are "children and adolescents who expose themselves on the Internet, **regularly creating social media content aiming to make a profit**" [*our emphasis*]. According to the institute, the artistic and labor nature of these activities on digital mass communication media is unequivocal, according to Act 6,533 (BRASIL, 1978)[63]. Moreover, such "activities are characterized by regularity, monetization, professionalization, and orientation towards external expectations, which may damage children's school routine and leisure time." However, it pointed out that digital child labor is still poorly understood.

The institute also proposed some measures to protect the rights of children and adolescents in that context:

[It] is essential that companies that profit from this new form of work – whether they are advertising companies that

[63] Act 6,533 (BRASIL, 1978) defines artists as "professionals who create, interpret, or perform cultural works of any nature for the purpose of public exhibition or dissemination through mass media or in places where public entertainment shows are held."

form partnerships with those children and adolescents, or the digital platforms on which their content is hosted – are held responsible for ensuring their labor rights and their activities comply with the current legislation.

Considering the current regulations on child performer labor in general[64], the Alana Institute proposed establishing **minimum wages and working conditions rules** for child digital influencers. Moreover, such activities can only be performed if **preceded by a judicial order**, with a statement from the Public Prosecutor's Office establishing the conditions to be monitored. Considering that such activities are an exception to the prohibition of child labor stated in the Federal Constitution (BRASIL, 1988), judicial orders are "essential for verifying the compliance of the content created by children and adolescents up to 16 years of age, and actions that constitute child advertising should not be permitted." The institute added that ensuring that judicial orders precede the work of child influencers is the responsibility of the companies that manage social media and platforms, which profit from the work of child digital influencers.

Another example mentioned by Alana Institute is Roblox, a platform on which users can play and create games and interact with each other. If, on the one hand, it teaches coding and programming to children and adolescents, on the other hand, it may be understood as based on child labor, as it encourages expectations of monetary gains.

Lastly, another relevant case mentioned is the **work of adolescents and children for delivery apps**, allowed by imprecise registration instructions and failures in the platforms' systems. According to the Alana Institute, this is one of the worst forms of child labor, given that, when working on the streets, particularly during the night, children and adolescents are exposed to considerable risks, often being victims of accidents, run-overs, and urban violence, and suffering immeasurable development losses. It added that the "profile of adolescents who are victims of this form of child labor is the same as the

[64] Current regulations include Law 6,533 (BRASIL, 1978), and ILO's Recommendation 146 (ILO, 1973b) and Convention 138 (ILO, 1973a), both ratified by Brazil, and Art. 149, II of the Brazilian Child and Adolescent Statute (BRASIL, 1990).

profile of child workers in Brazil. In other words, they are boys, between 14 and 17 years old, black, and from socioeconomically vulnerable families."

4.2.3 CONTENT MODERATION WORK

Human content moderation work sustains the moderation model at highly automated levels, consequently sustaining the business model of some of the leading Big Techs. Alana Institute argued that the precarity of this work tends to harm the quality of the information environment:

> *[...] there are countless reports of precarization of the work in this area, including low wages, lack of information on the nature of the work when hired for telemarketing advertisements, and even lack of adequate training. The well-being of those workers directly impacts the quality of moderation, and the pressure to make quick decisions impacts the quality of the information environment.*

Furthermore, according to the Alana Institute, although understanding the local context is required to perform good moderation work, today, there is no transparency about the teams that carry out these tasks, their location, or the quality criteria that guide their work. It also pointed out that platforms use other platforms to outsource tagging and data classification services, such as Amazon Turk, which is accused of allowing the circulation of child and adolescent sexual abuse and exploitation images.

Considering that this is a highly precarious sector worldwide, Carolina Christofoletti, from the scientific and technical community, proposed some mitigation measures, such as:

1. *Declaring the **invalidity of the nondisclosure clause** (NDA) that forbids content moderators from discussing their precarious working conditions;*
2. *Requiring the **provision of adequate psychological support**, including the need for counselors familiar with the content moderation environment;*
3. *Requiring **training** to prevent bullying, harassment, and other discriminatory behavior;*

> 4. *Requiring **fair wages**, providing a reasonable minimum number of days off, and restricting overtime hours due to the highly stressful environment to which content moderators are exposed [our emphasis].*

Risks related to the mental health of the workers responsible for moderating social media or training AI systems were also highlighted by José Galhardo from the government sector.

4.3 WORK DISCRIMINATION IN PLATFORMS AND OTHER RISKS

According to Tarcízio Silva (Mozilla Foundation), ranking different actors in the platform ecosystem may "intensify intersectional discrimination, generating biased working conditions, wages, and opportunities" because "platform customers, providers, and professionals are led to rank or evaluate other actors in the ecosystem" subtly or explicitly guided by intersectional discrimination. In addition to those incentivized ratings, current ranking algorithms do not isolate intersectional discriminations to the detriment of minority artists and content creators.

In this sense, Black Women Bloggers stressed that digital platforms must be headquartered in Brazil, hire predominantly Brazilians, comply with local labor laws, and respect Brazilian racial and gender diversity. Alex Camacho mentioned discrimination risks in job selection and allocation, suggesting that the regulation establishes measures to prevent discrimination on digital platforms, ensuring that workers have fair and equal access to job opportunities.

The Vero Institute indicated another related risk: data misuse for profiling and job offers, as using personal data for service distribution may aggravate biases that affect the diversity and the equitable offer of possibilities.

CEPI/FGV mentioned additional risks (including some of those previously addressed):

> *a) Risk of **worker demobilization**: workers are generally identified as self-employed and often not engaged in workers' unions or associations [...]*
>
> *c) **Professional development and career progression** challenges: need to implement training programs, retraining,*

> *and development of new skills and knowledge, focusing on workers' professional development* *[our emphasis]*

4.4 CONCLUSION ON WORK-RELATED RISKS

The group of risks related to threats to decent work received fewer inputs, which indicates the need to further discuss them within the CGI.br community and possibly in other forums. The private sector, for instance, either did not comment or stated that this was not the appropriate forum to discuss the matter.

However, some issues relevant to the regulation of digital platforms were addressed by the participants. Regarding precarious work risks, for example, transparency in processing workers' data and the opaque use of algorithms by platforms, which affects working conditions, were highlighted.

Other issues that were not previously mapped emerged, such as the need to improve platform communication channels with the workers and worker representation and overlaps between precarious work and discrimination on platforms caused by user or algorithm rankings, requiring measures to ensure equal hiring opportunities. The specificities of child labor on digital platforms, such as child influencers or teenage delivery workers, were also mentioned as relevant risks should be regulated, and compliance with the current legislation should be monitored.

Establishing adequate wages was pointed out as a challenge to be further explored, considering the flexibility provided by app structures, such as multihoming[65].

5 RISKS RELATED TO DEMOCRACY AND HUMAN RIGHTS THREATS

5.1 RISKS ASSOCIATED WITH INFODEMICS, SUCH AS DISINFORMATION, EXTREMISM, HATE SPEECH, INCITING TERRORISM, AND OTHERS

The inputs to the CGI.br consultation reaffirmed the relevance of infodemics-related risks, pointed out their harmful effects, illustrated

[65] Host or computer connection to more than one platform.

their severity, and attributed the magnitude of the phenomenon's scale to digital platform business models. The mitigation measures suggested by the participants reveal the infodemics phenomena' breadth, transversality, and multidisciplinarity.

5.1.1 HARMFUL EFFECTS OF INFODEMICS ON DEMOCRACY AND ITS ASSOCIATION WITH DIGITAL PLATFORMS

The term **infodemic** arose from the health sector, as pointed out by IAB Brasil. In 2003, during the Severe Acute Respiratory Syndrome (SARS-CoV) epidemic in the USA, the term was used to convey the notion of an information epidemic. In 2021, the term was adopted by the Brazilian Academy of Letters[66] (ABL) and incorporated into the Portuguese vocabulary, given its widespread use on the international scene to designate the deterioration of the communication environment. According to IAB Brasil, despite the term's theoretical foundation, it carries some subjectivity. Furthermore, its use is insufficient to respond to the complexity of defining the illegality of some speech types, a "common problem faced by the Judiciary, which frequently disagrees when determining if a statement should be or not" subject to removal or sanction.

IP.rec pointed out the inherent duality of the expansion of the Internet. Initial reactions to the Internet's expansion led academics worldwide to endorse its social development and communication and knowledge democratization possibilities. "While social media have democratized the access to information and amplified the voice of social minorities, problems such as misinformation, extremism, hate speech, and incitement to terrorism were also aggravated."

Several inputs highlighted the association of the advance of infodemics and their harmful effects with digital platform business models built on the "massive collection of users' personal data for targeted advertising," as stated by the Vero Institute. The inputs rely on theoretical approaches, such as surveillance capitalism and platform capitalism, to substantiate the association of the problems arising in the current communication environment

[66] Academia Brasileira de Letras.

with digital platform activities. The traditional media associations represented by ABERT, for instance, argued that "infodemic is undoubtedly a reality on digital platforms, and a fertile ground for the spread of disinformation and illicit content, such as extremist speech, hate speech, incitement to terrorism, among others."

CTS/FGV asserted that "algorithmic systems using engagement as a parameter inadvertently increase the visibility of disinformation and harmful contents, as these often provoke strong reactions, and, therefore, high engagement." It also mentioned "radicalization fueled by profiling and content microtargeting." Several participants expressed concerns over radicalization using expressions such as "bubble effect" or "information bubbles."

"Content filtering" was another concept used in the inputs. CDR argued that content moderation on digital platforms hinders effective political participation, putting the "right to communication in its various dimensions, in particular the right to information and freedom of expression, as well as its relationship with the democratic system" at risk. According to CDR,

> *[...] the reconfiguration of such phenomena within digital platforms is directly linked to business models and the logic of excessive data collection,* ***amplifying disinformation, and extreme and hate-speech content to generate engagement and keep users in these spaces longer*** *[our emphasis].*

A substantial part of the inputs characterized it as a system that favors groups willing to attack fundamental principles and rights and commit illegalities, taking advantage of digital platform business models to advance their political agendas. From the scientific and technical community, Alex Camacho noted that some social groups have based their political action on disinformation and used digital platforms to promote political destabilization by virally spreading false, misleading, violent, and other such content. IP.rec referred to the **disinformation industry** concept proposed in the CGI.br report "Internet, Disinformation and Democracy" (2020), which is "characterized by the continuous increase in the complexity and size of the production chains and user networks that have emerged stimulated by high financial investments destined for these activities." Several

inputs stressed that this system's effects are severe and related to violence in its various dimensions. Louise Karczeski, from the scientific and technical community, mentioned that one of the widely used strategies is:

> *[...]* ***hate speech****, which involves the progression, intensification, or overlapping of violations that originate from a power strategy based on aggressiveness, hostility, oppression, intolerance, and vilification of peoples or communities, and evolves, in its content and form, towards discursive extremism characterized by the dehumanization of its object and collectivization of its recipient*[67] *(BRASIL, 2023a) [our emphasis].*

Karczeski refers to the study of the researcher Adriana Dias, who identified a "270% increase in the number of extremist groups in Brazil between 2019-2021."[68]

The increase in **threats against ethnic, religious, gender, and sexual orientation minorities**, among others, and against vulnerable groups, such as black and mixed-race people, is also highlighted in several inputs. According to Gustavo Paiva, from the business sector,

> *[...] over the last few years, we have seen several minorities – native and quilombola populations, followers of African-Brazilian religions, LGBT+ people, among others –* ***becoming a pawn in the game of political radicalism allowed by large platforms****. We need to recognize that identifying minorities as "enemies" and attributing various social ills to their existence resurfaced in social media platforms [our emphasis].*

Several inputs also addressed the perception of the impact of the growth of violent speech on people's lives, illustrating it with

---

[67] Excerpt taken from the definition proposed by the Brazilian Ministry of Human Rights and Citizenship (MDH) workgroup on the report on strategies to address hate speech and extremism (BRASIL, 2023a).

[68] Adriana Dias was an anthropologist and researcher on neo-Nazi groups in Brazil deceased in 2023. She denounced more than a thousand extremist cells and was an activist in defense of Human Rights (ECOA UOL, 2023).

examples, such as violence in schools, the anti-democratic acts of January 8, 2023, and violence against black and mixed-raced people, women, and other vulnerable groups.

A single input to the consultation, submitted by Christian Abreu, had a structurally divergent view, denying that the public space for debates deteriorated due to the expansion of the use of digital platforms. According to Abreu, "[fighting] 'infodemics' – whatever that may mean – means restricting freedom of expression to silence a group of individuals who should have the right to express their ideas." It should be noted that, despite being an isolated contribution, that approach reflects a political position supported by a significant segment of Brazilian society.

5.1.2 ADDITIONAL DIMENSIONS RELATED TO INFODEMICS

Three themes associated with infodemics were addressed: digital inclusion and media regulation, which were not previously listed by the consultation, and digital platform impacts on journalism.

5.1.2.1 DIGITAL INCLUSION

Among the dimensions related to the challenges of improving the public sphere, digital inclusion was addressed from its most fundamental aspect: the lack of access to the Internet or meaningful connectivity[69] and issues related to digital platform regulation. One of the issues raised is the characteristics of the data plans/packets associated with using cell phones exclusively for Internet access. In this regard, Flávia Lefèvre highlighted the **relationship between the business model of this telecom industry segment and disinformation dissemination**:

> *[It] is unacceptable that, in Brazil,* ***access to the Internet is predominantly provided by mobile networks, which sell data plans based on subscriptions associated with the practice of zero-rating, which violates net neutrality***

[69] "Meaningful connectivity" is a term coined by the Alliance for Affordable Internet (A4AI), defined by the International Telecommunication Union (ITU) as "a level of connectivity that allows users to have a safe, satisfying, enriching and productive experience".

> ***and the right to continuous provision of Internet connection services**, […] encourages disinformation and hate speech dissemination, considering the results of surveys showing that most Brazilians obtain political information on Facebook and that network users are overwhelmed with disinformation campaigns mainly through Facebook and WhatsApp – precisely the two applications offered under the zero-rating system to more than 80 million Brazilians [our emphasis].*

Another topic mentioned by the Alana Institute is ensuring access to assistive technologies, accessible websites, and applications to allow people with disabilities to experience the benefits offered by the Internet fully. Visually impaired people, for instance, are constrained to use only digital platforms that apply accessible standards, whereas other sectors, including the government itself, still do not offer acceptable accessibility levels on their websites and applications.

Risks related to digital technology appropriation and digital literacy were also mentioned, which, according to the consultation inputs on the subject, are required to allow users to understand the data processing processes applied.

Lastly, the Alana Institute emphasized the importance of creating safe public spaces for Internet access and promoting invention, exchange, creativity, play, and studies in the digital space, increasing the opportunities to exercise the right to culture and education. That is related to a broad set of digital education mitigation measures discussed below.

5.1.2.2 MEDIA REGULATION

Some participants expressed concern about the lack of rules regulating the national media sector, mentioning the need to establish a single legal framework to replace the multiple laws currently in effect. Two central media regulation themes were addressed in the consultation.

The first concerns the lack of adequate content regulation in Brazil, establishing a more consensual ground to address, for instance, disputes related to content moderation by digital platforms. The Alana Institute mentioned that it is "difficult

to define regulatory criteria on suitable/appropriate content for children and adolescents up to 18 years old." Tarcízio Silva (Mozilla Foundation) mentioned concerns about local and national content production and digital platforms in light of the interests underlying the "relation of global digital platforms businesses with the financial capital and the economic-political goals of their home countries."

The second theme refers to regulating the funding of content production and distribution activities. Issues related to advertising and propaganda were the most cited. The almost complete lack of consensus embodied in regulations on the transfer of values paying for partial or entire content utilization by media outlets, including digital platforms; supporting public media outlets, independent national and regional media; and securing funds to support not-for-profit initiatives are additional challenges to develop a regulatory framework for digital platforms in Brazil, as pointed by Antônio José Abrantes Chaves, from the academic sector.

There is a clear dissent between the broadcasting and the Internet application provision industries. On the one hand, as Câmara.e-net argues, "the business model of digital platforms is different from that of traditional media outlets (newspapers, magazines, television)" because the latter has a "dedicated space for advertising, which transmission to the public is fully controlled by the outlet," whereas "Internet application providers operate under a different rationale, in which multiple advertisers can insert their advertising offers simultaneously for different audiences."

On the other hand, traditional media business associations stated that:

> *[...] in Brazil, the* ***platforms that mostly live off advertising revenues by selling advertising spaces and insertions to advertisers refuse to be considered advertising vehicles, which they effectively are*** *(according to Tercio Sampaio Ferraz Junior and Thiago Francisco da Silva Brito, in a legal opinion submitted in 2018 to the Executive Council of Standards [...]). That creates an asymmetrical and exceptional situation where they are simply not submitted to the same rules [our emphasis].*

5.1.2.3 RISKS RELATED TO THE NEGATIVE IMPACTS OF PLATFORM ACTIVITIES ON JOURNALISM

The challenges of journalism sustainability in the digital age and its relations with digital platforms were frequently addressed in the consultation. Although the inputs generally recognize such relations, their explanations and proposals for facing challenges differ. However, despite these differences, there is broad consensus that "**fighting the dissemination of fake news involves strengthening journalism**, an important mechanism to ensure citizens' access to information" [*our emphasis*], as emphasized by the Digital Journalism Association[70] (AJOR).

The inputs discussed the connection between infodemics growth and the "crisis in journalism," which has led to the extinction or reduced activity of Brazilian publishers and media groups, affecting citizens' access to information. AJOR pointed out, referring to News Atlas (Atlas da Notícia) data published in 2022 (PROJOR, 2022), that "more than 13% of Brazilian citizens live in regions considered as news deserts."

Many participants argued that this debate is related to the financial sustainability of journalism, considering the growing advertising revenue shift to digital platforms in recent years. Traditional media associations examined the concentration of power of applications made available by large digital platforms, mainly Google and Meta. According to those associations,

> *Websites, including news outlet pages, simply do not exist for a wide range of Internet users if search engines do not index them. The largest provider of this service has no competitor to threaten its position of dominance, which is therefore called gatekeeper or "keyholder" of a fundamental channel for distributing content published on Internet pages. In this context,* ***the relation between news outlets and digital platforms – specifically those focused on Internet page search – is set on absolutely unequal grounds*** *[our emphasis].*

[70] Associação de Jornalismo Digital.

According to entities operating in the media sector, this power asymmetry is due to the digital platforms' capacity to attract audiences, making journalism companies "hostages" to the terms they establish. In addition to controlling website search, "taking advantage of the dominance they exercise over content distribution channels on the Internet," they are encouraged to create methods to retain users on their services and applications, generating ever greater advertising revenues and reducing direct visits to news companies' websites. An example is platforms that, besides indicating links to pages of interest in their applications, display news excerpts or "snippets," further reducing visits to news companies' and journalists' websites. Such tools "economically disincentivize platforms to adequately remunerate media channels for utilizing their journalistic content."

Traditional media companies argued that if there is no refusal to negotiate, "we experience **negotiations based on opaque criteria or on the 'take it or leave it' model, in which the huge bargaining power of the platforms continues to prevail**" [*our emphasis*]. The imposed "terms and conditions are to the detriment of fair and balanced negotiations and broad and equal treatment of journalistic channels," therefore, such alleged negotiations are characterized by excessive bargaining power. They also pointed out that most of the current negotiations were enforced by the authorities due to investigations.

From a complementary perspective, CTS/FGV cautioned as to the harmful effects of this asymmetry on the type of news privileged by digital platforms:

> *[a] algorithmic recommendations often favor inflammatory content [...] that attracts clicks and shares but may distort the truth and radicalize audiences.* ***Such environments are conducive to the intensification of negative journalism practices, such as sensationalist headlines ("clickbait") and news designed to generate immediate outrage rather than reporting in an objective and balanced manner*** *[our emphasis].*

Inputs also mentioned that the impacts of advertising concentration on "alternative and community media" are even more severe and require, according to DiraCom, "policies to democratize funds and diversify content circulation means."

The main dissent observed in the inputs concerns the platforms' role in this crisis and its solutions. Nevertheless, inputs generally agreed that the "crisis in journalism" is not new and that the changes imposed by the Internet have worsened the situation. Entities representing digital platforms argued that digital platforms allow greater journalism plurality, sponsoring small initiatives that would not have space in the pre-Internet media system. In defense of the current model, Câmara.e-net points out that news outlets freely decide to "share links to their content because they benefit from the platforms' traffic" and, therefore, cannot expect remuneration given that this content is characterized as a voluntary publication. It cautioned the risk of creating "an industry of new low-quality news companies officially remunerated by the platforms."

Despite opposing the remuneration for content by digital platforms, ALAI recognized this situation is challenging and proposed:

a) convening cross-sector experts to identify focus areas and develop shared solutions;

b) investing in newsroom innovation and experimentation to identify and support sustainable business models and

c) supporting legacy institutions as they undergo digital transformation.

Finally, it was pointed out that journalism-related challenges are part of the larger context of the absence of an integrated regulatory framework for the Communications sector. For instance, traditional media associations argued that because platforms earn **advertising revenues** by selling advertising space and placement to advertisers, they should be considered **advertising channels**. Therefore, the current situation is asymmetric and exceptional, as digital platforms are not subject to the same rules.

5.1.3 MITIGATION MEASURES

Inputs on measures to mitigate risks related to infodemics expressed very different approaches in terms of scope and transversality. The proposed actions included threats to

journalism, holding platforms liable for third-party content, new liability approaches applying procedural measures and risk analysis, diversity of the content displayed to the users, digital literacy, and reporting and due process mechanisms.

5.1.3.1 MEASURES TO MITIGATE RISKS RELATED TO IMPACTS ON JOURNALISM

DiraCom proposed establishing a model for "sharing the financial resources obtained by digital platforms through monetization and advertising of journalistic content by imposing taxes and creating a fund" with the collected taxes. As proposed by Intervozes, the objective of that fund may aid in facing the sustainability challenge in journalism, promoting the "production of quality journalistic content," and funding independent journalism initiatives and innovation to support these projects.

AJOR supports establishing transparency mechanisms to aid decision-making processes related to the distribution of such funds. CTS/FGV mentioned that algorithmic transparency is critical to define criteria to "guide the distribution and visibility of journalistic content, thereby preventing the generation of information bubbles and ensuring the diversity and plurality of opinions." Moreover, DiraCom emphasized representativeness in this context, defending the inclusion of participants other than economic actors, such as news companies and application providers, ensuring participatory and multistakeholder decision-making.

The Activism and Communication Laboratory (ECO/UFRJ)[71] stressed the need to invest in the public service media and suggested:

> *[...] strengthening and updating the public service media system (Brazilian Communication Company - EBC, state TV channels, etc.) to create public communication platforms following the BBC's successful example, with funding sources other than advertising, a business model in crisis worldwide.*

[71] Laboratório de Ativismo e Comunicação da Escola de Comunicação da Universidade Federal do Rio de Janeiro.

ISOC Brasil, however, referring to recent cases of regulatory initiatives, such as the Canadian Bill for the compensation for journalistic content, warns that such regulations may jeopardize the experience of an "open, globally-connected, secure and reliable network." It argued that the Bill, "whose objective was to strengthen national producers of journalistic content by establishing new remuneration obligations," threatens the "access of Canadian citizens to global content, resulting in an imbalance of the experience of Canadian society on the Internet relative to other countries." In this sense, ISOC Brasil proposed that legislative solutions to problems related to the Internet should consider "the impacts of a national regulatory framework in terms of the fragmentation of the digital experience of Brazilian users."

Lastly, InternetLab suggested approaching this matter from a broader perspective, considering "the culture and the press," including copyright issues on digital platforms as a relevant part of the current problem and its solutions. That would allow, on the one hand, fostering diversity in the production of cultural goods in Brazil by applying models other than those driven by recommendation algorithms and, on the other hand, comprehensively supporting the sustainability of journalistic activities.

5.1.3.2 MITIGATION MEASURES RELATED TO THE RESPONSIBILITIES OF DIGITAL PLATFORMS FOR MODERATING THIRD-PARTY CONTENT

Among the approaches to mitigate risks related to infodemics, those associated with the liability of intermediaries stand out. Overall, participants stated that this issue still needs to be explored further, and building consensus on it is one of the central challenges for regulating digital platforms.

Considering that most inputs did not specify which liability regime they advocate, it was decided, for reporting purposes, to systematize them around i) maintaining the current terms of the MCI (BRASIL, 2014), ii) liability for failure to moderate promoted and monetized third-party content (as a crime against the rule of law), iii) liability for failure to moderate specific categories of third-party content, and iv) liability for failure to moderate content, considering the set of efforts employed by digital platforms. It should be noted that such approaches are not excludent, as they allow combinations of the different mechanisms mentioned in the inputs.

5.1.3.2.1 FULLY MAINTAINING THE LIABILITY REGIME ESTABLISHED IN THE BRAZILIAN CIVIL RIGHTS FRAMEWORK FOR THE INTERNET (MCI)

A representative group of participants analyzed the advantages of maintaining the current regime in force in Brazil, established by the MCI (BRASIL, 2014). ISOC Brasil stated that the model "completely responds to the demands that have been presented." It maintains that it is not "a general disclaimer or creates law immunity" but "provides accountability mechanisms for third-party content detailed in Section III [...] that preserve the principles and values established through broad public debate and aligned with the critical properties of Internet structure and functions."

ISOC Brasil considered that the capacity of digital platforms to analyze the content circulating on their networks and identify possible illicit acts committed by their users is limited and highly prone to errors, considering the size of social media or search engine operations. In contrast, the Judiciary has the grounds required to analyze it. It argued that the more responsibility is attributed to digital platforms, the greater their prerogative to interfere with the content circulating in their spaces, generating a chilling effect with massive content removals and raising fundamental rights protection concerns, such as freedom of expression and access to information.

Entities representing digital platforms and Internet service providers, such as ALAI, Câmara.e-net, Brasscom, and ITI also fully supported the effectiveness of the model created by MCI (BRASIL, 2014). ITI urged the Brazilian government to "carefully consider the impact of any significant changes to Brazil's Internet governance model, as provided in the Brazilian Civil Rights Framework for the Internet (MCI)." It emphasized that the MCI is internationally recognized, establishing "flexible and proven principles [...] that transcend the technology policy issues that arise at a given time."

The principle-based approach of the MCI (BRASIL, 2014) is considered beneficial in a rapidly changing environment. According to ALAI, the MCI established "a balance between the preservation of freedom of expression and the removal of illegal content" without creating obligations that could result in excessive content monitoring and removal.

ALAI also explained that digital platforms have sought to implement "measures to bring quality information to the surface in their services, such as contextual information about content disseminated by third parties, content created by fact-checkers, and news content." One of the examples mentioned by ALAI is the creation of the Global Internet Forum to Counter Terrorism (GIFCT) by Facebook, Microsoft, Twitter, and YouTube, which seeks to "establish technical collaboration between companies, advance research on the subject, and share information with smaller platforms."

5.1.3.2.2 LIABILITY FOR FAILURES TO MODERATE MONETIZED AND PROMOTED THIRD-PARTY CONTENT

Traditional media company associations advocated holding digital platforms liable for promoted and monetized content and proposed the following systematization of the different current positions:

> *The discussion on the civil liability of Internet application providers for content generated by third parties currently follows three main approaches: i) the non-liability of the provider for user conduct; ii) objective civil liability of the provider, based on the concept of activity risk or service provisioning failure; and iii) subjective civil liability, which is subdivided into two streams: iii.a) subjective civil liability due to inaction after detecting illegal content, and iii.b) that which defends liability only in the event of non-compliance with a specific court order.*

Traditional media associations argued that the mechanisms adopted in the current legal system based on the MCI (BRASIL, 2014) encourage the inaction of digital platforms in the face of illegal content published and disseminated by third parties. In this regard, they propose "reformulating of the 'general regime,' so to speak, of civil liability in force for content generated by third parties" as a strategy for a possible regulatory framework.

The media associations claimed that Art. 19 of the MCI (BRASIL, 2014) changed the current case law by establishing "the regime of subjective civil liability due to non-compliance with a court order." Before the MCI, the Judiciary understood

that "application providers were liable for damage resulting from content generated by third parties from the moment they are notified, regardless of a court order." At that time, platforms were prevented from carrying out prior monitoring of content; however, the associations explained that the platforms widely carried out this prior monitoring:

> *[...] to enforce their terms of use and prevent copyright violations, as well as* ***to operate their boosting and recommendation systems****, favoring some contents over others – which, not coincidentally, are related to violence, crime, fake news, and extremism because they generate the highest engagement and, accordingly, profits for the large platforms [our emphasis].*

Traditional media associations pointed out that, given the characteristics of Internet applications, the harmful effects on users become severe in seconds, "surpassing geographical and temporal barriers" and causing irreversible or hard-to-repair damages. They highlighted that the MCI instrument allows platforms "not only to fail to act when contents related to violence, crime, fake news, and extremism are posted on their networks, but also to act freely to encourage the dissemination of such content, solely and exclusively focusing on increasing their profits." The entities understand that Art. 19 of the MCI "distorts the objective of Art. 5 [of the Federal Constitution], which guarantees the victim the right – and not a duty – of access to justice" and, therefore, needs to be corrected. They added that both the EU Digital Services Act and the Alternate Bill presented by rapporteur Orlando Silva to the "Fake News Bill" (Bill 2,630) (BRASIL, 2020) include the "duty of care" (or similar terms) concept in their structure.

Based on the premise that relations within the scope of digital platforms (including information flow organization, algorithms, and network architecture) are under the protection of the CDC (Consumer Protection Code) (BRASIL, 1990b), Idec asserted that platforms are liable for boosted and monetized content posted by third parties. The rationale is that considering user-consumer vulnerability and quality and security aspects, **digital platforms should be governed by objective and joint liability**. According to Idec,

> *In lawsuits affecting consumer rights, the platform's participation in the consumption chain is presumed as it is directly or indirectly remunerated to promote or advertise specific contents and, therefore, should be subject to objective and joint liability i) for failure in the provision of the service and ii) for violation of other consumer rights (sole paragraph, Art. 7 of the CDC and Art. 14 CDC).*

Idec also stressed the need to balance the definition of content moderation actions by the platforms, with the aim of, on the one hand, avoiding "generating disproportionate and incorrect interventions, which poses risks of [...] expanding the power of private agents over which contents circulate and reach the public" and, on the other hand, protecting rights, such as freedom of expression and access to information. It emphasizes, however, that "fighting harmful practices [...] cannot justify the adoption of surveillance mechanisms."

CTS/FGV considered that the notion of joint liability for content promoted and monetized by business entities that operate digital platforms is pertinent because:

> *[...] the role played by those entities* ***goes beyond simple intermediation*** *when they cease to be only a passive channel between content producers and end consumers and assume a content amplification role. In other words, such platforms act as agents that strive to connect consumers with the content proactively [our emphasis].*

ITS, however, expressed strong reservations about the possibility of holding platforms liable for monetized content, arguing that discussions still need to mature before any measures are implemented. It referred to US Supreme Court cases related to liability for algorithm-recommended content. In one of them, the Court did not address the merits of the constitutionality of Section 230, given the lack of a causal link between the alleged damage (death of relatives due to terrorist attacks by the Islamic State in Europe) and the **action** of the platforms (Islamic State content recommendations, such as videos on YouTube). ITS added that there are reasonable arguments about the technical impossibility of distinguishing promoted from recommended content in the content moderation ecosystem.

5.1.3.2.3 LIABILITY FOR FAILURE TO MODERATE SPECIFIC THIRD-PARTY CONTENT CATEGORIES

Some organizations supported establishing a specific regime for digital platforms based on the description of illegal content to be removed by these companies.

Abranet, although supporting the current liability regime established in Art. 19 of the MCI (BRASIL, 2014), argued for the need for:

> *[...] updating the definition of which legal assets should be more emphatically protected" and suggested that a future regulatory initiative should "provide for reforms in the list of exceptions of the MCI in order to address the main concerns raised by lawmakers and democratically confirmed by the population."*

Traditional media associations proposed a special liability regime for content categories and specific actors: i) social media providers, ii) instant messaging service providers, and iii) search engines "due to the risks associated with the nature of their activities." Those associations, mentioning cases inspired in the latest version of Bill 2,630 (BRASIL, 2020), including threats against the Democratic Rule of Law, incitement to suicide, racial hate crimes, and threats against children and adolescents, argued that:

> *[...] the regime should be based* ***on civil liability independent of notification due to the duty of care to be imposed on digital platforms****, requiring proactive and diligent action to prevent, mitigate the dissemination, and remove content generated by third parties [our emphasis].*

The media associations added that the current exception of the MCI (BRASIL, 2014) for the "exclusion of content characterized as revenge pornography or child pornography, under the terms of Art. 21, is a good example of how the bill could address content associated with disinformation and hate speech", taking as an example German legislation, which, as they indicated, makes it illegal to share content classified in the German Criminal Code, such as those referring to the distribution of child pornography, the preparation or encouragement of violent crimes, incitement to hatred and the falsification of data.

Members of different sectors also discussed possible changes to the liability regime of the Brazilian Civil Rights Framework for the Internet (MCI). From the private sector, ALAI expressed concerns about the joint liability model based on simple notice to establish a platform's liability: "Several studies demonstrate that notice and removal models may result in excessive removals by intermediaries to avoid punishment and liability risks."

The Vero Institute, from the third sector, considered that the removal mechanism by simple notice is a disproportionate solution, as it imposes risks to the exercise of fundamental rights, which are broader than the possible benefits. It argued that economic incentives might lead to excessive content removal and that institutions or organized groups financially capable of and interested in "banning information from the Web while simultaneously limiting the moderation power of the platforms themselves" may benefit from mandatory content removal by prior notice.

CEPI/FGV agreed with this position and emphasized that, due to the high volume of information shared daily on large digital platforms, digital platforms are not expected to conduct a detailed analysis of the reported content, given the possibility of liability by prior notice. That would encourage platforms to remove any reported content immediately to protect themselves from future liability, even if it does not fit into pre-defined categories/types. As an alternative to the current model, it proposed adopting notice and action mechanisms that require platforms to act when notified (a duty of care element), without direct risk of liability for specific third-party content." This approach will be discussed in the next item.

5.1.3.2.4 LIABILITY FOR CONTENT MODERATION FAILURE, CONSIDERING THE SET OF EFFORTS MADE BY DIGITAL PLATFORMS

One set of inputs favored assigning broader responsibilities and duties to digital platform activities related to content moderation, including the duty of care[72] and duties considering systemic risks and platform moderation and organization

[72] Despite focusing on content categories, they involve a more systemic assessment of platform actions.

processes more comprehensively. CDR argued that vague and imprecise obligations may force "platforms to unduly exercise a jurisdictional function to determine whether contents are illegal." It highlighted that "**obligations to assess and mitigate systemic risks provide a more beneficial and safer path to protect users' rights**, as they seek to correct structural issues and mitigate potential service risks not limited to specific content matters" [*our emphasis*].

The Alana Institute, in line with CDR, argued that digital platforms "should be held responsible for publishing third-party contents that infringe children's and adolescents' rights when demonstrated they did not exercise their duty of care." It asserted that the MCI provisions (BRASIL, 2014) should be interpreted according to the Federal Constitution (BRASIL, 1988), the Consumer Protection Code (BRASIL, 1990b), and the Statute of the Child and Adolescent (BRASIL, 1990a). Therefore, digital platforms must exercise a "**general duty of care towards children and adolescents**" [*our emphasis*], making them liable when not taking the necessary measures to prevent harmful content from reaching these audiences.

IP.rec cited the example of the Online Safety Act (OSA) (AUSTRALIA, 2021), which establishes the duty of care as one of its fundamental principles. OSA includes the mechanism called "Basic Online Safety Expectations (BOSE)," comprising a "set of guidelines established to promote greater transparency and proactivity by online service providers."

In Brazil, the most recent versions of Bill 2,630 (BRASIL, 2020) integrate the notion of duty of care and obligations into their framework to analyze and mitigate systemic risks. According to Electronic Frontier Foundation (EFF), before the introduction of the duty of care in the Bill, the approach adopted was more focused on processes than on the control of specific contents. Its text now includes a list of illicit practices linked to illegal content, requiring Internet applications to "diligently act to prevent and mitigate [...], striving to fight the dissemination of illegal content

generated by third parties more effectively"[73]. That organization discussed the scope and lack of normative precision of that mechanism, as well as its effect of reinforcing the platforms' position control over online expression, analyzing that:

> *Such provision concerns the duty of care obligations that, despite not being defined in the bill, operationalize their application. The list of illegal practices in Article 11 refers to provisions of six different laws that cover around 40 criminal offenses – each containing a set of elements that must be present for a conduct to be considered illegal. Some violations also have grounds that exclude specific conduct from being the basis of a crime. [...]* ***In some cases, it is difficult to understand what exactly the application provider must monitor or whether it should be monitored at all*** *despite being on the list of criminal offenses in Article 11 [...] The duty of care obligations established in Bill 2,630 are based on a regulatory approach that reinforces [the role of] digital platforms as control points over people's online expression and actions [our emphasis].*

[73] It should be noted that EFF criticized the Bill 2,630 (BRASIL, 2020) proposal to establish immunity for the speech of public authorities. Several organizations have criticized this mechanism. According to the EFF, "Considering the current debate on Bill 2,630, it is worth mentioning that Article 33, paragraph 6, of the Bill, extends the immunity ensured by the Brazilian Constitution to parliamentarians for their opinions, statements, and votes during their term in office by including contents published by 'political agents' on social media and private messaging platforms. The term 'political agents' in the article [seems] to encompass all elected Executive and Legislative authorities at the federal, state, and municipal levels, as well as state ministers, heads of state and municipal agencies, and heads of government entities in general. If the provision is approved, this large body of authorities would be immune from civil and criminal liability for the content they publish online. The Bill provides special protections for the speech of public officials, while the standards of freedom of expression of the declaration of the [Inter-American Commission on Human Rights] recognize that such officials, on the contrary, have special obligations for their statements. Such obligations include the duty to ensure that their statements do not constitute arbitrary interference - direct or indirect - with the rights of those who contribute to the public discourse through the expression and distribution of their thoughts; the duty to ensure that their statements do not constitute Human Rights violations, and the duty to reasonably verify the facts on which their statements are based. [...] The current Brazilian regulatory debate is based on similar concerns and cannot ignore prominent public authorities' role in creating, financing, and disseminating harmful online content. Such provisions contradict the objectives of tackling the infodemic problem and should be discontinued."

Flávia Lefèvre pointed out the risk of granting even greater content and account moderation power to digital platforms, giving them greater control over information flow, which could increase the risks of "serious compromise of the guarantees of freedom of expression and the powers of the Judiciary to maintain the Democratic Rule of Law." Although recognizing the importance of respecting the principle of non-imputability of the network under the terms of Art. 19 of the MCI (BRASIL, 2014), Lefèvre asserted that it is necessary to recognize the principle set forth in this law: "accountability of agents according to their activities, under the terms of the law," arguing that there is a set of laws that establishes, in cases of damages caused by one's acts, hypotheses different from those expressed in this article for platforms. Lefèvre explained that product and service quality is based on the binomial models of quality-adequacy and quality-safety according to reasonable expectations, which not only involve safety regarding the physical integrity of users but also respect for their dignity, health, safety, and transparency in consumer relations, among others. Although Lefèvre did not mention – as did Idec – the need to define an objective and joint liability regime, she recognized that a specific discipline aimed at establishing security obligations, in accordance with the CDC (1990b), is required, as well as a liability regime harmonized with the legislation in force in Brazil, but that considers the risk of a disproportionate increase in the power of platforms over content moderation.

Regardless of the decisions on the liability regime of digital platforms, ITS discussed the possible development of "a code of conduct to be followed by all platforms covered in this scope" and questioned the effectiveness of such measure, arguing that:

> *[...] it may lead to an* ***undesirable standardization of content moderation rules across different platforms, with consequent innovation and diversity losses*** *in the digital space. Experts, such as Tarleton Gillespie and Evelyn Douek, say that content moderation is the commodity that platforms offer, ensuring a vibrant and plural Internet. The proposal for a "code of conduct" should, therefore, be viewed with caution and redesigned to prevent a standardization effect on content moderation [our emphasis].*

In addition to defining the scope of digital platforms' responsibility, other actions were mentioned, such as partnerships between fact-checkers and platforms, encouraging international cooperation among countries and organizations, investing in automatic detection and removal technologies, and encouraging platforms to share best practices.

5.1.3.3 CRITERIA AND MECHANISMS TO INCREASE USER EXPOSURE TO DIVERSITY

The mitigation measures proposed in this axis are based on two interrelated premises. The first refers to the development of mechanisms that allow digital platform users to establish content curation criteria. The second refers to the guidelines to be followed to create algorithms.

The Vero Institute mentioned the "possibility of the mandatory disclosure of content curation" to create different approaches to display posts, providing users the "power to define, in an active and informed manner, how the platform will deliver content curation."

It suggested the development of "feedback mechanisms for generative Artificial Intelligence (AI) training," arguing that the "critical evaluation of content generated by inserting prompts into generative AI tools may be an important educational strategy for children and adolescents." The Vero Institute, however, cautioned that feedback models may be influenced by biases introduced "by information manipulation chains." Nevertheless, it stated that the strategy may contribute to "the research of external sources and understanding value judgments in the content generated" by AI.

CTS/FGV suggested "options like 'Show me another view' to be included in the algorithm recommendation possibilities, displaying "other political/philosophical/religious opinions, if the user wishes." However, other inputs, such as that of IP.rec, considered that choosing one content involves suppressing other contents, which may generate biases, and argued that the definition of the divergent positions of content is open to interpretation, which may harm users.

Finally, Tarcízio Silva (Mozilla Foundation) recommended "mandatory feed options with no algorithmic curation, displayed only by publishing order."

5.1.3.4 DIGITAL EDUCATION

Several participants considered digital education (or digital literacy) essential[74]. Some asserted that digital education is critical to improving the environment of digital platforms. Others considered that it should be addressed as a challenge for society as a whole.

According to the inputs, digital education responsibilities should be attributed to a broader set of actors in addition to the State, such as schools, families, companies, and, specifically, the digital platforms themselves. The Alana Institute, for instance, supported several inputs that attributed to the State responsibilities related to the risks of digital platform activities for children and adolescents and asserted that the State should offer support and guidance to parents and caregivers in order to "maintain an adequate balance between the protection of children and their emerging autonomy" while using digital platforms and the Internet, through "mutual empathy and respect, rather than prohibition and control." It mentioned that the State should ensure "information and training opportunities for children on how to exercise this right effectively, and, in particular, how to create and safely share digital content, respecting the rights and dignity of others and not violating the law."

Schools are considered vital to face the challenge of digital education. The Alana Institute stated, "It is not a matter of discussing if technology should be used in schools, but rather, 'how' it is used." It proposed four complementary dimensions to be considered when developing digital education public policies: i) resources and infrastructure; ii) people: professionals and training; iii) security of personal data in education; and iv) national strategy.

Praxis Community, from the third sector, stressed that digital platform regulation should "be hand in hand with a broader project to incorporate regular discussions on this subject in schools" and associated digital education with digital sovereignty and citizenship. Relative to infrastructure, it considered it is the State's responsibility to "equitably invest in technological

[74] In Portuguese, three different terms, each with its own theoretical framework, are used to translate literacy: letramento, literacia, alfabetização.

infrastructure in schools and other learning environments, ensuring the availability of and accessibility to a sufficient number of computers, high-quality and high-speed broadband, and stable energy supply."

Another frequently mentioned topic was the production and dissemination of good quality digital educational resources that can be understood by children and adolescents, ensuring that the "existing inequalities are not reinforced." Albeit pointing out the benefits of Internet expansion, the Alana Institute maintained that the State must ensure "that the use of digital technologies does not weaken face-to-face education and is justified for educational purposes." It proposed "implementing digital literacy lessons from preschool level and throughout all school years."

Inputs indicated the need to develop specific skills, such as the ability to "identify and evaluate disinformation, extremism, and hate speech" associated with "critical skills to discern reliable information, verify sources, understand manipulation strategies, and evaluate content credibility," as suggested by Alex Camacho. The Alana Institute also mentioned "knowledge and skills to safely use a wide range of digital tools and resources, including those related to content, creation, collaboration, participation, socialization, and civic engagement," paying heed to the "adverse consequences of exposure to risks related to content, contact, conduct, and contract, including cyber aggression, trafficking, sexual exploitation and abuse, and other forms of violence."

5.1.3.5 REPORTING MECHANISMS AND DUE PROCESS FOR CONTENT MODERATION

Some mitigation measures suggested for fighting infodemics are improving the existing reporting mechanisms and ensuring due process to digital platform users whose posts were moderated, blocked, or deleted. Some inputs mentioned issues related to the communication of the existing mechanisms, their lack of effectiveness, and suggestions for measures that are not implemented. IRIS highlights that specific rules for defining due process measures "combined with the development of mechanisms to allow quick and concrete responses by the companies" are essential. It mentions that content moderation should provide mechanisms to inform users about:

A. The justification for the decision taken, distinguishing between legitimate political assessments, dangerous acts, and illegal acts, and specifying the violations that occurred;

B. The deadline to challenge the decision and the means to do so, as well as the deadline for reassessment by the platform;

C. Whether the decision was automated or not;

D. Whether the decision was automated, the specific penalty applied to the content, its definitive or temporary nature, and the suspension period.

Appeal mechanisms have also raised concerns. CDR highlighted that automated decisions need to be supported by more diligent action by platforms, such as "establishing specific reporting channels for these decisions" and adopting transparency measures, such as "regular reports with the parameters and policies applicable to content moderation, measures taken on posts (including their reach) and their motivations, reports received and responses adopted," to name a few examples. IRIS highlights the need to ensure a "human review and referral to a team that is familiar with the local political scenario, impartial, and speaks the local language" when algorithms take action.

5.2 RISKS ASSOCIATED WITH THREATS TO ELECTORAL PROCESSES AND INHIBITION OF MECHANISMS OF POLITICAL PARTICIPATION AND CIVIC ENGAGEMENT

The inputs to the consultation indicate a broad agreement on the relevance of digital platforms for the public debate. Some inputs mentioned the strong influence of the spaces made available by social media on the sphere of public debates, which poses risks of "public discourse domination," according to Narratives Network. DiraCom stated that such spaces "have gained enormous power and influence over the electoral processes because an increasing number of voters rely on information and form their opinions based on" applications made available by digital platforms, which have become central to the circulation of information. It mentioned the "growing privatization

of the public debate, particularly when various platforms build models that economically condition visibility," consequently reproducing "exclusionary public discussion models, favoring those who hold greater economic power."

Praxis Community added that such spaces provide a privileged channel that allows digital platforms to build strategies that contribute to advancing their interests. It cited the example of Google, which invested in advertising against Bill 2,630 (BRASIL, 2020), which is "currently being investigated by the Public Prosecutor's Office."

Idec referred to election cases that have been studied to understand the role of digital platforms in defining winning candidates or projects. According to that consumer protection entity, Brazil's 2018 and 2022 elections demonstrated "how digital platforms are used to spread fake or decontextualized news." IP.rec mentioned Donald Trump's election in the USA and the case of Brexit, "in which news against the migration of foreigners to UK territories was widely disseminated and shared with specific user types (based on personality classification and profile analysis)."

CDR stated that digital platforms are channels for disseminating "electoral disinformation and continue to use tools to monetize their content, promote it, or even deliver it applying algorithmic prioritization and recommendations on social media, such as YouTube." In this regard, the inputs generally agree that the risks associated with electoral and democratic processes "need to be specifically addressed in digital platform regulation," as highlighted by Vero Institute.

Several inputs mentioned the risks of harassment, which practice aims to inhibit individuals and organizations from acting and expressing their opinions, and of violence against vulnerable populations. Tarcízio Silva (Mozilla Foundation) defended creating mechanisms to protect "minority populations to prevent them from being targets of restriction on their free thought and expression on digital platforms." Silva pointed out the negative externality of algorithms, which restricts the space for expression of minorities, including "when they defend their rights to life and citizenship in the fight against racism, sexism, and LGBTIphobia, for instance."

Traditional media company associations highlighted that "content boosting by candidates for elective office benefits a single economic segment – the social media, which earn millions with this type of electoral propaganda on the Internet." According to them,

> *[there is an] asymmetry between social media and other media, such radio, television, and newspapers, which* ***threatens the constitutional principles of isonomy*** *(Art. 5, CRFB),* ***free competition*** *(Art. 1, IV and Art. 170, IV, CRFB),* ***freedom of expression, press, and information*** *(Art. 5, Sections IX, XIV, and 220, caput, and Art. 1, 2, and 3, CRFB) and the* ***democratic, republican and political pluralism principles*** *(Art. 1, caput, and Section V; CRFB) [our emphasis].*

EFF, from the third sector, warned about the risks of creating mitigation measures to prevent Democracy and Human Rights threats. According to the foundation,

> *[...] digital technologies have proven to be hugely transformative tools, enabling people to speak out against arbitrary acts committed by public and private powers, empowering historically vulnerable, marginalized, and silenced groups to express themselves, catalyzing civic organization and participation, and facilitating innovative ways to build and share knowledge collectively.*

To neutralize risks of "content-based regulatory abuse," EFF proposed addressing potential duty of care obligations and prioritizing systemic risk impact analysis, thereby preventing platforms from unduly monitoring and filtering their users' content. To this end, it suggested some control measures, namely:

- *Ensuring* ***robust checks, balances, and due process*** *when applying specific rules to conflict and imminent risk situations, if any.*
- *Carefully conceiving and ensuring appropriate means to establish an adequate structure for* ***independent, autonomous, participatory, and multi-stakeholder supervision*** *of the regulation under discussion.*

- *Establishing unambiguous* ***safeguards against increased surveillance and related security risks****.*
- *Abstaining from granting special protections to* ***statements made by State authorities****, who have unique responsibilities under international Human Rights standards [our emphasis].*

Câmara.e-net recommended that "measures to mitigate threats and risks associated with these issues should adopt approaches that minimize the excessive intervention on digital platforms," thereby ensuring diversity of opinions and protecting fundamental rights.

5.2.1 MITIGATION MEASURES

There was a broad consensus in the received inputs that more comprehensive obligations should be established during election periods. Many mitigation measures related to threats to electoral processes proposed in the consultation may be understood as more decisive versions of the mitigation measures to combat infodemics and other related challenges. That possibly results from the almost unanimous understanding that digital platforms play a central role in electoral dynamics and results.

5.2.1.1 MORE COMPREHENSIVE TRANSPARENCY OBLIGATIONS DURING ELECTION PERIODS

Relative to election periods and processes, transparency was the most prominent principle defended by the participants, including by entities representing digital platforms. Câmara.e-net highlighted that "transparency is essential to build trust in electoral processes"; therefore, "monitoring boosted content during the electoral campaign period" is unnecessary. The purpose is to ensure that "content boosting rules are clear and consistent, preventing it from being used to disseminate disinformation or unduly influence voters' opinions" and capable of restricting the reach of political messages boosted in a manipulative way.

In order to expedite the moderation process of such content, Felipe Saraiva (UFPA) proposed:

> *[...] implementing interoperable APIs, which the Superior Electoral Court (TSE) should require to allow sharing contents and moderation actions among different actors, such as the digital platforms themselves, third sector entities, fact-checking agencies, political parties, and others.*

5.2.1.2 BROADER CONTENT MODERATION RESPONSIBILITIES DURING ELECTION PERIODS

More stringent content moderation measures during election periods were also suggested. CDR suggested developing automation mechanisms, such as "prior content screening filters of terms related to the electoral process." The coalition considered implementing such a measure feasible, as platforms already apply "content filters to inhibit advertisements that contradict their policies."

Despite endorsing the development of specific content moderation plans during election periods, Câmara.e-net argued that content moderation is a "sensitive area, as it involves decisions about information removal or restriction, and requires contextual analysis." IAB Brasil also warned that establishing extensive obligations, even during election periods, may lead digital platforms to adopt excessively cautious approaches "resulting in the arbitrary removal or restriction of legitimate contents."

IP.rec, from the third sector, stated that the content removal provisions of the Digital Millennium Copyright Act (DMCA) "have often been used as a political censorship tool in several countries." It advised caution when establishing actions that "make the MCI model too flexible and demand more stringent action by the platforms."

5.2.1.3 LIMITING ADVERTISING EXPENSES ON DIGITAL PLATFORMS DURING ELECTION PERIODS

The topic of advertising during election periods received a substantial number of inputs.

On the one hand, entities such as IAB Brasil considered that restricting online advertising during such periods "may have negative consequences, particularly for candidates who

are not famous or known to the general public," hindering "equal opportunities in the electoral process," and, therefore, characterize an "indirect interference in the democratic debate." Furthermore, it stated that "specific regulations regarding their content, when and how they are authorized, the format they must have, and additional details, among other restrictions and guidelines," are already established.

Regarding the current system rules, Henrique Bazan explained that "Law 9,504/97 already provides for spending limits on electoral campaigns and, therefore, the measure should not be prioritized, and it is up to the candidate to choose his or her political advertising investments." According to Bazan, other measures may be more effective, such as "enhancing abuse monitoring, making it impossible for users to boost content if their previous posts have repeatedly violated platform policies," thereby making advertising on digital platforms less attractive.

CDR highlighted that "election advertising on platforms managed by Google and Meta have not undergone the due authorization process required by the Superior Electoral Court (TSE)." It argued that such content is often

> *[...] posted abroad, [and] it is up to the advertiser him/herself to declare that it is an electoral ad, which does not always happen. Despite being declared, other published contents are irregular, omitting the "electoral ad" label or the legal registry number of the entity responsible for the ad. Moreover, electoral content (involving candidate names, political parties, and election subject matters), called "political advertising" by the platforms, is promoted as not electoral, such that content paid by companies allows for evading the national legislation. A survey by Netlab of the Federal University of Rio de Janeiro (UFRJ) shows that 7 out of 10 ads on Google are irregular for the reasons mentioned above.*

Other measures are suggested by the CDR: i) encouraging partnerships between the TSE and research centers focused on monitoring advertisements and greater collaboration from digital platforms; ii) extending the "restriction period for broadcasting election ads and boosted political content" currently provided for in the TSE resolution, which prohibits "the broadcasting of election ads 48 hours before and 24 hours after voting"; iii)

suspend the "monetization, prioritization, and recommendation of channels that repeatedly disseminate disinformation narratives of an electoral nature."

Traditional media associations suggested changes to existing legislation to allow the placement of candidate ads "on websites belonging to any economic organization that produces, broadcasts, and/or publishes news directed to the Brazilian public through any printed or digital media, including television and radio (with the usual curation)," since the current advertising limitation imposed by law:

> *[...] can no longer achieve its intended purpose as it does not prevent candidates from posting messages and ads on the Internet until election day. Therefore, the fact is that the legislation imposes a [higher] regulatory burden on radio, television, and newspaper companies [...] notably considering that parties and candidates equally use the Internet and broadcasting as media during elections.*

5.2.1.4 LIMITING THE USE OF PROFILING FOR ELECTION ADVERTISING

Some inputs proposed that digital platforms should consider limiting profiling during electoral periods. Alana Institute defined profiling as a:

> *[...] technique that uses an individual's personal data to build, based on predictions and inferences typically made by artificial intelligence, a* ***profile of their personality, including tastes, preferences, opinions, trends, behaviors****, etc. [our emphasis].*

It also emphasized that profiling is responsible for "various forms of exploitation [...] in the digital environment, including economic exploitation by applying advertising micro-segmentation and behavioral advertising techniques." According to the institute, profiling may deprive users or user groups, such as children and adolescents, of fundamental rights.

Regarding profiling for election advertising, Tarcízio Silva (Mozilla Foundation) argued that the "advertising micro-segmentation enabled by large-scale social media platforms" generates power asymmetries that benefit the platforms,

large advertisers, and social groups whose "political projects are aligned" with their projects. According to Silva, micro-segmentation allows the advertising industry to "manipulate the public debate through individualized messages that harass people on the Internet." To mitigate the risks of those activities during election periods, he proposed "prohibiting advertising segmented by personal data categories, such as ethnicity, political views, or sexual orientation," allowing only the use of data on "general demographic characteristics, such as age and region." Silva also recommends prohibiting advertising topics that "undermine public and polite debates about elections, such as those mentioning violence, defending anti-democratic positions, or demonizing political groups."

For Idec, there is legal support to limit profiling by using "i) sensitive personal data – provided for in the exemplary list of Art. 11 of the General Data Protection Law (LGPD) – to combat unlawful discrimination and ii) children's and adolescents' data", which are also "rejected by several regulatory frameworks, including the Federal Constitution". It mentions that "the healthcare industry's economic exploitation of personal data should also be prohibited."

IAB Brasil, however, warned that profiling restrictions may generate "greater information pollution on platforms, increasing the prominence of less relevant content." According to the institute, "candidacies may become viable precisely because data-driven advertising helps to disseminate proposals in a targeted manner."

5.2.1.5 RESTRICTING CONTENT BOOSTING DURING THE ELECTORAL CAMPAIGN PERIOD

Many points of intersection were observed among the inputs on mitigation measures related to content boosting, profiling, and advertising placement. Intervozes, considering that digital platforms are public interest services, proposes the "prohibition of offering content boosting both for candidate exposure and search results ranking in the electoral context." It recommended that regulating digital social media spaces during election periods follow the same rationale applied to TV and radio broadcasting to ensure symmetrical "exposure of political, party, and electoral content."

IP.rec pointed in the same direction when proposing establishing the obligation of transparency during electoral periods to "reasonably, clearly, and explicitly identify political contents, ban boosted content, and block bulk posting of political messages."

Regarding this proposal, Henrique Bazam, from the scientific and technical community, considers that "completely prohibiting boosted content during the electoral campaign period may be an excessively restrictive measure." Bazan proposes that, instead, "during the electoral period, only candidates and political parties should be allowed to post boost content related to electoral disputes, as monitoring such contents would be more feasible."

5.3 RISKS ASSOCIATED WITH PRIVACY AND PERSONAL DATA PROTECTION

Privacy risks received only a few inputs. ALAI, for instance, mentioned that:

> *[the topic] has a specific regulatory framework governed by the General Data Protection Law (Law 13,709/2018) that regulates cases when personal data processing may pose risks to the freedom and rights of data owners (including discrimination for harmful purposes) and identifies measures to mitigate these risks (including reporting). Therefore, not only is creating new rules for situations already regulated by the LGPD unnecessary, but* ***creating new disconnected rules can generate overlapping and conflicting obligations regarding the same activity*** *[our emphasis].*

ALAI also considered that including mitigation measures is inappropriate "as those issues can be addressed via the LGPD." Other entities, such as IAB Brasil and Câmara.e-net, supported this opinion. The National Data Protection Authority (ANPD) itself asserted that some issues, although related to platform regulation, should remain under its jurisdiction:

> *From the standpoint of* ***personal data protection regulation matters, we consider that they should not be regulated by future legislation on digital platforms****,*

> *given that these are already covered by the LGPD.*
>
> *Among these issues, the following stand out: i)* ***legal hypotheses*** *for personal data processing, such as consent; ii) use of data for user* ***profiling*** *and* ***automated decisions*** *– including those intended to determine users' personal, professional, consumer, and credit profile or aspects of their personality; iii)* ***protection of children's and adolescents' personal data****; iv)* ***accessing personal data for study and research purposes****; and v)* ***assessing the impact on personal data in the digital environment****. All these issues are already regulated by the LGPD and subject to regulation and oversight by the ANPD [our emphasis].*

According to ALAI, complying with personal data protection standards affects the entire digital ecosystem and, therefore, "ANPD's actions to safeguard the fundamental right of personal data protection by restricting personal data abuse play a critical role in fighting disinformation, defending democracy, and limiting the abuse of economic power."

Digital Collective[75] pointed out some risks not mentioned in the consultation, such as the "mandatory use of platforms to access rights, services, and social projects," which may undermine the guarantee of fundamental rights, such as privacy, because users have to agree to the terms of use. Furthermore, it highlighted that once the digital service is used, it is virtually impossible for the user to cancel the service or delete his/her data.

Some inputs expressed privacy and data protection concerns but did not provide any additional contributions to the discussion held by public agents and civil society entities on the LGPD and the ANPD.

However, comments on privacy and data protection risks and mitigation measures were dispersed throughout the consultation as several topics are related to data protection, as data are essential to platforms' business models. For instance, concerns about the impacts of profiling based on personal data were mentioned at several points in this axis but were not addressed again to avoid repetition.

[75] Coletivo Digital.

5.3.1 MITIGATION MEASURES

Some participants mentioned that processing personal data related to health and children and adolescents requires special care. The Alana Institute highlighted the effects of inadequate sensitive health data management or their use for commercial purposes, which "may lead to discrimination of data holders or limit their future opportunities." Further information is included in the child and adolescent data inputs, organized under item 5.4 on "Risks associated with using digital platforms by children and adolescents."

Regarding the identification of potentially harmful situations, IP.rec emphasized the need to consider "the severe damages caused to individuals by pattern detection (behavior on social media, consumption, location, etc.)," mainly when data mining allows their identification, even when personal data are not used. IP.rec recommended "developing good practices and limits to protect people's privacy and individuality effectively."

Some inputs emphasized the importance of implementing privacy protections in application and software codes. The Alana Institute argued that the "failure to implement the concept of privacy by design during all stages of technological product development may turn an individual's fundamental right of personal data protection into an individual obligation." The Center for Integrated Studies, Childhood, Adolescence, and Health[76] (CEIIAS), added that "technology companies need to implement privacy BY DESIGN, as well as delete and block inappropriate contents by the use of their algorithms and technologies." Murilo César Ramos, from UnB, referred to the project conceived by Tim Berners-Lee, called Solid (2016), "centered precisely on the idea of restoring to citizens the control over their personal data."

Lastly, the ANPD expressed the reservation that any regulatory measure evaluating systemic risks – as mentioned in the discussion on the duty of care – that includes personal data processing aspects draws:

[76] Centro de Estudos Integrados, Infância, Adolescência e Saúde.

> *[...] to its scope elements relating to the Personal Data Protection Impact Report (RIDP) [...]. Therefore, in order to preserve the powers attributed by the LGPD to the ANPD relative to the regulation of the RIPD, any normative act should clarify that the effects of the risks arising from the use of personal data must be analyzed by the ANPD.*

Other mitigation measures mentioned throughout the consultation clearly overlap with those proposed for risks associated with privacy and personal data protection, such as i) restrictions on profiling during election periods, ii) restrictions on the commercialization of health and children's and adolescents' data, iii) restrictions on data sharing, particularly of health data, among companies of the same corporate group; iv) interpretations restricted to legal legitimate interest grounds to reduce data concentration; v) implementation of the right to portability (item 2.2.1.1 of Axis 2), among others. Such cases must be compatible with the LGPD and the ANPD's powers, as made explicit in the case of interoperability.

5.4 RISKS ASSOCIATED WITH THE USE OF DIGITAL PLATFORMS BY CHILDREN AND ADOLESCENTS

The risks associated with the use of platforms by children and adolescents received extensive input, especially from the Alana Institute, which is dedicated to children's and adolescents' protection. The inputs addressed the effects of externalities on those age groups in a broad sense. The inputs noted that the expansion of information and communication technologies (ICT) suddenly changed how children and adolescents relate to the world and each other and pointed out the challenges of understanding the effects that change fully.

Several participants reaffirmed the absolute priority of protecting children's and adolescents' rights, including their mental and physical health. In addition to the Brazilian legal framework, they mentioned several other references, such as research, documents, and international standards, to justify the priority of facing these challenges.

For reporting purposes, the inputs received were grouped into two topics: i) digital platforms' business models and ii) mental and physical health.

5.4.1 DIGITAL PLATFORMS' BUSINESS MODELS

Regarding the platforms' business models that affect children's rights, the main issues mentioned were data collection and processing, consumer culture, exposure to harmful content and relationships, online advertising, and sexual exploitation. The Alana Institute pointed out that:

> *The risks to privacy and personal data protection – to which everyone who surfs the Internet is exposed – are more severe for children and adolescents than for any other social group, and any processing of their personal data has a high risk of affecting their human and fundamental rights, as well as their freedoms and their best interests. Due to the vulnerabilities inherent to the developmental stage of children and adolescents, the undue processing of their personal data may result in several violations of their fundamental rights and harm to their development, including those of a discriminatory nature. The use of data for behavioral manipulation, content targeting, and profiling, for instance – common practices applied today on the Internet – may result in future opportunity losses and produce stimuli detrimental to those individuals' free and full development. Such risks are further aggravated by the fact that, as their discernment is still developing, children and adolescents are less capable of fully understanding the negative externalities they are exposed to in the information society and making informed decisions about the flow of their data.*

The institute brought to attention "platforms [that] currently offer free services for accessing student data, which has greatly increased data collection by large technology companies during school hours." It noted, in particular, the "biometric identification [...] in schools" and, more generally, the "lack of choice for children and guardians" regarding the use of tools made available by education systems.

The term 'sharenting,' a neologism combining the words 'sharing' and 'parenting,' was also addressed. "The most popular definition of sharenting is linked to excessively exposing and sharing children's private information by their family members in the digital environment, particularly on platforms and social media." The overexposure of children has generated debates on the balance of rights between freedom of expression and children's privacy and on the responsibility of Internet intermediaries, which are the repositories of this information. The invitation to overexposure often forces children and adolescents to maintain their daily [online] activities, thereby becoming a form of child labor (item 4.2.2 of Axis 2).

The Alana Institute also mentioned the risks "of a business model designed to promote a consumer culture in children and adolescents." Revenue generation depends on processes that:

> *[...] involve multiple business partners, creating a supply chain of business activities; personal data processing, which may result in violations or abuse of children's rights, including the use of advertising design features that anticipate and direct a child's actions towards more extreme content; automated notifications that may disrupt sleep; or the use of a child's personal information or location to target potentially harmful content for commercial purposes.*

The hypothesis that violent content increases the intensity of user engagement with the platforms was also highlighted. This results from the prioritization of such content by algorithms to increase ad exposure time. In this regard, the Alana Institute warned about the risks of exposing children to inappropriate content and encounters, causing severe damage. It mentioned, for example, "the increase in content related to firearms on social media." Researchers and public authorities have warned about the damages of boosting harmful content and the "pollution of the information environment," including the exposure to "harmful encounters or those intended to harm children," highly viewed online content that incites suicide, self-harm, extreme weight loss, and drug abuse; violent scenes; discriminatory content; abusive relationships; exposure of children and adolescents with disabilities to violence; cyber aggression; and sexual exploitation

and abuse. According to the institute, "extremist communities" have taken advantage of opportunities to act on digital platforms, which is associated with "the escalation of violence against schools." The gravity of sexual abuse and exploitation of children and adolescents, which is amplified by the use of digital platforms, was also highlighted.

Furthermore, concerns were raised about the massive use of advertising content targeting platform users of those age groups. One of the examples mentioned is the advertising of smoking products, particularly electronic cigarettes. The Alana Institute mentioned the risk of "disguising" advertising in digital content targeting children and adolescents, such as videos produced by young digital influencers "and ads placed by companies as trends to be followed by other users."

The Alana Institute mentioned the risks of using legal "legitimate interest" grounds for processing children's and adolescents' personal data, as this term is often used to justify processing operations that may potentially violate the rights of highly vulnerable data subjects:

> *Therefore, this legal basis essentially aims to safeguard the interests of data controllers, which is why its establishment includes parameters that guide its application and aims to safeguard the rights and expectations of data subjects. The article that enshrines legitimate interest as the legal grounds for data processing (Art. 7, section IX) has the proviso that it cannot be applied "in the event that fundamental rights and freedoms of the data holder that require personal data protection prevail." [...] For instance, platforms frequently use 'legitimate interest' to justify behavioral advertising targeting children and adolescents, thereby preventing data holders from consenting to these practices that may harm their development.*

5.4.2 MENTAL AND PHYSICAL HEALTH

The incorporation of digital platform applications and services into social processes has increased the use of media by children and adolescents, especially cell phones, resulting in worrying

levels of technological dependence[77] and an alarming increase in the exposure of children and adolescents who have little understanding of the risks of the activities they engage in. In this sense, Slowphone emphasized "technostress," manifested as a loss of empathy, increasing irritability and aggressiveness, changing behavior, family and social relationships, learning and school disorders, as well as several other illnesses.

Some inputs also addressed concerns with aesthetic and self-esteem issues resulting from the dynamics introduced by social media to their users, considering the pressure of business models on "children' and adolescents' self-perception of their body image." It was highlighted that "in the context of generative AI, image generation in popular applications is commonly linked to body whitening and slimming." Alana pointed to the risks associated with how children and adolescents interact on social media, stressing their poor understanding of the effects of their 'sphere of action' when building relationships and producing content, which produces unexpected reactions, such as virtual or even actual lynchings and other effects "harmful to their physical and psychological integrity," putting their very right to life at risk.

As potential mitigation measures, CEIIAS, for instance, proposed that digital platforms should "compensate" affected families and pay for the "pediatric treatment and psychotherapy" of users diagnosed with disorders until they turn 18. The entity considers that the only possible solution is to protect children's and adolescents' rights 'by design.' Other institutions, such as the Alana Institute, support the claim, which proposes the concept of "children's rights by design."

Lastly, the Alana Institute referred to the recommendation of the American Academy of Pediatrics (AAP) and advocates that "children under 2 years old should have no contact with screens, and limiting screen time to 1 hour daily for 2-to 5-year-

[77] Technological dependence was also mentioned by other entities, such as Telefônica Brasil S. A., which pointed to "the considerable market power of such companies, allowing them to manipulate users by developing solutions to maintain engagement and the longest possible screen time in order to sustain the value generation and the high profitability of their businesses. The biggest challenge for regulating the activities and content made available by digital platforms is that platform use and access are linked to social relations, creating consumer dependence."

old children." It also recalled that "the WHO recommends that children under 1 year old should not be exposed to screens, and that screen time should be limited to 1 hour per day for children up to 4 years old." Likewise, Slowphone stressed that "pediatric associations worldwide recommend that children should only have access to these devices (cell phones) after 13 years of age."

5.4.3 MITIGATION MEASURES

The mitigation measures proposed for the risks posed by platforms' business models involved establishing practical and reasonable parameters to ensure children's best interests. To coordinate these efforts, CEIIAS suggested creating "a tripartite coalition" of companies, government bodies (Anatel, ANPD, Secretariat of Social Communication, Ministry of Health, and Ministry of Human Development), and civil society stakeholders, such as the Brazilian Society of Pediatrics (SBP) and the National Council for the Rights of Children and Adolescents (CONANDA), in addition to CGI.br.

The principle of the "strict enforcement of the data minimization precept for the provision of services for children and adolescents by digital platforms" was emphasized. The Alana Institute states that data minimization implies limiting both the amount of data processed and how they are processed to the minimum necessary to achieve a specific purpose. According to the institute,

> *[...] LGPD stipulates that data controllers cannot condition the participation of children in games, Internet applications, or other activities to the provision of personal information beyond that strictly necessary for the activity in question. It is about maintaining the principle of necessity and limiting companies from restricting children's access to their services based on the non-consent of the use of their data.*

The Alana Institute advocated banning behavioral advertising, neuromarketing, immersive advertising, and advertising in virtual and augmented reality environments accessed by children and adolescents.

Lastly, it should be noted that some of Alana Intitute's suggestions, such as requiring digital platforms to create spaces "to listen to and involve users, including those who were subjected to harassment or abuse, their representatives, and users from diverse communities; to inform the platform's policies and processes;" and to cooperate with other platforms and public authorities in "crisis contexts (e.g., threats to schools) to ensure i) the removal of contents that incites violence against children and adolescents, ii) the creation of a database and sharing of hashtags of the identified content to assist in the removal of harmful content."

The associations representing the platforms also listed their initiatives and measures to mitigate risks related to the use of their products by children and adolescents, such as ALAI and Câmara.e-net:

> *Especially concerning children and adolescents, investments have been made to develop solutions and mechanisms to increase their security, including new settings and special resources, such as parental control mechanisms, restricting messages between adults and adolescents, security warnings in direct messages, setting adolescents' and children's accounts as private by default, and tools that limit bullying and harassment messages and comments. However, such measures are only effective when authorities and platforms devote efforts to help parents and guardians understand how to support and control their children's access to social media.*

5.5 RISKS ASSOCIATED WITH THE EFFECTS OF LACK OF TRANSPARENCY OF DIGITAL PLATFORM ACTIVITIES

Transparency was one of the most relevant topics mentioned in the inputs. In addition to being widely debated from the perspective of the risks associated with digital platform activities, transparency was emphasized as a general regulation principle in Axis 3 of this consultation. Several sectors and actors addressed the challenges of transparency (or its lack thereof) from different perspectives. The main dissent was observed between those who defend the need for more transparency obligations for digital

platforms, particularly digital social media, given the clear public interest in their data collection and processing activities, and those who support limiting transparency obligations mainly due to commercial secrets and business model sensitive information reasons. The underlying reason is the conflict between the participants who conceive data as a product of social relations and, therefore, are objects of social interest, as detailed below, and those who evoke intangible property rights and the harmful economic effects caused by the lack of protection of these assets.

The current legal framework on transparency obligations and the set of measures adopted by platforms to inform about their data processing and content moderation practices adds to the debate on trade secrets by commercial stakeholders, who strongly advocate limiting a possible increase in transparency obligations, as mentioned by IAB Brasil, an association of digital advertising companies.

> *Additional regulation on the topic [transparency] would only generate legal uncertainty, and it is opposed to the purpose of the policy itself, which is to act as a [model] for general, rather than sectoral, application to any economic activity, whether online or offline. Any regulation on prioritizing, targeting, recommending, and boosting content must consider that these criteria represent trade secrets, and their disclosure outside of particular contexts may have effects contrary to those desired, allowing bad actors to circumvent the rules established by each platform. Specifically, the obligation to provide clear, public, and objective information about the main characteristics of the service offered is already provided for in the MCI (Art. 7, VI and XI) and the CDC (Art. 6, III and 46). Furthermore, the provision of services and recommendation systems presuppose, to a greater or lesser extent, the processing of personal data, which is already extensively regulated by the LGPD – including the mandatory disclosure of clear and complete information on personal data processing (Art. 6, VI) and the obligation of the controller to provide, whenever requested, precise and sufficient information on the criteria and procedures used for automated decision-making, taking into account commercial and industrial secrets (Art. 20, Section 1).*

This position was supported by other business sector entities, such as ALAI and Câmara.e-net. According to Brasscom, any regulation on content prioritization, targeting, recommendation, and boosting practices "should consider that these are trade secrets, and their disclosure outside particular contexts may have effects contrary to those desired," and stressed that transparency is also a concern of digital platforms:

> *Digital platforms already establish strict transparency rules regarding content removal and publish transparency reports that detail the origin of requests and their outcome, which can be monitored by civil society. Moreover, several academic studies are based on the information disclosed by the platforms.*

Trade secret protection as grounds for opposing further transparency obligations reveals the central role of data collection and processing in extracting additional information and the heavy reliance of many data-intensive industries on new ways of establishing ownership over these intangible assets, as shown by the inputs that held this opinion. Brasscom, for instance, emphasized that:

> *[...] the Brazilian legal system grants trade and industrial secret protection to information with market value. Like many OECD countries, Brazil is a signatory to the TRIPS (Trade-Related Aspects of Intellectual Property Rights) Agreement, incorporated into the Brazilian legal system with superior hierarchical status per Legislative Decree 30/1994 and Presidential Decree 1,355/1995.*

It should be noted that TRIPS provided effective international protection to trade secrets through policies to restrain unfair competition. Brasscom also pointed out the relationship between encouraging innovation and protecting the confidentiality of data processing and algorithms:

> *Overall, digital platform services stand out for their innovation. [...] At the heart of this innovation are databases and algorithms, partially or fully owned by the platforms, allowing content to be organized in different ways, according to user preferences. Therefore, such companies should not*

> *be subject to data or source code disclosure requirements that may interfere with competition, inhibit innovation, or open the door to bad actors.*

On the contrary, other inputs stated that expanding transparency obligations is essential. Idec, for instance, in contrast with the private sector perspective, argues that transparency is not a matter of:

> *[...] trade secrets, but instead of public interest to users and society. Transparency is a fundamental right in many spheres – from data protection to consumer protection. Regulation should broaden such obligations. According to the Consumer Protection Code provisions, advertising must be displayed so that the consumer can immediately identify it (Art. 36). In the context of digital platforms, further measures are needed to enforce that right. Also, considering the basis of respect for Human Rights, the development of personality, and the exercise of citizenship in digital media (Art. 2º, II of the MCI), it is essential that platforms provide transparency regarding the amounts allocated to advertising and the identification of the user responsible for the boost or/and the advertiser.*

The CDR considered that transparency obligations may "balance the imposition of new responsibilities on digital platforms with the guarantee of the protection of human rights," while Instituto Vero proposed that "transparency obligations should be the backbone of platform regulation."

Regarding possible **algorithmic transparency mechanisms and criteria**, CTS/FGV proposed that algorithmic transparency has two main challenges. It affirmed that "the more complex the adopted software becomes, the more challenging it is to explain its operation intelligibly, making it difficult for platforms to provide accountability." The research center recognized that "technical details on how algorithms work may be considered trade secrets because algorithms are an essential part of the services offered by platforms in an intensely competitive market"; however, their adequate monitoring by users and regulatory authorities makes it urgent to establish means to ensure satisfactory accountability, including to "verify if the information imparted by platforms is valid and accurate." As a possible solution, CTS/FGV proposed

"auditing such information by technically qualified and legitimate authorities in a confidential manner," allowing the protection of technical aspects with market value and "validating the explanations disclosed."

5.5.1 MITIGATION MEASURES

The mitigation measures proposed in the consultation explored possibilities for increasing transparency obligations for content moderation rules, criteria, and procedures. Idec advocated that "monitoring content removal, prioritizing, targeting, recommendation and boosting practices, including advertising contents" should be subject to transparency obligations. Additionally, CDR proposed requiring "notifying users that the content is moderated," while DiraCom mentioned transparency about "complaints received by users, moderation measures applied, and the operation of appeal systems."

In this sense, CEPI/FGV highlighted that "content moderation systems heavily depend on third-party oversight" to identify posts that do not comply with established terms of use and illegality policies, particularly to enforce changes when harmful patterns and adverse effects of content boosting are identified. The understanding that automated content moderation, *per se*, is not sufficient to protect Human Rights is widespread: several inputs stated that monitoring is not only a pillar to protect the public interest in debate spaces on digital platforms but also a measure to improve the activities of the digital platforms themselves, the State and civil society.

According to CEPI/FGV, "accurate understanding of how moderation works is required for constructive feedback or accountability, which can only be achieved if there is some degree of transparency." Moreover, it criticized transparency reports, pointing out that:

> *[...] The disclosed information often does not allow for drawing relevant conclusions. In some cases, the reason is that* ***each platform tends to adopt its methodology and terminology for organizing data, making comparisons difficult and preventing a complete view of the phenomenon of proliferation and moderation of problematic content****. How information disclosed in reports is presented and*

> *classified tends to differ significantly among platforms, hindering comparing companies' activities and analyzing that information to obtain a comprehensive perspective of the proliferation of harmful contents [our emphasis].*

Some entities suggested establishing transparency mechanisms for digital platform **data sharing for academic research**, such as the Alana Institute, which proposed the "creation of 'access layers' for data sharing among researchers that incorporate a notion of risk regarding the information made available." Edson Vicari pointed to the importance of implementing data access mechanisms that "allow researchers to safely and effectively access data [...] by developing application programming interfaces (API)" to strengthen the link among universities and their faculty, researchers, and research groups with digital platforms.

Likewise, MTST's Technology Center discussed the role of digital platform data in research, saying that "it is beneficial and in the interest of the Brazilian society that this data is freely available for scientific research and public policy development purposes." It emphasized public interest and research data categories, such as "those related to content circulation in private messaging applications; public content on social media; road traffic news; advertisements on marketplaces; those related to the activities and compensation of app drivers, delivery workers, and service providers; and financial transactions." The center also mentioned the role of "open and free availability to all of the scientific publications and used and produced data, methodologies applied, and analyses performed" under open science standards to reduce power asymmetries generated by data concentration and processing.

Several participants proposed imposing more stringent obligations to specific areas that share data with specific audiences, such as those "related to the proliferation of disinformation to allow identifying viralization patterns," such as CEPI/FGV. Other inputs added that data on clearly illicit activities may contribute to "identify and locate victims [of sexual abuse and exploitation] to halt violence situations and initiate victims' support," as suggested by the Alana Institute. Many inputs supported the idea that content targeting children and adolescents must be "subject to stricter transparency obligations."

Regarding imposing possible **transparency obligations on content monetization and targeted advertising**, there was a high degree of consensus on the importance of ensuring greater transparency of the platforms' decisions on monetized and advertising content to fight infodemics and effectively hold "political agents who benefit from disinformation through the constant engagement of voters, and carry out coordinated attacks on the reputation of their opponents" accountable, including starting political campaigns earlier than allowed and abuse of economic power, as stated by the SEADE Foundation.[78]

Lastly, while not disagreeing with the need for effective transparency mechanisms, several entities expressed concerns about the risk of transparency and monitoring obligations becoming surveillance measures, threatening fundamental rights. Specifically regarding encryption, IRIS warned that the transparency and sharing of data requested by authorities should not "impose measures that oppose or weaken encryption in the digital environment, particularly in messaging services."

5.6 CONCLUSION ON RISKS RELATED TO DEMOCRACY AND HUMAN RIGHTS

The scope of the risks to Democracy and Human Rights is reflected in the number of inputs received and the depth with which the various topics listed in the consultation were addressed. Initially, it is worth highlighting the recognition of the duality inherent in the expansion of the Internet: if, on the one hand, it democratized access to information and provided groups previously silenced a space to express themselves, on the other, it generated unforeseen externalities, unanimously accepted in the inputs related to the deterioration of social relations and the public space for debate. The vast majority of inputs mentioned threats to freedom of expression, access to reliable information, cultural diversity, and democracy, expressed by several challenging issues, such as disinformation, the rise of extremism, hate speech, and, mainly, incitement to violence. Consequently, as the third sector and the scientific and technical

[78] Fundação SEADE - Sistema Estadual de Análise de Dados (Data Analysis State System Foundation)

community pointed out, minority groups understand their situation to be more serious. More importantly, such problems are directly related to digital platform activities, mainly digital social media.

Regarding the challenges posed by infodemics, the third sector and the scientific and technical community described three elements as the pillars of models that contribute to undermining the information environment: i) massive data collection and processing, ii) profiling and micro-segmentation, and iii) algorithmic systems programmed to increase engagement time and provide digital platform user visibility to monetize posted content, fundamentally through advertising.

The private sector sent fewer inputs on infodemics, only questioning the use of the term, which it considered inaccurate.

Two other elements received fewer inputs. The first relates to digital inclusion challenges and addresses strategies for selling Internet access to mobile devices associated with data plans applying the zero-rating practice. The second element refers to the risks of technology appropriation and digital literacy. The other elements addressed were challenges related to the lack of media regulation.

Regarding the risks to quality journalism, there was a consensus that fighting infodemics involves strengthening journalism, an important mechanism to ensure the citizens' access to information. The main focus of the third sector and the scientific and technical community was the significant transfer of advertising revenues to digital platforms and their power over the content circulating on the Internet. Some argued that alternative and community media are severely affected by advertising concentration, requiring the development of policies aimed at democratizing funds and diversifying forms of content circulation.

However, there was no consensus on the role platform activities play in the problems faced by journalism or the mitigation measures for the risks presented. On the one hand, entities representing digital platforms recalled that the "crisis in journalism" phenomenon is not new and that digital platforms offer opportunities to increase journalism plurality. They added that news outlets freely decide to share links to their content because they benefit from the platforms' traffic and, therefore, cannot

expect remuneration. On the other hand, entities representing traditional media companies argued that the capacity of digital platforms to attract audiences generates power asymmetry, making news companies hostage to the terms established by the platforms. In addition to controlling website search, platforms create ways to maintain users connected to their services and applications, generating increasing advertising revenues and reducing direct visits to news outlet websites.

Regarding democracy and electoral processes, there was broad consensus on the relevance of digital platforms in the construction of public debate. Narratives Network stated that the powerful influence of digital social media on the public debate poses the risk of domination of the public discourse. IP.rec proposed studying election cases to understand how digital platforms influenced the victory of political candidates and projects.

Several inputs mentioned that, despite disseminating electoral disinformation, some digital platforms continue to apply tools to monetize their content, promote it, or even have it delivered through algorithmic prioritization and recommendations on social media. In this context, several participants sought to describe a system that privileges groups that attack fundamental principles and rights and perpetrate illegalities, taking advantage of digital platform business models, which evidently allowed such groups to advance their political agendas.

Regarding transparency, the main dissents were observed between those who advocate for the need for increasing digital platform obligations – particularly digital social media –, considering the indisputable public interest in how data are collected and processed, and those who expressed reservations on such obligations in light of the protection of trade secrets and sensitive information related to the business models of large platforms.

On the one hand, business sector entities argued that the current legislative framework addressing transparency obligations and the measures adopted by platforms to inform about their practices suffice, citing trade secrets to oppose the creation of further new transparency obligations, also claiming that such obligations may generate legal uncertainty. On the other hand, third-sector entities disputed the trade secret claim,

asserting that transparency is a matter of public interest for users and society because it is a fundamental right in many spheres, from data protection to consumer protection. Their inputs emphasized the need for new transparency obligations for rules, criteria, and procedures applied to content moderation and for notifying users when content is moderated. In addition, stricter transparency obligations should be imposed during the electoral period, establishing specific rules to prevent distorting the democratic systems.

The inputs related to data protection risks were generally dispersed throughout the consultation. However, suggestions from the third sector stand out, including restrictions on data-based profiling and the concern raised by the ANPD regarding preserving its powers and adequately aligning any platform regulation policies with those provided for in the LGPD (BRASIL, 2018).

Relative to children and adolescents, several inputs – in particular, the extensive input of the Alana Institute – addressed the vulnerability of this age group to digital platform strategies and business models, emphasizing the absolute priority of protecting their rights, including their mental and physical health, involving issues such as dependence on technology, coined technostress, which leads to loss of empathy, increased irritability and aggressiveness, deterioration of family and social relationships, learning disorders, among others.

Mitigation measures were summarized in broad themes that indicate some of the main approaches presented in the consultation. The first theme, organized into four groups, addresses the responsibility of digital platforms for third-party content. The participants' opinions were based on widely diverse approaches, which may be simultaneous. For instance, the general platform liability regime provided for in the MCI (BRASIL, 2014) should be maintained even if Brazil adopts objective liability for promoted/paid content.

One group supported preserving the current terms of the MCI (BRASIL, 2014), arguing that they are entirely satisfactory in meeting content moderation demands, as stated by ISOC Brasil, from the third sector. Entities representing digital platforms, such as ALAI, ITI, and Câmara.e-net, fully endorsed this approach.

The second group argued that digital platforms should be liable for promoted and monetized third-party content. This opinion, supported by third-sector and academic entities, such as Idec and CTS/FGV, considered that platforms should be governed by objective and/or joint liability. Traditional media company associations also endorsed this position, suggesting the need to create a general regime for digital platforms that alters the MCI (BRASIL, 2014).

The third group proposed developing a special liability regime requiring digital platforms to moderate specific content categories, such as those violating the rule of law. Abranet defended including legal assets that require a higher degree of protection in the list of exceptions to the MCI (BRASIL, 2014). Traditional media associations also proposed developing a special liability regime addressing content categories and added that, in the business sector, the liability of intermediaries has been the subject of intense debates.

The fourth group advocated establishing obligations to assess and mitigate systemic risks arising from digital platform content moderation to protect users' rights and mitigate other harmful effects beyond specific content moderation. This group included third-sector organizations, such as CDR and IP.rec, which referred to European experiences based on the duty of care principle.

Significant dissent on the notice and takedown mechanism suggested by traditional media business associations that support the duty of care principle was observed. In agreement with the proposals of this fourth group, CEPI/FGV proposed, as an alternative to the model based on notice and action mechanisms, to require a platform to act when notified in compliance with the duty of care.

Still relative to mitigation measures, participants proposed initiatives to democratize content production, including journalism content. To this end, third-sector and academic entities recommended establishing a model to share the financial resources obtained by digital platforms via content monetization and advertising, including journalistic content, by imposing taxes on those activities and creating a fund to manage the collected taxes.

A set of inputs submitted by the third sector and academia supported strengthening data-sharing partnerships between digital platforms and researchers in the context of the discussion on stricter transparency obligations. Furthermore, third-sector entities proposed making data available, free of charge, for scientific research and public policy development, considering that digital platform activities, mainly those relative to social media content flow, are evident objects of public interest.

Lastly, inputs advocated measures to restrict personal data collection and processing, particularly children's and adolescents' data, whether personal or not, and health data. In this regard, the Alana Institute emphasized the absolute priority of protecting the rights of children and adolescents, including their mental and physical health, proposing several prohibitions relative to the collection and use of their data. Furthermore, the importance of strictly applying the logic of data minimization to provide services on digital platforms was highlighted as a mitigation measure, especially for children and adolescents.

AXIS 3 – HOW TO REGULATE

1 INTRODUCTION

Despite the global consensus that regulating digital platforms is urgent, the capacity of institutions and social actors to act jointly and in a coordinated manner in this mission is complex. Over the past two decades, data protection authorities have emerged in different countries, ranging from "super regulatory agencies," such as the DMU in the UK, to private oversight boards, such as the Facebook Oversight Board. In this context, the possible institutional arrangements for regulating platforms in Brazil are one of the main topics under debate.

This chapter presents a quantitative and qualitative summary of the inputs on "how to regulate" digital platforms (Axis 3). In total, 135 inputs were received for the five questions of Axis 3, representing 8% of the total received throughout the consultation.

In general, Axis 3 presented diverse institutional design possibilities for the national regulation of digital platforms. As described in the methodological introduction of this report, the inputs were classified according to the analytical plan developed by Mendes and Miskulin (2017) to generate possible quantitative analyses to determine, in addition to the distribution of inputs, the levels of agreement and disagreement of each of them, as well as qualitative analyses of the different proposals and approaches.

Based on this analytical plan, the inputs were divided into six subthemes:

1. Principles and guidelines for defining a governance model for platform regulation;
2. Legal nature, characteristics, and decision-making process of the institutions involved;
3. New entities and their responsibilities;
4. CGI.br's responsibilities;
5. Proposed sanctioning and redress compensation measures; and
6. Regulatory approaches.

Finally, it should be noted that the drafting of the report of Axis 3 allowed – in specific topics and to a greater extent than in the other axes of the consultation – grouping inputs per sector based on their shared perspectives; however, even in such cases, shades of opinion within each sector were often observed.

2 PRINCIPLES AND GUIDELINES FOR DEFINING A GOVERNANCE MODEL FOR PLATFORM REGULATION

The set of principles defined in this topic sought to identify and group those presented by a set of actors to obtain a general overview of the principles mentioned by the consultation participants, namely: i) multistakeholderism, ii) independence, iii) transparency, iv) international cooperation, v) proportionality and adequacy, vi) innovation; vii) specialty, and viii) legality.

2.1 MULTISTAKEHOLDERISM

The most frequently mentioned term in the inputs related to a value for the governance of digital platform regulation was **multistakeholderism**. In total, 32 inputs stated the importance of multistakeholderism, equivalent to around a quarter of the inputs to Axis 3 (24%).

The mentions highlighted the importance of encouraging the participation of different sectors and actors and the consequent consideration of thematic diversity in decision-making processes. Terms such as **multidisciplinarity** and **transdisciplinarity** were also values associated with multistakeholderism. Some inputs emphasized the value of multistakeholderism, mentioning the successful activities and projects implemented by CGI.br and Ponto BR's Information and Communication Center (NIC.br). The terms **parity** or **equal representation**, referring to the representativeness of social groups, were also emphasized. **Participatory governance** or **democratic and collaborative governance** were used in proposals to enhance the dialogue among **the government, the industry, and the society**.

In general, the inputs relate multistakeholderism to an institution's decision-making process, focusing on the **participation** of different sectors in a multi-stakeholder

regulatory environment; however, they did not delve into the more practical aspects of decision-making processes. Although there was consensus on multistakeholderism as a value, its implementation forms differed among the participants, as detailed in the following items.

2.2 INDEPENDENCE

Independence was also frequently asserted as a fundamental value for regulation, especially in proposals for creating new bodies and institutions. The principle of independence was almost unanimous among those who responded to questions on the topic and was mentioned by a significant set of inputs (25), as well as all those suggesting new regulatory bodies. Independence was associated with concepts such as **autonomy**, **technical and administrative autonomy**, and **functional independence**.

The concern about the lack of independence or autonomy was based on two main perspectives. The first refers to the lack of representation and transparency in the discussions that shape democratic decision-making processes and ensure the supremacy of the public interest. According to this perspective, independence is a barrier against pressures exerted by regulated economic sectors and the government in power.

The second perspective is associated with the term **capture** and is based on the historical experiences of regulatory agencies, which have yielded to the influence of the interests of regulated economic groups in their decision-making processes.

2.3 TRANSPARENCY

One of the most emphasized principles in the inputs was **transparency**. It was mentioned 17 times or in 12,6% of the inputs from Axis 3; however, it carried different nuances and meanings.

A significant number of the inputs cited transparency based on the three perspectives described in the literature on the subject (GOMES, AMORIM, ALMADA, 2018): i) strengthening of the will and opinion of citizens by providing available information and knowledge; ii) citizens' power to hold authorities accountable for

their actions and omissions, and iii) enabling ethical judgment on the action or omission of authorities by the public. In different degrees and contexts, the mentions of transparency pointed to the harmful effects of the lack of information for social control, articulating the principle of transparency with social participation and active accountability.

Companies' transparency regarding the use of algorithms was frequently noted. Abranetcited that the "European Commission established a specific unit for algorithmic transparency (European Centre for Algorithmic Transparency)" as a measure to increase the citizens' power to counter the power of digital platforms.

Inputs, such as ISOC Brasil's, highlighted concerns about the transparency of monitoring and sanctioning measures, advocating "greater transparency and communication of measures when the blocking of digital platforms is determined," for instance. In this regard, José Antônio Galhardo, from the government sector, proposed "imposing transparency obligations before inspection bodies and the Judiciary."

Several inputs criticized the **lack of transparency**, as mentioned in the comments in Axis 2 of this report. In particular, inputs submitted by the third sector and the scientific and technical community warned about the negative externalities of the "opacity of platform business models" on the political power of other social actors, such as platform workers and the government, when levying these companies. The inputs asserted that transparency is essential for developing a regulatory model capable of addressing the challenges generated by the platformization of society.

Private sector inputs, in particular, advised caution when establishing numerous and rigorous obligations. For instance, Brasscom stated that achieving "the delicate balance between ensuring transparency of platform use and imposing excessive and disproportionate obligations or restrictions is essential." ALAI emphasized and described the transparency mechanisms already applied by digital companies to promote transparency.

Lastly, the transparency obligations of the legislation in force, notably the LGPD (BRASIL, 2018), were cited in several inputs. Other legislation and regulatory mechanisms, such as the MCI (BRASIL, 2014), establishing specific transparency obligations, were also mentioned.

In summary, although the principle of transparency was postulated in many inputs, there were differences and shades regarding the specific rules required for its implementation in digital platform regulation.

2.4 INTERNATIONAL COOPERATION

With only three mentions, **international cooperation** was proposed as a guideline for facing the challenges related to the consolidation of a global infrastructure of communication networks. Such cooperation was associated with the promotion of international data transfers. ALAI and Câmara-e.net argued that international cooperation is "technically required for Internet operations [and its development]" and "support the global and Brazilian economies, directly benefitting citizens by providing access to diverse information," respectively.

In this regard, the compatibility of legal frameworks, sharing of regional experiences, training, and crime monitoring and investigation were considered dependent on international cooperation (global and regional) and essential for the protection of fundamental rights, given the cross-border nature of the Internet.

2.5 PROPORTIONALITY AND ADEQUACY

There was broad consensus on the principle of **proportionality**, which requires a regulatory model that considers the asymmetries between digital platforms and their different fields of activity and between platforms and the actors affected by their activities. DEIN stated that "to achieve legal and regulatory proportionality and the diversity of models and sizes of digital platforms, the regulation should be considered asymmetrical, in principle." Brasscom emphasized that the regulation should "contemplate the different services, their potential risks, scope, and nature to make an appropriate and proportional public policy choice based on this information."

A specific example was given by TelComp, who pointed out the need to tackle the imbalances and asymmetries "of the relations between telecommunications providers and content providers, in order to ensure fair remuneration for the use of the Telecommunications Operators' networks," referring to a fair

share, or the sharing of revenue between large content providers and telecom operators.

There are two dimensions to the approaches mentioned: respecting the differences among regulated entities based on the proper assessment of regulatory risks and attributing a role to proportionality and adequacy to reduce asymmetries that harm the economy and innovation.

Lastly, proportionality was considered relevant in the scope of sanctioning and liability to ensure that the measures applied are proportional to the damage and the negative impacts caused by the sanctions themselves, as ISOC Brasil and DiraCom mentioned.

2.6 INNOVATION

A set of inputs, especially from the business sector, considered the possible adverse effects or externalities of regulatory measures on **innovation**. The inputs, in general, advised caution when imposing possible restrictions on the freedom of business models. For instance, ITI expressed concerns about possible "data flow restrictions, generating business uncertainty and frictions in the Brazilian business environment that could hinder data innovation, without enhancing data protection." Concerns about establishing data collection and processing restrictions were also raised. According to IAB Brazil, "it generates many more risks than benefits because some harmful practices often can only be prevented by data processing."

In this context, the concern about possible restrictions on innovation was used to justify a regulatory approach based on "regulated self-regulation," as ALAI and Câmara.e-net mentioned.

2.7 SPECIFICITY

The principle of **specificity** was frequently mentioned in the inputs, grounded on the concept of the Brazilian administrative law, which establishes that "state entities" cannot abandon, alter, or modify the purposes for which they were constituted and must always act according to the purposes that motivated their creation (PINTO, 2008).

Although not mentioned directly, the principle was approached from two complementary perspectives. The first supports a decentralized or polycentric governance model, in which the role of public entities in digital platform regulation is based on established roles and responsibilities. The ANPD expressed concern in this regard, mentioning that:

> *[...] regardless of the decision taken on the regulatory approach and the regulatory body, the ANPD's powers to protect personal data must be preserved, including regulating, supervising, and applying administrative sanctions under the terms of the LGPD.*

The second perspective was manifested in the inputs that refuted the possibility of Anatel[79] assuming responsibilities related to digital platform regulation, given its specificity in telecommunications regulation. In this regard, entities such as Abranet, NUPEF Institute[80], CDR, and EFF, among others, stated that Anatel should not assume responsibilities beyond those established by law.

2.8 LEGALITY

The principle of **legality** was mentioned in some inputs and was generally associated with sanctions. According to IP.rec, from the third sector, it is necessary to characterize illicit conduct and its administrative sanctions and standardize the degree and application of these sanctions to prevent legal uncertainty. ISOC Brazil emphasized the importance of legality, especially when applications are blocked as a sanctioning measure, given the risks of the abusive use of this measure. Brasscom stated that the regulating body's powers and functions must be precisely defined to make its actions predictable and limited by legality.

[79] Agência Nacional de Telecomunicações (National Telecommunications Agency).

[80] Núcleo de Pesquisa Estudos e Formação (Research, Studies, and Training Center).

Expressing similar underlying concerns relative to the principle of lawfulness, EFF's input mentioned ensuring due process so that sanctions are applied "per human rights standards and due process guarantees, particularly when blocking online applications is involved."

3 LEGAL NATURE, CHARACTERISTICS, AND DECISION-MAKING PROCESS OF THE INSTITUTIONS INVOLVED

Several institutions were proposed for implementing and monitoring the digital platform regulation, which mainly differed in their legal nature, the role of the State and private entities, and the level of concentration in the decision-making poles.

Of the 31 participants who expressed their views on establishing new entities to regulate digital platforms, around 80% (25) said they should be created or adapted for regulation[81]. Three organizations or individuals who rejected the proposal made subsidiary suggestions detailing the nature and roles of such new entities. Therefore, most participants supported establishing an entity responsible for regulating platforms (or at least acknowledged this possibility) and asserted that influencing its characterization was relevant.

The entities proposed ranged from autonomous public bodies[82], regulatory agencies (a specific type of autonomous

[81] For reporting purposes, the comments of those in favor of creating and those in favor of adapting an existing authority are presented together, considering that this new competence would require profound changes to the structure and capabilities of any entity. A broad concept of "entity" was also adopted, which includes not only the creation of bodies and agencies but also councils, private entities, and new structures that are considered necessary for implementing regulation.

[82] According to Art. 5, I of Decree-Law 200 (BRASIL, 1967) and Art. 41, IV of the Civil Code (BRASIL, 2002), an autonomous federal body is a legal entity under public law, "created by law, with independent legal personality, assets, and revenue, responsible for performing typical public administration activities that require decentralized administrative and financial management to function properly."

public body)[83] , and various formats of councils, committees, and private entities. Among the 28 respondents supporting a new entity, subsidiary proposals were presented. Six (19.3%)[84] proposed developing a regulatory system involving a combination of an autonomous public or public council as the primary regulator linked to a multi-stakeholder council or committee. Another six suggested an autonomous body (including an agency), and another six, a council (generally multi-stakeholder). Furthermore, 13 respondents did not specify which entity type, as shown in Table 4 below.

TABLE 4 – ENTITY TYPE SUGGESTED TO SUPERVISE THE LEGAL FRAMEWORK OF PLATFORMS AMONG THOSE WHO ADVOCATED THE CREATION OF AN ENTITY OR SYSTEM

RESPONSIBLE ENTITY(IES)	NUMBER OF PARTICIPANTS	PERCENTAGE
Regulatory system	6	19.3%
Autonomous federal body	6	19.3%
Multi-stakeholder council or committee	6	19.3%
No specification	13	42%
TOTAL	31	100%

SOURCE: PREPARED BY THE AUTHORS.

Several inputs proposed that the entity responsible for implementing platform regulation be endowed with technical autonomy and operational independence. According to

[83] Regulatory agencies are special-purpose federal autonomous entities, according to Law 9,986 (BRASIL, 2000). Its special nature is "characterized by the absence of hierarchical oversight or subordination; by operational, decision-making, administrative, and financial autonomy; and by a fixed term of office and stability thereof," per Art. 3 of Law 13,848 (BRASIL, 2019).

[84] Out of the six, five are from the third sector (CDR, DiraCom, Flávia Lefèvre, Idec, and IRIS), and one is from the government sector (DEIN).

business associations, such as Abranet, ALAI, Brasscom, and Câmara.e-net, if a digital platform regulation is implemented, it should be established a **new supervisory entity endowed with autonomy, technical competence, and operational independence** to allow it to act impartially. Multistakeholderism should be the core value of such an entity, whose composition, as detailed by Abranet, should include representatives of the public sector (Cade, ANPD, Anatel, National Consumer Secretariat - Senacon, SECOM, Ministry of Justice and Public Security - MJSP, Legislative and Judiciary, among others), private sector, third sector, and academia, in addition to CGI.br.

Other inputs, such as that of Flávio Wagner (UFRGS) from the technical and scientific community, proposed creating a **self-regulatory entity** – of a private nature, therefore, composed of digital platforms – to review content moderation decisions and an autonomous supervisory entity, with multi-stakeholder representation, but its legal nature, i.e., whether public or private, was not specified in the inputs.

In contrast, other participants argued that typical State activities cannot be delegated to private entities, including police, taxing, and punishing powers, which should be vested in a possible public supervisory body regulating digital platforms. In this sense, Idec and IRIS, from the third sector, supported limiting the powers of the self-regulatory entity.[85]

Moreover, a significant number of inputs proposed creating a **governance system** that gathers institutions of different natures and powers. Some third-sector organizations suggested establishing **an authority to regulate, implement, and monitor the established standards associated with a multi-stakeholder council with deliberative capacity**. As detailed by IP.rec, this authority should have administrative, financial, and

[85] According to IRIS: "the private sector can establish a self-regulatory entity, following the successful example of the National Advertising Self-Regulation Council (CONAR). This entity could encourage the adoption of good practices and support the development of voluntary codes of conduct in the sector. It would also be beneficial for platforms to proactively create independent spaces with a multi-sectoral composition to monitor the guidelines applicable to content moderation and propose improvements". According to Idec: "as a complement to regulation, so that platforms have independence and responsibility in their operations and that individual content analysis is not the responsibility of a new authority".

operational autonomy, include an expert technical body, have an autonomous legal nature, and, consequently, be attributed to indirect public administration. Moreover, according to DiraCom, the multi-stakeholder council, given its deliberative capacity, should protect the authority from regulatory capture and increase public participation, thereby ensuring the technical expertise and public participation required to detail the rules, monitor their compliance, and apply sanctions in case of violations. Although the inputs did not specify the legal nature of the council, due to its association with a public autonomous body, it is assumed that it would be a public body.[86]

Other inputs also supported the development of a regulatory system but did not advocate the creation of an autonomous regulatory body. Third-sector inputs, such as Flávia Lefèvre's, proposed a regulatory structure composed of a company representative body, an Interministerial Council, and the CGI.br, arguing that "a centralized regulatory model with little democratic representation, as is the case of agencies [...] will not be able to regulate to ensure rights duly across such a broad spectrum." The Special Commission for Digital Law of the Brazilian Bar Association (OAB) also proposed creating a tripartite "Brazilian System for the Regulation of Digital Platforms" with a composition different from that of the Digital Policy Council.[87]

---

[86] According to Art. 6 of Law N. 9,784 (BRASIL, 1999): "I – body – the unit of action that is part of the structure of the direct Administration and the structure of the indirect Administration".

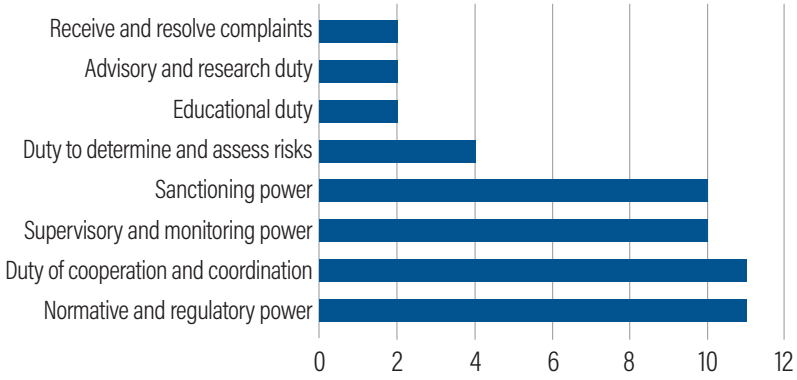
[87] According to a statement by the OAB's Special Commission on Digital Rights: "We disagree only with regard to the composition of the council, as we understand that it should be broader, made up of several ministries that already have their own specific bodies with regulatory power, under the terms of Art. 87, Inc. I and II, of the Federal Constitution, and police power to promote inspection and impose sanctions, as occurred recently with the publication of Ordinance 351/2023 by the Ministry of Justice, through which the National Consumer Secretariat was mandated to adopt measures with the platforms, in the context of Operation Safe School. In other words, we understand that the Council should be made up of the Ministries of Justice, Human Rights, Education and Culture, Health, Labor, the Civil House – which currently includes the Secretariat for Digital Policies, Communications, CGI.br, given the powers it received from the MCI, and also by the ANPD, given the highly specialized technical nature of monitoring the exploitation of personal data by companies and public sectors. It is important that the Council also include representation from civil society."

4 NEW ENTITIES AND THEIR ROLES

The analysis of the set of inputs reveals differences and similarities as to the roles of each of the new proposed entities. The duties and powers of each proposed entity were analyzed and classified according to the classic functions of regulatory bodies: i) power to inspect and monitor; ii) normative and regulatory power; iii) sanctioning power; iv) power to receive and resolve complaints; v) advisory and research duty; and vi) educational duty.[88] Furthermore, given the frequent mention and specificity of the topic, two classifications were added: i) duty to determine and assess risks and ii) duty of cooperation and articulation, in addition to the comprehensive category "others" for the *sui generis* suggestions that had a low number of mentions.

Graph 1, below, shows the number of mentions made in the inputs to the desired roles of a digital platform regulatory body. "Normative and regulatory power" and "duty of cooperation and coordination" were the most frequently mentioned (11 mentions each), followed by "sanctioning power" and "supervisory and monitoring power," with 10 mentions each.

GRAPH 1 – NUMBER OF MENTIONS OF THE DESIRED ROLES OF THE REGULATORY AUTHORITY



SOURCE: PREPARED BY THE AUTHORS

[88] Such classification was inspired and adapted from Simão, Oms and Torres (2019) "investigative power; intervention power; power to receive and resolve complaints; normative and consultative power; duty of transparency, accountability and participation; and educational duty. Such factors [...] are important to understand the structure of each authority and its capacity to give effect to a national personal data protection policy in each country" (p. 10).

It should be noted that the "duty of cooperation and coordination" was also mentioned in the set of traditional regulatory authorities' roles. This duty generally arises as a response to the transversality of digital markets, covering the competencies of different agencies and authorities and, therefore, demanding articulation among the competent entities.

As pointed out, most **business associations** argued that there is no need to create a regulatory entity; however, they specify their roles and powers in the event of its creation (except for ITI). ALAI, Brasscom, and Câmara.e-net mentioned that this authority – if created – must have **normative and regulatory powers**. However, following the "regulated self-regulation" framework proposed by the associations, this power would be principled and limited by the platforms' commitments, as highlighted by ALAI and Câmara.e-net.

> *In this scenario, regulated self-regulation appears to be the best solution since, based on the **establishment of guiding principles by the supervisory body with commitments established by the platforms**, it is an effective mechanism that will allow the particularities of the actors involved to be considered and will enable the continuity of innovation [our emphasis].*

Brasscom added that this power must be exercised by ensuring the dialogue among the government, the industry, and the society, i.e., by observing "all the stages of the regulatory process, particularly Subsidy Requests, Regulatory Impact Analysis (RIA), and Public Consultations."

Following the same regulated self-regulation approach, Abranet only mentioned **supervisory power**. According to the association, the regulatory entity would be responsible for "monitoring the application of legally established guidelines, as well as the compliance with self-regulation commitments." However, it emphasized that "the public authority is the primary responsible entity for supervising and monitoring the self-regulation activity, developed and conducted by the market agents themselves." ALAI and Câmara.e-net also mentioned that exercising sanctioning power requires knowledge and competence "due to the specificities of the digital world and its continuous transformations."

TelComp did not mention any specific duty or power. However, as it proposed assigning Anatel as the regulatory body for platforms, it is assumed that all roles and powers of a regulatory agency are applicable.

Among **third-sector entities** (CDR, Idec, DiraCom, Vero Institute, and IRIS) that proposed the creation of a regulatory entity –excluding councils and private entities, which, in general, appeared in a regulatory system and linked to another higher authority – the most frequently cited were **supervisory and monitoring power**, **normative and regulatory power**, and **sanctioning power**. It should be noted that IRIS mentioned the "promotion of digital education" as a responsibility of the autonomous regulatory body. Moreover, DiraCom's input was very detailed, listing several specific duties and powers of this authority, including, in addition to those mentioned, the **power to receive and resolve complaints**, **advisory and research duties**, and **the duty to determine and assess risks**. The Vero Institute also mentioned the latter as "systemic risk impact analyses,"[89] probably referring to Bill 2,630 (BRASIL, 2020).

Several other duties and powers mentioned by those third sector entities, such as promoting multi-stakeholder participation in their fields of activity (IRIS), defining advertising limits and duties and establishing concrete transparency measures (Idec), analyzing transparency reports (Instituto Vero), approving and reviewing the codes of conduct of regulated application providers (DiraCom), communicating and applying General Comment 25 of the United Nations (UN) on children and adolescents in the digital environment (INSTITUTO ALANA; MPSP, 2022), among others. Despite being more specific, such functions may also be considered part of the regulatory, supervisory, or intervention powers.

As previously mentioned, some inputs of the third sector proposed not only an authority along the lines of an autonomous public body but a regulatory system, with a multi-stakeholder council and/or

[89] According to the contribution of the Vero Institute: "Among the attributions, we highlight: i) competence to regulate obligations; ii) competence to monitor and apply sanctions; iii) competence to analyze transparency reports and analyze the impacts of systemic risks; iv) coordination with other public spheres, such as ANPD, Cade, consumer protection agencies."

associated self-regulatory entity, but, in general, did not specify its roles. According to the CDR, the council must have deliberative powers to establish the authority's checks and balances. IRIS and DiraCom stated that the council should be the CGI.br.

From the **scientific and technical community**, LABID/UFBA detailed the duties and powers of that body, highlighting its fundamental role of centralizing the interpretation and application of standards, considering the polycentrism of the Brazilian public administration. REDE highlighted the power to advise the Legislative, Executive, and Judiciary, understood as normative powers. Regarding the moderation of third-party content, Flávio Wagner (UFRGS) mentioned receiving reports and complaints from the self-regulatory entity.[90] Relative to the proposed autonomous supervisory entity, the researcher mentioned "investigation procedures and criteria for applying administrative sanctions to violations of legislation" but did not specify how this sanctioning power would be exercised.

In the **government sector**, DEIN highlighted that a possible specialized entity – whether a new or current institution – must hold the appropriate tools and resources to fulfill its mission.[91]

All sectors supported the **duty of cooperation and articulation**, which, together with normative and regulatory powers, was frequently mentioned and assigned to autonomous

[90] Flávio Wagner (UFRGS) points out "A self-regulatory entity, formed by the platforms themselves, intended to review content and account moderation decisions by its members, through provocation by those directly affected by the decision".

[91] DEIN: "considering the possibility that the same entity eventually created or designated to regulate digital platforms may also be responsible for, for example, defining guidelines and monitoring artificial intelligence markets. In this scenario, the specialized entity responsible for this task – whether it is a new institution or an existing institution with new competencies – must have its own tools and resources in place to fulfill its central objectives, which would appear to be, at this stage of the debate: regulating, economically and socially, digital platforms and companies that develop and implement artificial intelligence systems; periodically defining the list of risks to be mitigated by the actions of these companies; monitoring and sanctioning abuses committed by these companies; in addition to other attributions. Finally, the existence of a possible specialized entity should not exclude the actions and role of other actors and agencies with sectoral regulatory powers – on the contrary, their actions should be harmonious and complementary."

entities and councils or committees. ALAI, for instance, argued that, if created, the regulatory entity should establish an efficient communication channel and seek to cooperate with ecosystem stakeholders and with existing sectoral regulators, thereby avoiding policy and definition conflicts. Idec, from the third sector, asserted that public authorities' actions must be coordinated, preventing *bis in idem*[92] and improving the performance of the public administration through institutional cooperation. DEIN suggested that a possible entity should establish governance committees to coordinate and articulate the actions of the bodies directly related to the matter, organizing the different functions.

5 CGI.BR ROLES AND DUTIES

The mentions on CGI.br positively emphasized the parity of participation of the various social actors and sectors in the council's decisions related to regulating digital platforms. For instance, Slowphone asserted that "the most important aspect is that authorities should always maintain good parity of sectors, i.e., all sectors must be equally represented." Abranet added that "multistakeholderism should be the pillar of the composition of this new administrative structure, composed of representatives of the public and private sectors, civil society, and academia." Several institutions emphasized social participation in the development of the regulation. According to IRIS:

> *The regulation of digital platforms must be guided by the principle of democratic and collaborative Internet governance, taking multistakeholderism as an indispensable reference. The CGI should be responsible for* ***developing guidelines and studies and issuing advice for the governance of platforms, as it does for the Internet****, operating as a space for dialogue and social participation [our emphasis].*

The concern about the independence of institutions involved in regulation was also frequently expressed in the inputs, such as in another excerpt of IRIS' input:

[92] Double liability for the same fact.

> *Within the scope of public power,* ***a governance system that articulates the creation of an independent regulatory authority*** *with an expert technical body and administrative and financial autonomy needs to be established. This authority should be responsible for regulating, monitoring, and applying sanctions in the event of non-compliance to the regulation [our emphasis].*

On this matter, DiraCom's proposal supports the possibility of CGI.br acting as the board of the regulatory body to be created to protect this body from possible capture. To this end, the entity provided more detailed roles for the committee in addition to existing ones:

1. to develop and approve policies and guidelines for Internet applications aiming at achieving the goals of the platform regulation legislation approved in the country;
2. to propose and submit the policies and guidelines referred to in item I to society for consultation;
3. to monitor compliance with the specific legislation based on monitoring analyses and reports by the regulatory body;
4. to formulate and approve guidelines for information disclosure and compliance with transparency obligations by Internet application providers to the regulatory body provided for in specific legislation;
5. to issue guidelines and criteria for defining the hypotheses of crisis/emergency protocols/imminent risks of serious violations to collective harm;
6. to approve, after consulting the regulatory body or at the request of the regulatory body, crisis/emergency protocols/imminent risks of serious violations, including collective harm;
7. to issue guidelines for the development of codes of conduct and validate the codes agreed between large Internet application providers and the regulatory body;
8. to issue guidelines and requirements for the analysis of systemic risks by Internet application providers to be carried out by the regulatory body based on information provided by those providers;

9. to decide, as the last administrative instance in the appeal stage, on an administrative sanction adopted by the regulatory body and
10. to establish guidelines for cooperation and coordination with the Judiciary to comply with the objectives and provisions of specific legislation on platform regulation.

On the other hand, some inputs also expressed concern about preserving the **nature of CGI.br**. Flávio Wagner, from the scientific and technical community, highlighted that the "CGI.br cannot be granted powers that pertain to State bodies, as this would be completely incompatible with its mission." Regarding possible legislation on content moderation, Wagner stated that CGI.br should not have "operational duties, such as validating terms of use of digital platforms or evaluating transparency and 'duty of care' reports prepared by digital platforms." He also mentioned the importance of maintaining the roles established in current legislative instruments, such as the MCI (BRASIL, 2014):

> *The Marco Civil da Internet already provides that CGI.br must establish guidelines to be followed by bodies, such as Anatel, Cade, and Senacon, in dimensions strongly related to digital platform regulation.* ***There is no reason to change this setting. Other regulatory or supervisory activities intended to be assigned to CGI.br may denature the Committee, affecting the Information and Coordination Center of Ponto BR****, which is undesirable, given the history of achievements of the entity, regarded as an international model for Internet governance [our emphasis].*

Some mentions asserted that CGI.br should participate in the councils or entities proposed to regulate the platforms but did not provide further details, indicating the need to determine its possible roles in this regulatory system model.

The CGI.br was also mentioned regarding **advisory and research duties** when building a digital platform regulation system. For instance, CDR emphasized the CGI.br's role in conducting studies, which was mentioned in Bill 2,630 (BRASIL,

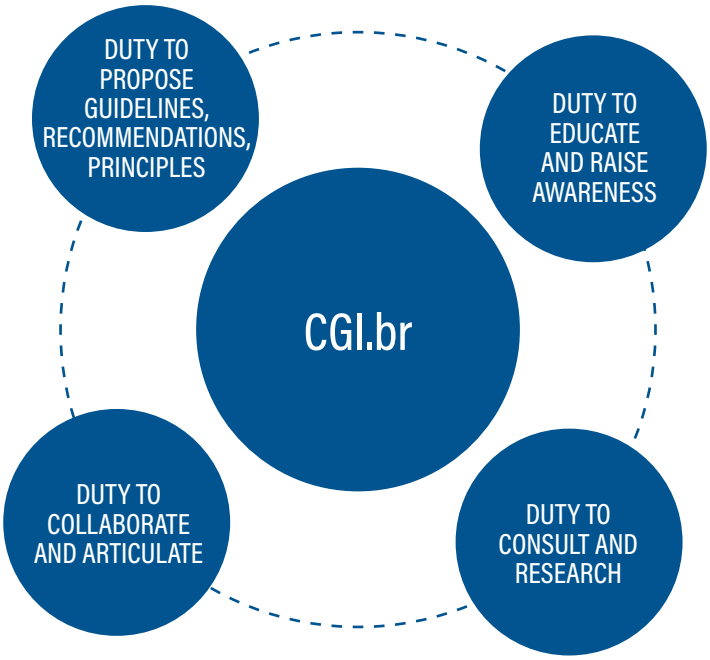
2020).[93] IRIS highlighted that the Committee must develop "guidelines, studies, and advice for digital platform governance, as it does for the Internet, functioning as a space for dialogue and social participation." The technical expertise of the Committee was also considered relevant, as in ISOC Brasil's input, recognizing its importance in the development of significant Brazilian legislation related to the Internet and highlighting its international recognition, which demonstrates it can "guide, with the required restraint and quality, the dialogue in search of the solutions that society demands," given the growing challenges arising from the digitalization of the society and the economy.

As mentioned by the Alana Institute, CGI.br must also strive to carry out activities related to the **duty to educate**, stating that the committee "plays an important role in the dissemination of knowledge related to the digital space."

Figure 3, below, seeks to organize the primary roles assigned to CGI.br in the inputs to the consultation:

[93] According to the CDR: "The Committee's responsibilities related to the regulation and supervision of the functioning of the Internet in Brazil must be maintained, in accordance with Laws N. 12,965/14 and N. 13,853/19. Furthermore, as provided for in Bill 2,630, the CGI.br may conduct studies, issue opinions and propose strategic guidelines on matters related to the regulation of platforms. It would involve three fronts: i) a supervisory and deliberative entity formed by representatives of the three branches of government (Legislative, Executive, Judiciary), the Brazilian competition and data protection authorities, Anatel and OAB; ii) a self-regulatory entity responsible for dealing with specific cases of content moderation and iii) the CGI.br, which already plays a fundamental role in publishing studies, guidelines and recommendations for the development of the Internet in the country."

FIGURE 3 – MAIN ROLES AND DUTIES PROPOSED FOR THE CGI.BR



SOURCE: PREPARED BY THE AUTHORS.

The duties more frequently associated with CGI.br are to provide guidelines and advice, which may be defined as a **normative and regulatory power**. The inputs did not detail its roles and duties, which were broadly described as related to Internet governance and the protection of users' rights and interests, for instance. The development of **principles** by the CGI.br was also mentioned in some inputs.

Generally, inputs mentioning CGI.br support maintaining its duties, as described in Decree 4,829 (BRASIL, 2003). However, the inputs suggesting the integration of CGI.br into a regulatory system did not explain what changes would be required to preserve the committee's roles and duties regarding the use and development of the Internet and simultaneously include those related to digital platform regulation. The need to further discuss how CGI.br's integration into this system is illustrated by the proposal by LABID/UFBA, for whom the public regulatory authority should be linked to CGI.br while maintaining its structure unchanged, which would require further description, as the CGI.br is a private entity.

6 ANATEL'S ROLES AND DUTIES

An important issue discussed in Axis 3 was Anatel's possible duties for digital platform regulation, changing the traditional "separation between telecommunications infrastructure and the Internet as a Value-Added Service, a principle provided for in Norm 4" and recognized in the General Telecommunications Law (BRASIL, 1997a), as explained by Flávio Wagner, from the scientific and technical community.

TelComp strongly supported transforming Anatel into a digital platform regulatory body. Other suggestions for adapting the existing bodies, such as DEIN's, were made but did not explicitly mention Anatel. According to TelComp, the layered structure of the value chain in which the "infrastructure and telecommunications services support the upper layer, conventionally called 'over the top' (OTT) structure," puts Anatel in a favorable position to assume the role of a new regulatory agency that includes digital platforms in its scope. TelComp argued that the separation between services provided by telecommunications and OTT companies no longer makes sense due to the competition for digital markets such as messaging, given that "the entire Brazilian population [has replaced] traditional voice and messaging services by the voice and messaging functionality of OTT applications, for instance." For the same reason, i.e., the regulatory proximity of those industries, Abranet stated that "at best, because the regulation of the network infrastructure tangentially touches the operation of the application layer on the Internet, Anatel may be considered as yet another representative of the public sector in the new authority now being outlined."

According to TelComp, Anatel, as it already regulates telecommunications service providers and Internet access providers, is in a privileged position to analyze the entirety of the relationships among the different layers of the Internet and monitor the set of rules eventually established for digital platforms. TelComp's proposal, therefore, is closer to a model with a greater degree of centralization and state protagonism; however, the association stated that the assignation of Anatel as a digital platform regulator must be guided by the adoption of rules that promote the use of responsive regulation tools and their incentives, in order to move away from the command and control model (according to regulatory approaches presented in Axis 1 of this document).

On the other hand, several organizations from the third sector and the scientific and technical community expressed concern about the possibility of Anatel becoming the regulatory entity for digital platforms, alleging the low effectiveness of the sanctions applied by it, its lack of expertise on this matter, and the mismatch between Anatel's actions and the problems identified by consumers, which, these entities claim, are the result of a process of regulatory capture by economic interests. In summary, according to the CDR systematization, a large part of these third-sector entities consider that:

> *i) Anatel* ***does not have the necessary expertise*** *in platform regulation issues, in addition to having repeatedly failed to fulfill its duties in the telecommunications sector; ii) assigning platform regulation to the agency could worsen this scenario, hindering the advancement of significant connectivity in Brazil and causing the economic interests of platforms and telecommunications companies to prevail over the interests of users; and iii)* ***Anatel has historically resisted the participation of civil society****, which is incompatible with the multi-stakeholder and collaborative Internet governance model in the country [our emphasis].*

7 SANCTIONING AND REDRESS MEASURES

Nineteen inputs on sanctioning measures were identified. Some, such as those of Alex Camacho from the scientific and technical community and Black Women Bloggers from the third sector, asserted that principles and values should guide the application of reparation and sanctioning measures, mentioning that sanctions and their criteria must be transparent, clear, and proportional to the gravity of the violations and the impacts caused. DEIN's contribution specified these criteria in the context of digital platforms, proposing that sanctioning and reparation measures be "subject to weighing and consideration according to the level of risk, the abuse committed by the inspected entity, its field of activity, its gatekeeping power, and its size."

Two sanctions were notably mentioned: fines and blocking and suspension of applications.

Regarding **blocking**, ISOC Brasil warned that the indiscriminate use of this sanctioning measure may fragment the experience of entire populations in terms of network connection in its various facets.[94] The entity emphasized the importance of i) establishing principles for the application of blocking as a legal sanction, defining it as an extreme measure; ii) establishing specific and restricted criteria and guidelines for its application, and iii) establishing transparency and communication measures regarding the unavailability of the service to mitigate economic and social impacts. Possible blocking abuses were also addressed by EFF, CDR, and DiraCom, who proposed that the measure should only be applied when agreed by the absolute majority of a collegiate judicial body. Victor Lippi Zaccariotto, from the scientific and technical community, stated that direct sanctions against users should be avoided as much as possible.

The **levying of fines** was mentioned regarding the failure to comply with obligations to the reporting channel, according to Câmara.e-net's input.[95] In addition to being proportional to the impact caused, Black Women Bloggers stated that fines should be levied on services that do not comply with anti-racist local laws. However, Câmara.e-net mentioned imposing limits on any compensation sought.

Another relevant topic discussed in this section was the **liability regime**. Câmara.e-net stressed that the implementation of reparation and sanction measures should consider digital platform liability limitations, which, specifically in the case of third-party content, must comply with the liability regime of the MCI. The Nupef Institute, in contrast, supported enhancing the liability of platforms that deliberately disseminate disinformation, particularly indisputably false content.

---

[94] According to ISOC Brasil: "Blocking applications in national territory materializes the fragmentation of the network. Even if it does not do so on a global scale, the suspension of an application imposes a territorial limitation on network users. This is because measures of this type prevent users in Brazil from sharing information with users in other regions of the world and vice versa, thus creating breaking points in the network connection."

[95] For Câmara.e-net: "under penalty of i) encouraging the filing of lawsuits that seek especially compensation and, consequently, overloading the already busy Judiciary and ii) creating an excessive burden for the platforms, making their business model unfeasible by creating such unpredictability of their eventual exposure with the launch of advertising campaigns"

An alternative described by the ITS, although it does not change the MCI liability regime (BRASIL, 2014), points to new responsibilities and, therefore, other possibilities for sanctioning platforms: administrative sanctions should be focused on content moderation as a "system," i.e., for failure to comply with the "duty of care" and to act to fight systemic risks, as provided for in Bill 2,630 (BRASIL, 2020). However, such sanctions still need to be defined more precisely to prevent their abuse in the future. The change in the liability regime is also addressed in Axis II of this report. Likewise, DiraCom's contribution emphasized that the regulatory body must apply collective measures.

Idec defended the importance of guaranteeing the participation of third-party stakeholders in sanctioning or inspection processes. Regarding the inspection process, José Antônio Galhardo, from the government sector, argued that any competent agency should be equipped to detect any non-compliance with regulations, using technology to monitor and audit the various layers of the digital platform business systems.

Lastly, the Alana Institute addressed the issue of redress, arguing that "adequate redress includes restitution, compensation, and satisfaction, and may require an apology, correction, removal of illegal content, access to psychological recovery services or other measures." For the institute, in the digital environment, "the vulnerability of children and the need to act promptly to stop current and future damage" must be considered, ensuring that violations do not recur.

8 REGULATORY APPROACHES

Due to the diversity of terms and nomenclatures used in the inputs to identify regulatory approaches, this report organized such approaches for systematization and comparison purposes according to regulatory models: i) self-regulation, ii) co-regulation, and iii) command-and-control regulation. Few inputs proposed the **classic command-and-control regulation model**. Although frequent in regulatory debates, the **responsive regulation model** was not explicitly or frequently mentioned in the inputs to the consultation, and several of its mechanisms were dispersely cited, especially in co-regulation approaches. It should be noted that most inputs suggested characteristic elements of different classic models, creating

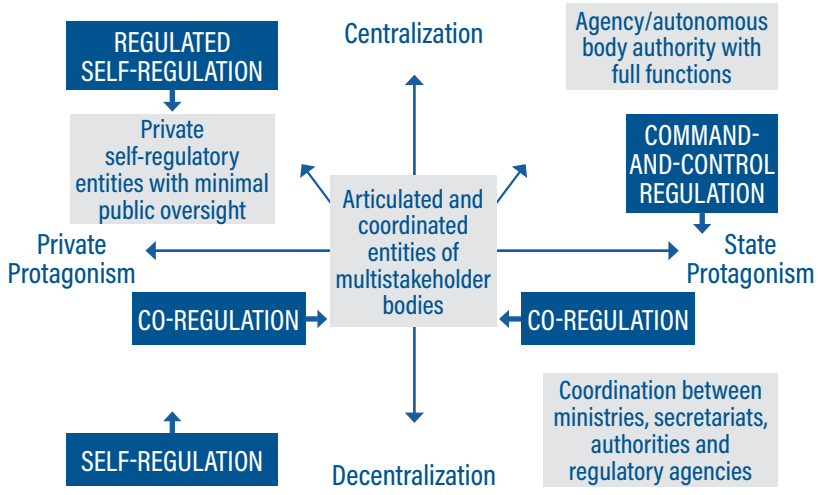
additional challenges for the organization and classification of the regulatory approaches mentioned.

The analysis of the inputs suggests that the **approaches are essentially defined by two conceptual vectors**. The first vector discusses whether the State or the private sector should have a protagonist role, while the second considers whether the locus of decision-making should be concentrated in a single institution or decentralized across several entities and actors.

Strict self-regulation, for instance, would have little or no State protagonism and a decentralized decision-making locus, as it would be dispersed across digital platforms. In contrast, in regulated self-regulation, the locus of decision-making would be concentrated in a single private self-regulatory entity, and the State would have little protagonism.

In a setting of higher State protagonism, of co-regulation (or even command-and-control regulation), regulatory responsibilities may be concentrated in a single or several public bodies. In this case, flows and instruments that expand the role attributed to multi-stakeholder bodies are expected, balancing state protagonism with that of other sectors. The highest point of State protagonism would be the typical, highly concentrated command-and-control type, as illustrated in Figure 4.

FIGURE 4 – CONCEPTUAL APPROACHES FOR DISCUSSION OF REGULATORY MODELS



SOURCE: PREPARED BY THE AUTHORS.

Based on those vectors, the inputs to the consultation were divided into three groups: i) supporting **self-regulation**, with an attitude of caution or opposition towards State regulation; ii) the defense of **regulation along the lines of independent regulatory authorities**, approaching a form of governance characterized by strict lawfulness and the delegation of powers to institutions that are autonomous to the government and; iii) the defense of **governance based on direct action by the State, structured essentially in ministerial departments and existing regulatory agencies or authorities**. Despite the significant model differences, the defense of multistakeholderism, transparency, and social participation as principles of regulatory arrangements is noteworthy. The main differences observed are related to how actors participate and the decision-making locus.

8.1 DECENTRALIZED SELF-REGULATION AND REGULATED SELF-REGULATION

Some business associations recommended caution and risk analyses before creating any digital platform regulatory entity to preserve values such as innovation and free enterprise. A set of inputs stands out, such as those from Câmara.e-net and ALAI[96], which consider that tools available in the Brazilian legal and regulatory framework are sufficient to face the challenges presented by the emergence of digital platforms in an approach identified as decentralized self-regulation.

A larger group of business associations supported regulated self-regulation. As explained by Abranet, "the public authority is essentially responsible for supervising and monitoring the self-regulatory activity, which is developed and performed collectively by the market agents themselves," in opposition to the classic command-and-control regulation model, where the public authority establishes the rules and imposes sanctions on non-compliant private agents. As Abranet and Brasscom argued, a possible supervisory body, despite having technical competence and functional independence, should only establish guiding

[96] According to ALAI: "It is impossible to assess the creation of new institutions without a clear definition of the issues that regulation intends to remedy. It is prudent to assess the impact of any legislation/regulation before doing so."

principles and oversee the self-regulatory activities developed and executed by market agents and, therefore, have limited powers.

Regarding the regulated self-regulation approach, Brasscom proposed adopting a regulatory perspective based on risk assessment, i.e., "which identified [...] the greatest risks of platform activities and addresses them individually to ensure that the intervention is truly required and proportional, thereby avoiding extensive administrative activity."

8.2 CENTRALIZED CO-REGULATION AND DECENTRALIZED CO-REGULATION

Many inputs supported the concept of co-regulation (concentrated or decentralized). Those who defended concentrated co-regulation suggested creating a specific autonomous entity for digital platform regulation, endowed with technical and administrative autonomy and acting in coordination with public and private bodies.

This perspective is supported by third-sector entities, such as CDR, Idec, IRIS, and IP.rec, for whom an independent regulatory authority should centralize the application and interpretation of platform regulation standards, concentrating standardization, inspection, and sanctioning functions. Therefore, there is high State protagonism, and the regulatory autonomous public body has the decision-making power. However, a multi-stakeholder council with deliberative capacities – be associated or not with CGI.br – should establish checks and balances for such a body.

LABID/UFBA's input also indicates regulatory concentration as it proposed establishing an authority that would centralize the interpretation, supervision, and application of the digital platform regulation "given that polycentrism may generate legal uncertainty." The concern with possible legal uncertainty was also mentioned by ANPD, who stated that imprecise limits for exercising legal powers in the absence of cooperation rules would bring legal uncertainty and **risks of regulatory fragmentation**.

Regarding possible governance models, DEIN suggested a hybrid model in which a specialized entity coordinates and articulates with other public or private entities.

Other inputs suggested that existing public bodies regulate digital platforms, such as ministries and regulatory agencies, with

distributed or shared attributions, i.e., not creating new bodies, in an approach identified as **decentralized co-regulation**. In this model, the regulation would be dispersedly enforced, coordinating and distributing functions among ministries and authorities according to previously existing thematic competencies. The main concerns raised were public spending and, in particular, possible regulatory capture and the liberalizing nature of the Regulatory State model, as pointed out by Flávia Lefèvre[97] and the Nupef Institute from the third sector, for whom "the possible capture of a single regulatory body by private economic or political interests significantly increases the risk of imbalance in regulation." Therefore, creating a regulatory system based on existing bodies should be considered. The Special Commission on Digital Law of the Federal Council of the OAB also proposed a tripartite Brazilian System for the Regulation of Digital Platforms, composed of a Digital Policy Council, CGI.br, and a Self-Regulation Entity.

Flávia Lefèvre also supported the institutional arrangement established by Decree 8,771 (BRASIL, 2016), which regulated the MCI (BRASIL, 2014) and assigned to Senacon, SBDC, and Anatel, in line with the guidelines established by CGI.br, the role of ensuring transparency and monitoring of digital platforms, in addition to the enforcement of the rights established by law.

Likewise, the Nupef Institute advocated creating a regulatory system based on the existing bodies, emphasizing that the established regulatory structures should apply the existing laws to digital platforms. According to Nupef, this system would involve establishing a structure to monitor and supervise the application of the law and have multi-stakeholder participation.

---

[97] According to Flávia Lefèvre: "the regulatory agency model – the mainstay of neoliberalism – despite advertising its autonomy and independence has historically acted in a way captured by private interests and, therefore, it is clearly inadequate for regulating digital platforms. Consequently, I believe a regulatory structure comprising a body representing companies, an Interministerial Council, and CGI.br makes more sense. Platform activities involve multiple sectors with the potential for large-scale impact on fundamental, economic, cultural, educational, political, social, and labor rights, among others, and a centralized model of regulation with reduced democratic representation, as is the case with agencies due to their legal configurations, will not be able to regulate properly to guarantee rights across such a broad spectrum."

8.3 CONSENSUS AND DISSENT ON REGULATORY APPROACHES

Based on the thematic groupings presented, consensus and dissent were identified. Inputs supporting regulated self-regulation and concentrated co-regulation defended an entity with financial, functional, and administrative autonomy. However, their main differences are related to the powers and duties of that public authority. In the regulated self-regulation approach, the authority's supervisory and sanctioning powers must be limited to the rules defined in the self-regulation framework, and its normative power must be fundamentally based on principles. On the other hand, in the concentrated co-regulation model, the regulatory agency or authority would have full normative, supervisory, and sanctioning functions and impose specific transparency rules for digital platforms, for instance. In other words, despite some consensus among most business associations and part of the third sector regarding concentrating decision-making in an autonomous institution, there is disagreement regarding State protagonism.

The inputs also indicate dissent among third-sector organizations regarding the decision-making locus and administrative nature, concentrated in a regulatory authority of indirect administration or dispersed across several public institutions and articulated by a council or similar structure. Nevertheless, most organizations agree on the central role of the State in safeguarding social participation instruments and its association with multi-stakeholder councils.

9 CONCLUSION OF AXIS 3

The inputs to Axis 3 of the consultation on '**how to regulate**' indicate some consensus, particularly on the guiding principles of the institutions responsible for regulation. However, significant dissent and nuances were identified regarding the potential conceptual models and institutional designs of the agents responsible for ensuring the obligations imposed by regulation.

As for the principles and guidelines for the platform regulation governance model, there was no fundamental dissent about the stated principles. The most cited principles were multistakeholderism, independence, and transparency. The principles of specificity, international cooperation, innovation, proportionality, and lawfulness were also mentioned.

The institutions proposed for implementing and monitoring digital platform regulation varied in legal nature, the role of the State and private entities, and the level of concentration in the decision-making poles. A relevant group of participants proposed creating an authority for policy regulation, implementation, and monitoring, endowed with administrative, financial, and functional autonomy and located in indirect public administration. Several inputs asserted that such an entity should be linked to a multi-stakeholder council with deliberative capacity, creating a regulatory system. Another significant group proposed creating a governance system with no central regulatory entity composed of institutions of varying legal nature and roles. Furthermore, among those supporting the creation of a regulatory system, many mentioned the participation of CGI.br. Finally, although in smaller numbers, some participants proposed a self-regulatory entity and an autonomous supervisory multi-stakeholder entity. In particular, the potential benefits and risks of the participation of CGI.br and Anatel in this institutional design of regulatory governance were emphasized.

Variations and agreements on the responsibilities of each of the proposed institutions were identified in the inputs. The most mentioned duties and powers include supervisory and monitoring power, normative and regulatory power, sanctioning power, power to receive and resolve complaints, the duty to research, educational duty, the duty to identify and assess risks, and the duty of cooperation and articulation. Although mentioned by all sectors, such have different meanings. For instance, in the regulated self-regulation approach proposed by a significant part of the private sector, the scope of the inspection and regulatory powers are narrower than in models with greater State protagonism.

Fines and blocking/suspending applications were the most frequently mentioned sanctioning measures. Some participants expressed concerns about the proportionality of sanctions, particularly regarding suspensions and blocking.

Regarding the regulatory models that should inspire Brazilian regulation, in general, the inputs received are divided between those that defend i) self-regulation, which may include a monitoring regulatory authority with restricted powers; ii)

regulation along the lines of independent regulatory authorities; and iii) governance as a 'system' structured essentially in ministerial departments and existing regulatory agencies or authorities.

Although the proposed models were significantly different, all defended multistakeholderism, transparency, and social participation as principles of regulatory arrangements, varying only relative to how actors participate and where the decision-making locus is.

REFERENCES

AUSTRALIA Online Safety Act 2021, no. 76. Canberra: Australian Government, Mar 17. 2021. Available at: https://www.legislation.gov.au/Details/C2021A00076. Access on Dec 11, 2023.

BRASIL Decree-Law 200 of Feb 25, 1967. It provides for the Federal Administration's organization, establishes Administrative Reform guidelines, and contains other provisions. Brasília: Presidency of the Republic, Feb 25, 1967. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm. Access on Dec 11, 2023.

BRASIL Law 6,533 of May 24, 1978. It regulates the professions of artists and technicians in entertainment shows and contains other provisions. Brasília: Presidency of the Republic, May 24, 1978. Available at: https://www.planalto.gov.br/ccivil_03/leis/l6533.htm. Access on Dec 11, 2023.

BRASIL Law 8,069 of Jul 13, 1990. It provides for the Statute of Children and Adolescents and other measures. Brasília: Presidency of the Republic, Jul 13, 1990a. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Access on Dec 11, 2023.

BRASIL Law 8,078 of Sept 11, 1990. It provides for consumer protection and other measures. Brasília: Presidency of the Republic, Sept 11, 1990b. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Access on Dec 11, 2023.

BRASIL Law 8,213 of Jul 24, 1991. It provides for Social Security Benefit Plans and other measures. Brasília: Presidency of the Republic, Jul 24, 1991. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8213compilado.htm. Access on Dec 11, 2023.

BRASIL Law 9,472 of Jul 16, 1997. It provides for the organization of telecommunications services, the creation and operation of a regulatory body, and other institutional aspects under Constitutional Amendment 8 of 1995. Brasília: Presidency of the Republic, Jul 16, 1997a. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Access on Dec 11, 2023.

BRASIL Law 9,504 of Sept 30, 1997. It establishes rules for elections. Brasília: Presidency of the Republic, Sept 30, 1997b. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Access on Dec 11, 2023.

BRASIL Law 9,784 of Jan 29, 1999. It regulates the administrative process within the Federal Public Administration. Brasília: Presidency of the Republic, Jan 29, 1999. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Access on Dec 11, 2023.

BRASIL Law 9,986 of Jul 18, 2000. It provides for the management of human resources in regulatory agencies and other measures. Brasília: Presidency of the Republic, Jul 18, 2002. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9986.htm. Access on Dec 11, 2023.

BRASIL Law 10,406 of Jan 10, 2002. It establishes the Civil Code. Brasília: Presidency of the Republic, Jan 10, 2002. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Access on Dec 11, 2023.

BRASIL Decree 4,829 of Sept 3, 2003. Provides for the creation of the Internet Steering Committee in Brazil – CGI.br, on the Internet governance model in Brazil, and contains other provisions. Brasília: Presidency of the Republic, Sept 3, 2003. Available at: https://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Access on Dec 11, 2023.

BRASIL Law 12,485 of Sept 12, 2011. It provides for conditional access to audiovisual communication; amends Provisional Measure 2,228-Sept 1 6, 2001, and Laws 11,437 of Dec 28, 2006, 5,070 of Jul 7, 1966, 8,977 of Jan 6, 1995; and 9,472 of Jul 16, 1997; and contains other provisions. Brasília: Presidency of the Republic, Sept 12 2011a. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12485.htm. Access on Dec 11, 2023.

BRASIL Law 12,529 of Nov 30, 2011. It structures the Brazilian Competition Defense System; provides for the prevention and repression of economic order violations; amends Law 8,137 of Dec 27, 1990, Decree-Law 3,689 of Oct 3, 1941 – Code of Criminal Procedure, and Law 7,347 of Jul 24, 1985; repeals provisions of Law 8,884 of Jun 11, 1994, and Law 9,781 of Jan 19, 1999; and contains other provisions. Brasília: Presidency of the Republic, Nov 30, 2011b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm. Access on Dec 11, 2023.

BRASIL Decree n. 8,135, of Nov 4, 2013. It provides for data communications by the direct federal public administration, federal autonomous bodies, and federal foundations, as well as for the exemption from bidding in contracts that may compromise national security. Brasília: Presidency of the Republic, Nov 4 2013a. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm. Access on Dec 11, 2023.

BRASIL ANP Resolution 41, of Nov 5, 2013. It establishes the requirements for authorizing the retail sales of automotive fuels and their regulation. Brasília: ANP, 5 Nov. 2013b: Available at: https://www.legisweb.com.br/legislacao/?id=261502. Access on Dec 11, 2023.

BRASIL Law no. 12,965, of Apr 23, 2014. It establishes the principles, guarantees, rights, and duties for using the Internet in Brazil. Brasília: Presidency of the Republic, Apr 23, 2014. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Access on Dec 11, 2023.

BRASIL Decree 8,771 of May 11, 2016. It regulates Law 12,965 of Apr 23, 2014, to address the admitted hypotheses of discrimination of data packages on the Internet and traffic degradation, establishes data storage and protection requirements to connection and application providers, establishes transparency measures for the disclosure of registration data requested by the public administration, and establish parameters for monitoring and investigating violations. Brasília: Presidency of the Republic, May 11, 2016. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/de-creto/d8771.htm. Access on Dec 11, 2023.

BRASIL Law 13,709, of Aug 14, 2018. General Data Protection Law (LGPD). Brasília: Presidency of the Republic, Aug 14, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Access on Dec 11, 2023.

BRASIL Law 13,848, of Jun 25, 2019. It provides for the management, organization, decision-making process, and social control of regulatory agencies; amends Law 9,427 of Dec 26, 1996, Law 9,472 of Jul 16, 1997, Law 9,478 of Aug 6, 1997, Law 9,782 of Jan 26, 1999, Law 9,961 of Jan 28, 2000, Law 9,984 of Jul 17, 2000, Law 9,986 of Jul 18, 2000, Law 10,233 of Jun 5, 2001, Provisional Measure 2,228-Sept 1 6, 2001, Law 11,182 of Sept 27, 2005, and Law 10,180, of Feb 6, 2001. Brasília: Presidency of the Republic, Jun 25, 2019. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm. Access on Dec 11, 2023.

BRASIL Bill 2,630. Institutes the Brazilian Law of Freedom, Responsibility, and Transparency on the Internet. Brasília: Federal Senate, Jul 3, 2020. Available at: https://www.camara.leg.br/propostas-legislativas/2256735. Access on Dec 11, 2023.

BRASIL *Attacks on schools in Brazil*: analysis of the phenomenon and recommendations for government action. Brasília: GT Specialists in Violence in Schools, 2023a. Available at: https://www.gov.br/mec/pt-br/acesso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados/relatorio-ataque-escolas-brasil.pdf. Access on December 11, 2023.

BRASIL *Working Group seeking regulation for app freelance labor is set up in Brasília.* Brasília: MTE, June 5, 2023b. Available at: https://www.gov.br/trabalho-e-emprego/pt-br/noticias-e-conteudo/2023/junho/grupo-de-trabalho-que-busca-regulacao-de-trabalho-por-aplicativo-e-instalado-em-brasilia. Access on Dec 11, 2023.

'NAZI hunter,' she discovered 1,117 extremist groups in Brazil. Ecoa UOL,May 18, 2023. Available at: https://www.uol.com.br/ecoa/ultimas-noticias/2023/05/18/com-ossos-de-vidro-ela-lutou-contra-neonazistas-e-pelos-diretos-dos-pcds.htm. Access on Dec 15, 2023.

CAMELLO, A. P. *et al*. Briefing temático #2: Trabalho sob demanda no Congresso (2010-2020) [*Thematic briefing #2: Work on demand in in the National Congress (2010-2020)*]. São Paulo: CEPI FGV Direito SP, January 29, 2021a. Available at: https://repositorio.fgv.br/server/api/core/bitstreams/43c3c6cb-8101-460b-8f6d-f75933b6ba3c/content. Access on Jan 21, 2024.

CAMELLO, A. P. et al. Gig economy e trabalho em plataformas no Brasil: do conceito às plataformas [*Gig economy and platform work in Brazil: from concept to platforms*]. São Paulo: CEPI FGV Law SP, 2021b. Available at: https://repositorio.fgv.br/items/7048f45b-945a-42a-2-9474-58e9624435fb. Access on Dec 11, 2023.

COMENTÁRIO Geral n. 25 sobre o direito das crianças em relação ao ambiente digital [*General comment 25 on children's rights in relation to the digital environment*]. São Paulo: ALANA INSTITUTE; MPSP. 2022. Available at: https://alana.org.br/wp-content/uploads/2022/04/CG-25.pdf. Access on Dec 11, 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.BR). Ações e Diretrizes para a Regulação de Plataformas Digitais no Brasil [***Actions and Guidelines for the Regulation of Digital Platforms in Brazil***]. São Paulo: NIC.br|CGI.br, Jan 27, 2023a. Available at: https://cgi.br/publicacao/acoes-e-diretrizes-para-a-regulacao-de-plataformas-digitais-no-brasil/. Access on Dec 11, 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.BR). Consulta sobre Regulação de Plataformas Digitais [***Consultation on Digital Platform Regulation***]. São Paulo: NIC.br|CGI.br, 2023b. Available at: https://dialogos.cgi.br/documentos/debate/consulta-plataformas. Access on Dec 11, 2023.

EUROPEAN UNION (EU). Regulation (Eu) 2016/679 of the European Parliament and of the Council of Apr 27, 2016, on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, p. 1-88, May 4, 2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Access on Dec 11, 2023.

EUROPEAN UNION (EU). Document 32022R1925. Regulation (EU) 2022/1925 of the European Parliament and of the Council of Sept 14, 2022, on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). ERL-Lex, Oct 12, 2022. Available at: https://eur-lex.europa.eu/eli/reg/2022/1925. Access on Dec 11, 2023.

FERNANDES, V. O. Direito da Concorrência das Plataformas Digitais – entre abuso de poder econômico e inovação [***Competition Law of Digital Platforms – between abuse of economic power and innovation***]. São Paulo: Thomson Reuters, 2022.

GAWER, A. Bridging differing perspectives on technological platforms: Toward an integrative framework.Research Policy, vol. 43, no. 7, p. 1239- 1249, Sept. 2014. Available at: https://www.sciencedirect.com/scien ce/article/pii/S0048733314000456. Access on Dec 11, 2023.

GOMES, W.; AMORIM, P. K. D. F.; ALMADA, M. P. Novos desafios para a ideia de transparência pública [***New challenges for the idea of public transparency***]. E-Compós, v. 21, n. 2, April 4, 2018. Available at: Available at: https://e-compos.org.br/e-compos/article/view/1446. Access on Dec 11, 2023.

GOV.UK. Competition and Markets Authority (CMA). London: CMA, n.d. Available at: https://www.gov.uk/government/organisations/competition-and-markets-authority. Access on Dec 11, 2023.

GRUPO DE TRABALHO INTERNET E DEMOCRACIA DO CGI.BR (GT INTERNET E DEMOCRACIA). (coord.). Relatório Internet, Desinformação e Democracia [*Internet, Disinformation and Democracy Report*]. São Paulo: NIC.br|CGI.br, 2020. Available at: https://www.cgi.br/media/docs/publicacoes/4/20200327181716/relatorio_internet_desinformacao_e_democracia.pdf. Access on Dec 11, 2023.

INSTITUTO PARA O DESENVOLVIMENTO DO JORNALISMO (PROJOR). Atlas da Noticia 2022. [News Atlas 2022]. São Paulo: Projor, Feb. 2022. Available at: https://docs.google.com/presentation/d/e/2PACX-. Access on Dec 11, 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Aspirational targets for 2030. Achieving universal and meaningful digital connectivity in the Decade of Action. Geneva: IUT, April 19, 2022. Available at: www.itu.int/itu-d/meetings/statistics/umc2030/. Access on Dec 11, 2023.

LUMA PARTNERS. *A Visual Guide to the Digital World*. New York: Luma, n.d. https://lumapartners.com/lumascapes/. Access on Dec 11, 2023.

MENDES, R. M.; MISKULIN, R. G. S. A análise de conteúdo como uma metodologia [*Content analysis as a methodology*]. Research Notebooks, v. 47, n. 165, p. 1044-1066, Jul./Sept. 2017. Available at: https://www.scielo.br/j/cp/a/ttbmyGkhjNF3Rn-8XNQ5X3mC. Access on Dec 11, 2023.

NOOREN, P. *et al.* Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options. Policy & Internet, vol. 10, no. 3, p. 264-301, Sep. 2018. Available at: https://onlinelibrary.wiley.com/doi/abs/10,1002/poi3,177. Access on Dec 11, 2023.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). Regulação de Plataformas. Os modelos de negócios das plataformas. [*Platform Regulation. The business models of platforms*]. São Paulo: NIC.br|CGI.br,May 20, 2021. Available at: https://www.youtube.com/watch?v=HuUbUpvnw2Y&list=PLQ-q8-9yVHyOb6o0oRk55-KtDtgna_-qeL. Access on Dec 11, 2023.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). Seminário Regulação de Plataformas Digitais no Brasil. Parte 1 (Manhã). [*Seminar on Regulation of Digital Platforms in Brazil. Part 1 (Morning)*]. São Paulo: NIC.br|CGI.br, 1 Sep. 2022. Available at: https://www.youtube.com/watch?v=iGqx8Z96eUc&list=PLQq8-9y-VHyObJyyjdRDttwq0YtTN-sNUv. Access on Dec 11, 2023.

OBSERVATÓRIO EDUCAÇÃO VIGIADA. Mapa Brasil. [*Map of Brazil*]. Belém: IEA; LAES/UFPA, 2021. Available at: https://educacaovigiada.org.br/pt/mapeamento/brasil/. Access on Dec 11, 2023.

OLIVEIRA JÚNIOR, M. et al. (coord.). Guia Análise de Atos de Concentração Horizontal [*Guide to Analysis of Horizontal Concentration Acts*]. Brasília: CADE, 2016. Available at: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/guia-para-analise-de-atos-de-concentracao-horizontal.pdf. Access on Dec 11, 2023.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). *Data Portability, Interoperability and Digital Platform Competition.* Paris: OECD, 2021. Available at: https://web-archi-ve.oecd.org/2021-10-31/591383-data-portability-interoperability-and-digital-platform-competition-2021.pdf. Access on Jan 21, 2024.

INTERNATIONAL LABOUR ORGANIZATION (ILO). *Convention 138.* About the minimum age for admission to employment. Brasília: TST, June 6, 1973a. Available at: https://www.tst.jus.br/documents/2237892/0/Conven%C3%A7%C3%A3o+138+da+OIT++Idade+m%C3%ADnima+de+admiss%C3%A3o+ao+emprego. Access on Dec 11, 2023.

INTERNATIONAL LABOUR ORGANIZATION (ILO). *Recomendation 146.* Recommendation regarding the minimum age for admission to employment. Brasília: TST, June 6, 1973b. Available at: https://www.tst.jus.br/documents/2237892/0/Recomendação+146+da+OIT+Idade+mínima+de+admissão+ao+emprego#:~:text=(1)%20Devem%20ser%20tomadas%20medidas,anos%20alcancem%20um%20nivel%20satisfatório. Access on December 11, 2023.

PINTO, A. G. G. Os Princípios mais Relevantes do Direito Administrativo. [*The Most Relevant Principles of Administrative Law*]. Revista da EMERJ, v. 11, n. 42, p. 130-141, 2008. Available at: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista42/Revista42_130.pdf. Access on Dec 11, 2023.

POELL, T.; NIEBORG, D. B.; DIJCK, J. V. Platformisation. Police Review, vol. 8, no. 4, nov. 2019. Available at: https://www.researchgate.net/publication/337717560_Platformisation#:~:text=Download%20full%2Dtext%20PDF. Access on Dec 11, 2023.

ROCHET, J. C.; TIROLE, J. Platform Competition in Two-sided Markets. Journal of the European Economic Association, vol. 1, no. 4, p. 990-1029, Jun 2003. Available at: https://www.jstor.org/stable/40005175. Access on Dec 11, 2023.

SILVA, V. J.; CHIARINI, T; RIBEIRO, L. C. Economia de plataformas digitais no Brasil. Uma primeira abordagem [*The Economy of Digital Platforms in Brazil. A first approach*]. In: VII Encontro Nacional de Economia Industrial e Inovação (ENEI), Porto Alegre. Anais. Porto Alegre: ABEIN, May 15, 2023. Available at: www.even3.com.br/Anais/vii-enei/642988-A-ECONOMIA-DE-PLATAFORMAS-DIGI-TAIS-NO-BRASIL-UMA-PRIMEIRA-ABORDAGEM. Access on Dec 15, 2023.

SIMÃO, B.; WHO, J.; TORRES, L. P. Autoridades de Proteção de Dados da América Latina: um estudo de modelos institucionais da Argentina, Colômbia e Uruguai. [*Data Protection Authorities in Latin America: a study of institutional models in Argentina, Colombia and Uruguay*]. São Paulo: Idec, May 3, 2019. https://idec.org.br/file/32258/download?token=R8sGSMJD. Access on Dec 11, 2023.

SOCIAL LINKED DATA (SOLID). *Solid*: Your data, your choice. Cambridge: MIT, 2016. Available at: https://solidproject.org/. Access on Dec 11, 2023.

SRNICEK, N. Platform Capitalism. Cambridge, UK; Malden, MA: Polity Press, 2016. Available at: https://mudancatecnologicaedinamicacapitalista.files.wordpress.com/2019/02/platform-capitalism.pdf. Access on Dec 11, 2023.

UNITED STATES S2992 American Innovation and Choice Online Act (AICO). Washington DC: Senate, 2022. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/2992. Access on Dec 11, 2023.